California Department of Public Health

Enterprise-wide On-line Licensing System

Feasibility Study Report

January 15, 2008

California Department of Public Health
1500 Capitol Avenue
Sacramento, CA 95899-7413

TABLE OF CONTENTS

APPENDICES

Information Technology Project Summary Package
Section A: Executive Summary

2.0 INFORMATION TECHNOLOGY: PROJECT SUMMARY PACKAGE

1	Submittal Date	January 15, 2008

		FSR	SPR	PSP Only	Other:
2	Type of Document	X			
	Project Number				

			Estimated Project Dates	
3	Project Title	Enterprise-wide On-Line Licensing	Start	End
	Project Acronym	EOL through Implementation	7/2/2007	7/22/2011
		With Maintenance and Operations Period	11/15/2010	11/15/2011

4	Submitting Department	California Department of Public Health

5	Reporting Agency	Health and Human Services

6	Project Objectives
	The objectives of the EOL project are: • Improve CDPH's ability to protect public health and safety by ensuring accurate and current data is available to perform its responsibilities. This will be done by instituting a standardized system for all licensing and licensing-related functions. • Facilitate customer service through providing the ability to conduct online transactions with CDPH. • Ensure ability to respond to future program requirements by providing flexibility to adapt to a changing statutory, regulatory, and policy environment. • Provide a modern means of internal workflow for regulatory functions. • Provide adequate support for current and future business needs.

7	Proposed Solution
	CDPH proposes to advance the health and safety of Californians by deploying a proven, off-the-shelf integrated software solution that supports the licensing, enforcement, and billing functions of the participating CDPH programs; operates in a manner consistent with CDPH's strategic direction; is scalable to accommodate potential future expansion within CDPH; provides expected levels of customer service (for regulated entities) and public service (to the general public); and complies with the standards defined by the State of California's Chief Information Officer (CIO) and Department of Technology Services (DTS).

8.	Major Milestones	Estimated Completion Date
	FSR Approval by Control Agencies	4/1/2008
	IPOC/IV&V Vendor Procurement	7/1/2008
	Project Management Services Vendor Procurement	7/1/2008
	Systems Integration Vendor Procurement	6/23/2009
	Special Project Report Approval by Control Agencies	10/9/2009
	Implementation Complete: Radiation Safety and Food and Drug Programs	11/15/2010
	Implementation Complete: Medical Waste, Drinking Water OCP, Safe Drinking Water Programs	7/22/2011
	PIER	6/14/2012
	Key Deliverables	Estimated Delivery Date
	Approved Feasibility Study Report	4/1/2008
	Systems Integration Vendor Approval by Control Agencies	9/2/2008
	Phase 4 Systems Testing Documents Completed	11/15/2010
	Phase 5 Systems Testing Documents Completed	5/20/2011
	Phase-out of HAL For Radiologic Health Branch Completed	6/15/2011
	PIER Completed and Delivered	6/14/2012

Information Technology Project Summary Package
Section B: Project Contacts

Project #	
Doc. Type	**FSR**

Executive Contacts								
	First Name	**Last Name**	**Area Code**	**Phone #**	**Ext.**	**Area Code**	**Fax #**	**E-mail**
Agency Secretary	**Kimberly**	**Belshé**	**916**	**654-3724**				**kbelshe@chhs.ca.gov**
Dept. Director	**Mark**	**Horton**	**916**	**440-7400**				**Mark.Horton@cdph.ca.gov**
Budget Officer	**Debbie**	**Shepherd-Juch**	**916**	**324-9238**				**Debbie.Shepherd-Juch@cdph.ca.gov**
CIO	**Bob**	**Ferguson**	**916**	**445-8057**				**Bob.Ferguson@cdph.ca.gov**
Proj. Sponsor	**Mary**	**Winkley**	**916**	**558-1700**				**Mary.Winkley@cdph.ca.gov**

Direct Contacts								
	First Name	**Last Name**	**Area Code**	**Phone #**	**Ext.**	**Area Code**	**Fax #**	**E-mail**
Primary Contact	**Kevin**	**Reilly**	**916**	**445-0275**				**Kevin.Reilly@cdph.ca.gov**
Project Manager	**Anne**	**Drumm**	**916**	**440-7518**				**Anne.Drumm@cdph.ca.gov**

Information Technology Project Summary
Section C: Project Relevance to State and/or Departmental Plans

	What is the date of your current Operational Recovery Plan (ORP)?	Date	August 2007
	What is the date of your current Agency Information Management Strategy (AIMS)?	Date	11/14/2003
	For the proposed project, provide the page reference in your current AIMS and/or strategic business plan.	Doc.	Strategic Plan
		Page #	Goal #3 (not yet paginated)

Project #	
Doc. Type	FSR

		Yes	No
	Is the project reportable to control agencies?	X	
	If YES, CHECK all that apply:		
X	The project involves a budget action.		
	A new system development or acquisition that is specifically required by legislative mandate or is subject to special legislative review as specified in budget control language or other legislation.		
X	The estimated total development and acquisition cost exceeds the departmental cost threshold and the project does not meet the criteria of a desktop and mobile computing commodity expenditure (see SAM 4989 – 4989.3).		
	The project meets a condition previously imposed by Finance.		

Information Technology Project Summary
Section D: Budget Information

Project #	
Doc. Type	FSR

Budget Augmentation Required?		
No	X	
Yes		If YES, indicate fiscal year(s) and associated amount:

FY		FY		FY		FY		FY	
$		$		$		$		$	

PROJECT COSTS

1.	Fiscal Year	FY 2008-09	FY 2009-10	FY 2010-11	FY 2011-12	FY 2012-13	TOTAL
2.	One-Time Cost	480,307	2,685,774	2,073,593	181,765	0	5,421,439
3.	Continuing Costs	0	79,329	700,540	1,007,055	953,055	2,739,979
4.	TOTAL PROJECT BUDGET	$480,307	$2,765,103	$2,774,133	$1,188,820	$953,055	$8,161,418

SOURCES OF FUNDING

5.	General Fund	0	0	0	0	0	$0
6.	Redirection	41,707	257,227	980,297	1,188,820	953,055	$3,421,106
7.	Reimbursements	0	0	0	0	0	$0
8.	Federal Funds	0	0	0	0	0	$0
9.	Special Funds	438,600	2,507,876	1,793,836	0	0	$4,739,312
10.	Grant Funds	0	0	0	0	0	$0
11.	Other Funds	0	0	0	0	0	$0
12.	PROJECT BUDGET	$480,307	$2,765,103	$2,774,133	$1,188,820	$953,055	$8,161,418

PROJECT FINANCIAL BENEFITS

13.	Cost Savings/ Avoidances	$ 0	$ 0	$493,859	$899,218	$904,000	$2,297,077
14.	Revenue Increase	$ 0	$ 0	$ 0	$ 0	$ 0	$ 0

Note: The totals in Item 4 and Item 12 must have the same cost estimate.

Information Technology Project Summary
Section E: Vendor Project Budget

Project #	
Doc. Type	FSR

Vendor Cost for FSR Development (if applicable)	$ 244,705
Vendor Name	Continuity Consulting, Inc.

VENDOR PROJECT BUDGET

1.	Fiscal Year	FY 2008-09	FY 2009-10	FY 2010-11	FY 2011-12	FY 2012-13	TOTAL
2.	Primary Vendor Budget	$ 0	$ 1,134,000	$ 1,239,000	$ 126,000	$ 0	$ 2,499,000
3.	Independent Oversight Budget	$ 48,000	$ 48,000	$ 48,000	$ 4,000	$ 0	$ 148,000
4.	IV&V Budget	$ 57,600	$ 57,600	$ 57,600	$ 4,800	$ 0	$ 177,600
5.	Other Budget	$ 333,000	$ 172,800	$ 230,400	$ 19,200	$ 0	$ 755,400
6.	TOTAL VENDOR BUDGET	$ 438,600	$ 1,412,400	$ 1,575,000	$ 154,000	$ 0	$ 3,580,000

----------(Applies to SPR only)----------

PRIMARY VENDOR HISTORY SPECIFIC TO THIS PROJECT

	Primary Vendor	
	Contract Start Date	
	Contract End Date (projected)	
	Amount	$

PRIMARY VENDOR CONTACTS

	Vendor	First Name	Last Name	Area Code	Phone #	Ext.	Area Code	Fax #	E-mail

Information Technology Project Summary
Section E: Vendor Project Budget

2.6 Section F: Risk Assessment Information

Project #	
Doc. Type	FSR

RISK ASSESSMENT

	Yes	No
Has a Risk Management Plan been developed for this project?	X	

General Comment(s)
Please refer to FSR Section 7, Risk Management Plan.

3.0 BUSINESS CASE

The health and safety of all Californians is entrusted to the California Department of Public Health (CDPH). Despite the enormous responsibilities carried out by this Department, the residents of the state are currently facing significant health and safety risks due to operational challenges and obstacles within the department which can be directly addressed by technology that is currently available in the open market. Through the examples shown in this section – which are representative of many other situations faced by this department every day – this section sets forth the dangers inherent in the current situation, and the business case for implementing available modern technology solutions.

Spotlight – Maximizing services through effective communication

In September 2006, an outbreak of *e. coli* bacteria in California spinach infected approximately 200 people, including some in California, and was international in scope. The infections resulted in 3 deaths. And the effects of the crisis went beyond health. Within our state, where three-quarters of all domestically grown spinach is harvested, farmers faced up to $74 million in economic losses due to this one outbreak (Source: Associated Press). And four months after the outbreak, sales of bagged lettuce products were down nearly 40% (Source: USA Today).

A principal function of CDPH's Food and Drug Branch (FDB) is to respond to such emergency situations, illnesses, outbreaks and product contaminations. Whether it is this example of *e. coli* bacteria on fresh spinach, or pesticides on imported ginger, or bacterial toxins identified in a bottled mint water product, the ability to rapidly communicate with regulated food processing and drug or medical device manufacturing firms can make the difference between an effective recall and removal of a contaminated product from the marketplace,. A comprehensive system with real time data on FDB's regulated community that can be accessed remotely by investigators provide FDB the ability to disseminate information that is critical to protecting the public.

Spotlight – Rapid response to an emergent food safety issue

On November 7, 2007, a container ship struck the San Francisco-Oakland Bay Bridge releasing approximately 58,000 gallons of bunker fuel into the San Francisco Bay. As the spill spread around the bay and out to sea, the fuel oil posed a potential human health concern due to contaminated fish, shellfish and crab harvested for consumption, prompting a closure of all fishing in the affected area. At the same time, CDPH recognized the use of bay water by food processing plants, posing the potential for additional food contamination. A system able to use geographic information system tools to rapidly identify affected businesses from the thousands of licensed firms – particularly queries from field staff working directly with those businesses – would allow more rapid notifications and timely regulatory actions (i.e. embargo or remove-from-sale orders).

Spotlight – Data needed in a major emergency, to protect drinking water safety

In October 2007, a series of major wildfires devastated several parts of Southern California, particularly in San Diego, San Bernardino, and Los Angeles counties. Local health jurisdictions and operators of public water systems were at the forefront of keeping their citizens safe from numerous threats to health and safety, including drinking water safety. CDPH needed to be in immediate contact with more than 1,000 public water systems on a continuous basis. The Ramona public water system in San Diego County, for example, was forced by the emergency to be offline for about a week, requiring extensive contact, support, and monitoring from state CDPH staff. In situations like these, critical information such as the equipment used in water treatment systems must be readily available. Currently, updates are done manually process and at times, updated information is not available in field locations. A more accessible and timely contacts and information system would have been beneficial to staff in responding to the October 2007 fires. This would ensure that the best available data was in the hands of emergency responders, and further underscores the need for electronic storage and access to this critical information from multiple sites.

Spotlight – Paper-based records, manual processes

Due to the many severe limitations of the HAL system (detailed further in this report), many records within the Radiologic Health Branch (RHB) are kept on paper. The offices of this Branch contain so many paper records, that many files can only be kept in stacked boxes, or underneath counters, or in stacked columns. This situation causes unnecessary delays.

In addition to the public health risks created by the current situation, there are numerous lesser problems such as unnecessary burdens placed on regulated entities; backlogs; inadequate customer service; and decreased internal efficiencies which increase the state's costs unnecessarily.

This Feasibility Study Report (FSR) describes the state's initiative to address many public health and safety risks and other problems, such as the ones mentioned briefly above. The department has initiated the Enterprise-wide On-line Licensing (EOL) System project to address these significant operational problems and issues across five CDPH programs:

- Medical Waste Management Program
- Food and Drug Program
- Drinking Water Operator Certification Program
- Safe Drinking Water Systems Program
- Radiation Safety

This section provides the business case for the development and implementation of an EOL system. It describes the programs to be supported by EOL, key problems that the project will address, expected results to be achieved through the implementation of the proposed solution, and the functional requirements.

The remainder of this section is organized as follows:

3.1 Business Program Background

3.1.1 CDPH Mission and Organization Structure

CDPH is dedicated to optimizing the health and well-being of the people in California. CDPH accomplishes this mission through improved access to quality public health services, improved health outcomes, and through reduced health care costs through prevention with services such as disease screening and vaccinations, and patient safety initiatives. The CDPH collaborates with local health departments, agencies and other organizations in these efforts.

The CDPH also ensures these outcomes through the careful regulation and oversight of health care providers and their supporting organizations. The proposed EOL system supports the mission by providing the ability for the CDPH to consistently receive and review applications for initial licenses[1] and renewals, and to oversee services provided under this licensure for adherence to governing law and regulations.

The CDPH is a department under the direction of the California Health and Human Services Agency. On September 14, 2006, the Governor signed Senate Bill 162 (SB 162). SB 162 enacts the California Public Health Act of 2006, which establishes the California Department of Public Health (CDPH) within the existing California Health and Human Services Agency and provides statutory authority to transfer the responsibilities of certain programs from the legacy Department of Health Services (DHS) to the new CDPH. The reorganization became effective July 1, 2007. The new CDPH organization chart is shown in Figure 1.

[1] Throughout this feasibility study report, the terms “license” and “licensing” may be used generically to refer to all licenses, certifications, and registrations issued by CDPH programs.

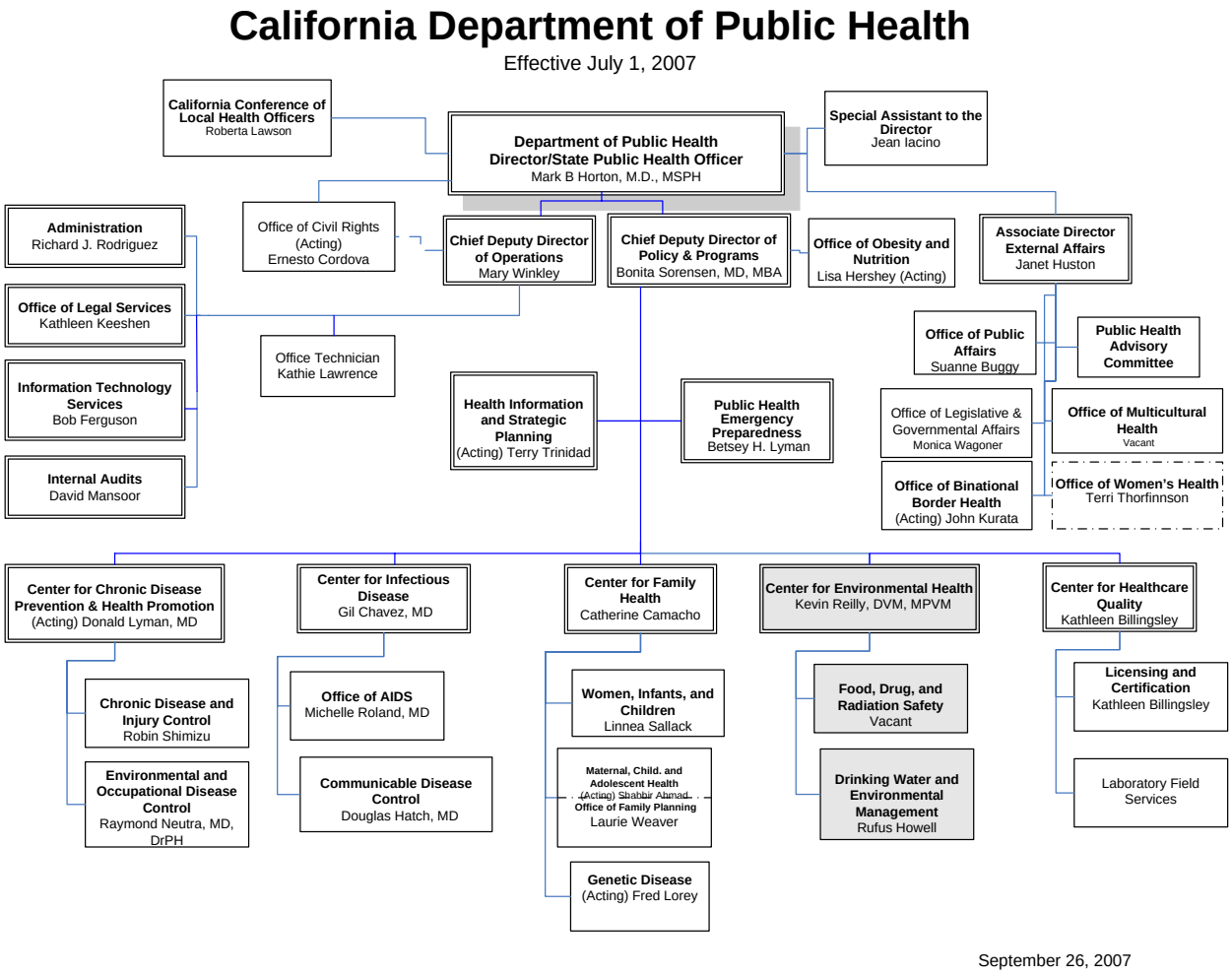


Figure 1: California Department of Public Health Organization Chart

The reorganization was designed to "streamline management of complex program components along functional lines"[2], among other benefits. The proposed EOL system supports this alignment by providing a common platform for the programs' licensing-

[2] California Senate Bill 162.

related functions. The five participating programs each fall within the grey shaded boxes in Figure 1. (Specific program organization charts are provided in Appendix E.)

3.1.2 Current Systems

The five program areas are very diverse and are governed by different state regulations and federal laws, yet they exhibit similarities within their **common functions** that make a shared licensing and state certification solution attractive to consider. The **common functions** of these programs are:

- Application/approval process
- Inspection or proficiency testing (including scheduling)
- Renewal
- Inquiry/lookup
- Maintenance of historical information (including education tracking where applicable)
- Complaint investigation
- Billing
- Enforcement

Other functions of some of the programs are not addressed by these common functions. Examples include public education, training delivery, time capture, etc.

Today, the common functions are supported by a mixture of technological platforms. Many of these platforms have become outdated and are difficult to maintain, supported by only a small number of staff, or reliant on dwindling skill sets due to retirements and obsolescence of technology. In fact, some systems now have no skilled staff remaining to support the system. In addition, numerous stand-alone MS Access and MS Excel systems are created as work-around quick-fix solutions.

Table 1 lists many of the information technology systems in use currently by the five participating programs.

Table 1: Current Systems

Program	System	Technology Used	Application / Approval	Inspection or Proficiency Testing	Renewal	Inquiry / Look up	Maintain Historical Information	Complaint Investigation	Billing	Enforcement
Food & Drug Program	Licensing System	MS Access on CDPH Server	X		X	X	X		X	
	Food Inspection Activity Tracking	Clipper on CDPH Server		X		X	X			X
	Drug and Device	MS Access on CDPH Server		X		X	X	X		X
	Exemptee	MS Access on CDPH Server	X	X	X	X	X	X	X	X
	Export	MS Access on CDPH Server	X			X	X			
	Complaint	MS Access on CDPH Server		X			X	X		X
Radiation Safety Program	Health Application Licensing (HAL) System	Natural and COBOL, with an ADABAS database management system (DBMS)	X	X	X	X	X	X	X	X
	California Mammography Information System (CAMIS)	MS Access 2003	X	X	X	X	X	X	X	X
	RAM2000	MS Access 2003	X	X	X	X	X	X	X	X
	MAIL2000	MS Access 2003	X	X	X	X	X	X	X	X
	5010 Tracking Database	MS Access 2003						X	X	X
	NOV Tracking Database	MS Access 2003						X	X	X
	Radiologic Technician Schools Database	MS Access 2003	X	X	X	X	X	X	X	X

Program	System	Technology Used	Application / Approval	Inspection or Proficiency Testing	Renewal	Inquiry / Look up	Maintain Historical Information	Complaint Investigation	Billing	Enforcement
	Low Level Radioactive Waste Tracking System (LLRWTS)	MS Access on CDPH Server	X			X	X			X
	Generally Licensed Devices	MS Access on CDPH Server	X			X	X			X
	Various Tools	MS Excel	X	X	X	X	X	X	X	X
Drinking Water Operator Certification	Operator Certification Database (for Water Treatment Operators)	FileMaker DB on LAN	X	X	X	X	X	X		X
	Operator Certification Database (for Water Distribution Operators)	FileMaker DB on LAN	X	X	X	X	X	X		X
	Deposits to CDPH Accounting	MS Excel	X		X				X	
Safe Drinking Water Systems	Permits Inspections, Compliance Monitoring & Enforcement (PICME)	MF-Focus on DTS IBM Mainframe	X	X		X	X	X	X	X
	Permits Tracking	FileMaker (on PC)	X	X		X	X			X
	Permits Tracking	MS Excel (Netware server on LAN)	X	X		X	X			X
	Check Tracking	MS Excel (Netware server on LAN)				X	X		X	
	Deposit Transmittal	MS Excel (Netware server on LAN)				X	X		X	
	Payment Posting	MS Excel (Netware server on LAN)				X	X		X	
	Past Due Notices	MS Excel (Netware server on LAN)				X	X		X	
	Collection Tracking	MS Excel (Netware server on LAN)				X	X		X	

Program	System	Technology Used	Application / Approval	Inspection or Proficiency Testing	Renewal	Inquiry / Look up	Maintain Historical Information	Complaint Investigation	Billing	Enforcement
	Rebate Calculations	MS Excel (Netware server on LAN)				X	X		X	
	Hourly Cost Rate	MS Excel (Netware server on LAN)				X	X		X	
	Permit Fees	MS Excel (Netware server on LAN)				X	X		X	
	Field Citation Payments	MS Excel (Netware server on LAN)				X	X		X	
	Reports	MS Excel and MS Word				X	X		X	
Medical Waste Management Program	FileMaker Pro	FileMaker DB on LAN	X	X	X	X	X	X	X	X

The following sections describe the five participating CDPH programs and the current issues impairing their ability to adequately protect Californians' public health and safety. Process flow diagrams for each program (approximately 50 pages in total) are provided in Appendix D.

3.1.3 Food and Drug Program

Program Background

The Food and Drug Program, through the Food and Drug Branch (FDB), licenses and regulates food manufacturers, retail water facilities, bottled water facilities, drug manufacturers, medical device manufacturers, and home medical device retailers by:

- Assuring that foods, drugs, and medical devices, and certain other consumer products are safe and not adulterated, misbranded, or falsely advertised.
- Ensuring drugs and medical devices are effective.
- Enforcing laws related to food, drug, and medical device manufacturing through licensing and inspections, and through effective industry and consumer education.
- Providing education to businesses to understand the public health basis for regulatory requirements and encouraging businesses to voluntarily correct deficiencies.

- Uniformly enforcing regulatory requirements to prevent unfair competition.

Applications are received annually from approximately:

- 5,000 medical device manufacturers and retailers;
- 600 drug manufacturers
- 1,200 bottled water facilities, haulers, distributors and vendors
- 5,000 food manufacturers
- over 18,000 food and drug exporters.

Governing Legislation

The Food and Drug Branch's responsibilities and authorities are established in Division 104 of the California Health and Safety Code (HSC). HSC Section 106500 establishes the authority of Food and Drug Branch investigators as peace officers, and authorizes them to enforce the provisions of the Health and Safety Code. The following Health and Safety Code sections provide specific licensing and registration authority to FDB:

- California Health and Safety Code, Sections 110460 et seq. – Processed Food Manufacturer and Warehouser Registration.
- California Health and Safety Code, Sections 111070 et. seq. – Bottled and Vended Water Licensing.
- California Health and Safety Code, Sections 110810 et. seq. – Organic Processed Product Registration.
- California Health and Safety Code, Sections 112150 et. seq. – Shellfish Certificates.
- California Health and Safety Code, Sections 112350 et. seq. – Cold Storage Licensing.
- California Health and Safety Code, Sections 112500 et. seq. – Frozen Food Locker Licensing.
- California Health and Safety Code, Sections 112650 et. seq. – Cannery Licensing.
- California Health and Safety Code, Sections 112875 et. seq. – Olive Oil Licensing.
- California Health and Safety Code, Sections 113025 et. seq. – Pet Food Licensing.
- California Health and Safety Code, Sections 111615 et. seq. – Drug and Medical Device Manufacturer Licensing.
- California Health and Safety Code, Sections 111656 et. seq. – Home Medical Device Retailer Facility Licensing.

- California Health and Safety Code, Sections 111656.14 et. seq. – Home Medical Device Retailer Exemptee Licensing.
- California Health and Safety Code, Sections 111795 et. seq. – Cosmetic Manufacturer Voluntary Registration.

Major Processes:

- ***License New Facilities:*** This process involves receipt and processing of a paper-based application and fee to license over 6,900 new food processing, drug and medical device manufacturing, and home medical device retail facilities annually. This process is supported by an MS Access (Microsoft Access) Licensing Database.
- ***Renew Facilities:*** This process involves licensee notification and receipt and processing of paper-based application and fee to renew over 13,000 food processing, drug and medical device manufacturing, and home medical device retail facilities annually. This process is supported by an MS Access Licensing Database.
- ***Inspect Facilities:*** This process involves approximately 7,000 inspections annually, which are triggered by a high relative risk factor or a volatile history. Inspections are scheduled within an MS Access Licensing Database.
- ***Process Complaint Against Facilities:*** This process involves the investigative steps and potential enforcement taken when a complaint against a food processing, drug and medical device manufacturing, or home medical device retail facility is made. This process is supported by an MS Access Licensing Database.
- ***Process Food Reinspection Fees:*** This process generates a payment letter for a food reinspection fee.
- ***Certify Products for Export:*** This process involves the receipt and processing of approximately 8,000 paper-based applications and fees annually to certify a food, drug, medical device, or cosmetic for export to another state or county. Data is entered into an MS Access Export database.

Current Observations:

The following observations are impairing FDB's ability to protect health and safety:

Californians' health and safety are at risk because regulators may not have access to data when needed

Immediate access to information on entities regulated by the Food and Drug Branch is vitally important when outbreaks and disease are linked to products from these firms. The ability to stop the distribution of contaminated foods, drugs or medical devices as rapidly as possible, and to reach out to the community with specific information to prevent exposures will prevent sickness, suffering and even death. Ready access to good information means effective public health protection. FDB lacks a comprehensive automated licensing and tracking system. The current set of systems uses antiquated

technology for core regulatory functions such as storage and retrieval of licensees' data. These systems have been repeatedly "band-aided," have failed several times, and are in danger of collapse.

For example, there have been instances where the MS Access database used for licensing has not properly pulled and sent renewal notices to firms, and as a result these regulated firms have incurred late payment penalties for not promptly renewing their licenses. FDB has also had experienced data loss from the licensing system, which has caused FDB to lose track completely of an applicant for licensure, leading to significant delays in inspection and enforcement. A major risk is that the next failure could have even worse consequences.

Californians' health is at elevated risk due to complete lack of technical support

The primary database for food inspection activity tracking is not documented or supported and is in disrepair. Inspections data has been lost by the system on several occasions. This database was developed in "Clipper," a long-outdated technology popular in the early 1990s for some data capture and reporting purposes. The homegrown system was developed by a non-IT-trained individual who has since retired. There is currently *no* remaining technical support staff for this critical system – this is a significant direct threat to food safety for all Californians. In multiple cases, staff has entered inspection activity data, closed the database, and upon reopening the database, the data is not present. This has placed the state at high risk due to the criticality of the food inspection function for the safety of all Californians.

High-volume functions are all handled through manual processes and paper files, creating delays and increasing State costs by $300,000 every year

Processing applications, preparing renewals, and related functions are all core, high-volume functions of FDB's program. These are all handled through manual processes and paper files. Current systems do not support online completion of applications, e-mail of renewal and late notices, and other high-volume functions. Current systems do not support the workflow of the program.

FDB calculates that program staff costs of about $300,000 for manual processing of applications could be redirected toward health and safety functions, by moving administrative processes onto electronic methods.

The state unnecessarily limits the regulated entities' available payment options, delaying payments and issuance of licenses

Since licenses are not issued until appropriate fees are paid, any delay in the payment process necessarily delays Californians' access to the medications or foods being licensed. FDB requires all payments to be in check or money order form, limiting customers' options, due solely to the state's own processing limitations. Reasonable customer expectations – based on the prevalence of modern payment methods in virtually every aspect of today's society – are not fulfilled. This is a compound problem that increases the state's workload even while it limits customers' options and fails to meet even basic modern expectations. As a result of the system limitation, a significant manual cash management process exists whereby payments are received; associated

to the proper program's applicant or licensee; and manually logged, batched, and sent to CDPH Accounting for deposit. Standard accounts-receivable functionality does not exist, so that when checks are received for an incorrect amount (for which the check is returned) or are dishonored due to non-sufficient funds, this results in additional work steps to resolve and obtain proper payment, requiring program staff to conduct multiple contacts to clarify data with the applicant. To summarize:

- Fees billed are often not correct due to various system limitations
- Payments received are often not correct
- Delays and back-and-forth contacts are created
- Reasonable customer expectations (which could easily be met) are left unmet
- Californians' access to life-saving medications and foods is delayed accordingly.

An estimated $14.3 million per year is collected by the FDB via checks and money orders, and handled by manual processes. (When all five programs are combined, the figure totals an estimated $49.9 million per year in check/money order payments handled by manual processes, with no other payment options available to customers.) This is an efficiency problem, compounded by poor customer service to the regulated community, and results in increased risk to the public.

3.1.4 Radiation Safety Program

Program Background

The Radiation Safety Program, conducted by the Radiologic Health Branch (RHB), currently operates under the Division of Food, Drug, and Radiation Safety (DFDRS), located within the Center for Environmental Health. RHB enforces radiation control laws and regulations designed to protect the public, radiation workers, and the environment through legislation as defined in the California Health and Safety Code (HSC) sections 106965 through 115295. RHB collects approximately $21 million per year in fees and is chartered to conduct licensing, enforcement, and billing activities for four major types of regulated entities:

- Radiation Machines: This program addresses the registration and monitoring of an estimated 78,000 medical (e.g., X-ray machines, mammography machines) and non-medical (e.g., baggage scanners) radiation machines housed within an estimated 35,000 facilities. This includes 758 medical facilities that operate mammography machines; 733 of which are accredited for Federal Certification under the Mammography Quality Standards Act (MQSA).
- Radiation Machine Operators: This program addresses the certification and monitoring of 83,000 physicians, technologists, and technicians who operate radiation machines.
- Radiologic Technology Schools: This program addresses the certification and monitoring of 96 radiologic technology schools and an estimated 1,000 affiliated clinical sites that offer courses and training required for individuals to be certified in operating radiation machines.

- Radioactive Materials: This program addresses the licensing and monitoring of facilities that use or possess radioactive materials, as well as environmental evaluations to ensure radiation safety. This includes 2,100 facilities that handle radioactive materials and 50,000 generally licensed devices (GLD) that use radioactive materials.

In addition to ensuring the enforcement of state regulations for the radiation programs, RHB also serves as a contractor to the U.S. Food and Drug Administration (FDA), under the MQSA, and is federally-approved as California's Agreement State representative for the U.S. Nuclear Regulatory Commission (NRC) Agreement State program under the federal Atomic Energy Act of 1954, as amended.

Radiation Safety is administered by the Radiologic Health Branch through its four sections as follows:

Registration and Certification

The Registration and Certification section manages the registration of approximately 35,000 facilities in the State of California that house over 78,000 registered radiation machines. This encompasses a variety of radiation machine types including mammography machines, oncology (cancer) X-ray machines, dental X-ray machines, fluoroscopy machines, computerized tomography (CT) scanners, linear accelerators used for computer chip manufacturing, and baggage scanners. In addition, the Registration and Certification section certifies:

- approximately 83,000 physicians, technologists, and technicians who operate radiation machines.
- 96 radiologic technology schools.
- 1,000 clinical sites that provide radiation machine coursework.

By July of 2008, certification will include industrial radiation machine operators.

The Registration and Certification section also performs enforcement functions for radiologic technology schools, including on-site audits and inspections. RHB's Inspection, Compliance, and Enforcement (ICE) sections perform these activities for the radiation machine, radiation machine operators, and radioactive materials programs.

Licensing

The Radioactive Materials Licensing section licenses approximately 2,100 facilities and registers approximately 50,000 GLDs that use radioactive materials for a broad range of applications.

This section receives and processes approximately 150 initial radioactive materials-related applications annually and approximately 2,500 radioactive materials-related addenda and renewals annually; performs approximately 2,300 evaluations for radiation safety annually; maintains a registry of 340 active devices manufactured in California for medical and industrial uses; monitors approximately 15 decommissioning activities annually; and monitors approximately 133 off-site environmental radiation and activities around nuclear power plants and other major radiation facilities annually.

Inspections, Compliance, and Enforcement

Inspections, Compliance, and Enforcement (ICE) is comprised of two sections: one section monitors 31,000 radiation machine facilities, over 78,000 radiation machines, and approximately 83,000 operators; the other monitors approximately 2,100 radioactive material licensees. In addition, RHB contracts with the Los Angeles County Department of Public Health and San Diego County Department of Environmental Health to perform 135 and 160 inspection, compliance, and enforcement activities respectively.

This section is responsible for performing approximately an estimated 10,000 annual inspections based on a defined schedule, as well as ad hoc inspections and audits. In addition, ICE is responsible for activities related to performing approximately 200 to 250 investigations annually that may result from allegations, complaints, or incidents; identifying violations and imposing enforcement actions, as needed; and responding to incidents and emergencies.

Financial Operation and Analysis

The Financial Operations and Analysis section is responsible for managing all incoming mail, cashiering, and billing activities for all RHB programs. In addition, Financial Operations and Analysis provides significant data entry support to the Radioactive Materials Licensing and ICE sections. Databases and spreadsheets are used to track incoming and outgoing correspondences, notice of violations related to financial default of payment, financial surety information, licensing data, staff assignments, and inspection data.

Governing Legislation

RHB is governed by a variety of state and federal legislation and regulations as follows:

- California Health and Safety Code (HSC) sections 114960 et seq. governs the effective regulation of sources of ionizing radiation for the protection of the occupational and public health and safety.
- HSC 106965 – 107111, & 114840 – 114896 (Radiologic Technology Act) establishes standards of education, training, and experience for persons who use X-rays on human beings and to prescribe means for assuring that these standards are met.
- HSC 107150 – 107175 (Nuclear Medicine Technology) governs the standards for and qualification of nuclear medicine technology.
- Federal Atomic Energy Act (AEA) of 1954 governs civilian and military uses of nuclear materials.
- California Code of Regulations (CCR) Title 17, California Mammography Quality Assurance Act (MQAA) of 1992, and the federal Mammography Quality Standards Act (MQSA) governs the registration and inspection of mammography machines.
- CCR Title 17, Division 1, Chapter 5, Subchapters 4.0 (Radiation) governs the

registration of sources of radiation and licensing of radioactive materials, 4.5 (Radiologic Technology) governs the training and certification of radiologic technologists, and 4.6 (Nuclear Medicine Technology) governs certification of nuclear medicine technologists.

Major Processes:

The following provides an overview of the major processes performed by each of the four sections within RHB.

- ***Register Radiation Machines:*** This process involves the receipt and processing of an estimated 78,000 paper-based applications to register new radiation machines, amend existing registration data, and renew machine registrations.
- ***Certify Radiation Machine Operators*****:** This process involves the receipt and processing of about 83,000 paper-based applications annually from individuals who will operate radiation machines; reviewing and validating approximately 6,100 examination results annually; and issuing certificates.
- ***Certify Radiation Technology Physicists*****:** This process involves the receipt and processing of 35-40 new and approximately 90 annual renewal paper-based applications from individuals certified by a national body, or as demonstrated through continuing education, as possessing the expertise to calibrate radiation machines.
- ***Certify Mammography Facilities and Machines, and Authorize Linear Accelerators for Breast Cancer Treatment*****:** This process involves the receipt and processing of paper-based applications from 420 facilities (new, renewal, and amended) with mammography machines who are seeking State certification (30 more each year) annually. Use of any of these machines for patient care without this authorization could expose patients, healthcare workers, and the public to dangerous amounts of radiation. In addition, breast cancer tumors could go undertreated.
- ***Reconcile Report of Assembly:*** This process involves the receipt and processing of paper-based report of assembly forms received from vendors who install or make changes to the radiation machines manufactured, validating existing information, and determining if radiation machine registration changes must occur.
- ***Certify School/Clinical Site:*** This process involves the receipt and processing of paper-based applications to certify 96 radiologic technology schools and an estimated 1,000 associated clinical sites annually.
- ***Perform Radiologic Technology School Inspection:*** As part of the certification process, radiologic technology schools and their respective clinical sites must undergo an inspection within their first probationary year, as well as periodic inspections thereafter. This process describes the steps associated with the approximately 144 radiologic technology school inspections conducted annually.
- ***Issue School Billing Notices:*** Since RHB's core systems do not maintain radiologic technology schools data, billing notices must be manually developed.

This process describes the steps associated with issuing annual billing notices for approximately 96 radiologic technology schools.

- ***Process Returned Mail:*** This process involves reviewing and processing approximately 1,600 returned pieces of mail received annually which has resulted from an incorrect address in RHB's core systems.
- ***Perform Radioactive Materials Licensing Action:*** This process involves the receipt and processing of 5,500 paper-based applications for new, renewal, amended, and terminated radioactive materials licenses.
- ***Perform Radiological Survey:*** This process involves RHB's activities related to receiving a request for a radioactive site survey; assigning staff; and preparing for, conducting, and documenting the survey results.
- ***Perform Radiological Document Review:*** This process involves the processing approximately 9,625 annual requests for a radioactive materials-related document review, assigning staff, and performing the assessment.
- ***Perform Radiation Machine Inspection:*** This process involves identifying radiation machine (non-mammography) inspections required, assigning staff, preparing for and conducting an estimated 7,610 annual inspections, and documenting results.
- ***Perform Mammography Machine Inspection (State):*** This process involves identifying 1,427 annual mammography machine inspections required by the State, assigning staff, preparing for and conducting the inspection, and documenting results.
- ***Perform Mammography Machine Inspection (MQSA):*** This process involves identifying 1,203 annual MQSA inspections required, assigning staff, preparing for and conducting the inspection, documenting results, and submitting information to the FDA.
- ***Perform Radioactive Materials Inspection:*** This process involves identifying radioactive materials inspections required, preparing for and conducting an estimated 550 annual inspections, and documenting results.
- ***Perform Radioactive Materials Investigation:*** As with investigations related to radiation machines, radioactive materials investigations can also be initiated from a variety of internal and external sources. This process includes the steps to initiate, conduct, report on, and close an investigation.
- ***Perform Incident Response:*** This process includes responding to incidents annually related to radioactive materials and radiation machines.
- ***Track Radioactive Materials Correspondence:*** This process involves tracking all correspondences received from and sent to radioactive materials applicants and licenses.
- ***Issue Radioactive Materials Billing Notices:*** Since the Health Application Licensing (HAL) System does not maintain data on radioactive materials, billing notices must be manually developed. This process involves the issuance of

radioactive materials billing notices.

- ***Perform Cashiering:*** This process involves receiving approximately 59,000 annual payments from RHB's customers, recording payments into the respective systems, and addressing overpayments, underpayments, and dishonored checks.
- ***Reconcile Deposits:*** This process involves reconciling approximately 1,400 annual RHB-prepared cash deposits to the State's accounting system.

Current Observations:

The following observations affect the ability of RHB to provide the safety required by its mission:

Thousands of radiation machines are overdue for inspection, placing California patients and healthcare workers at risk for exposure to dangerous radiation.

Public health and safety concerns are identified during the inspection process. Delayed inspections results in more exposure of healthcare workers or the general public to unsafe situations or practices that will be identified and remedied with an inspection. The state has become overdue on the inspection timelines for certain types of radiation machines, in violation of required timelines. There is currently a backlog in excess of 4,000 radiation machines and facilities overdue for inspections, in some cases more than a year behind, placing thousands of California patients and healthcare workers at elevated risk for exposure to dangerous radiation. This exposure is growing every year, as backlogs increase across the state.

RHB's safety mission is impaired due to lack of systems for core regulatory functions

The Radiologic Technology School Program, Radioactive Materials Licensing Program, Inspection Compliance and Enforcement Program are not supported by any workflow system, including the HAL system, resulting in a proliferation of ad hoc single-user and non-integrated databases and spreadsheets. The HAL system serves as the repository for license and billing data related to radiation machines. In the absence of a core system such as HAL, these programs rely on the use of often incomplete and inconsistently used spreadsheets. These spreadsheets track critical programmatic data including registration and certification applications data, radiation machine license exemptions, mammography facilities and approval letters, fee calculation, calculation of radioactive material isotope allowances. Having data in many different systems results in regulators' time being spent on data issues, instead of their core regulatory mission of protecting Californians' health and safety.

Radioactive incident/emergency responses may be impeded

Timely responses to radiation emergencies is vital to the public's safety. For example, if a spill of potentially radioactive materials occurs on a California highway, RHB is required to dispatch staff to the site to determine if the spill is radioactive, determine how best to protect the public, and oversee cleanup. However, staff assignment, location identification, documentation and reporting are manual activities. Management

must manually determine which staff to assign, attempt to determine the exact location of the occurrence and cross-reference against staff's geographic location. This could mean the closest and best officials are not the ones dispatched. This inefficiency and delay in processing can cost lives due to inadequate response to a radiation emergency.

Regulated entities are forced to use paper submission methods for applications; staff manually process paper-based submissions

For all entities regulated by RHB, customer transactions (e.g., application, renewal, payment) are paper based. Staff manually sort submissions, conduct follow-up contacts, create licenses and certificates, track and file numerous and complex correspondences, and research historic files. This results in regulators' time being even further spent on administrative tasks, instead of their core regulatory mission of protecting Californians' health and safety.

State revenue is lost due to miscalculated fees, overdue payments and non-payments

RHB collects approximately $21 million per year in fees, even though its current system does not adequately support billing requirements. These system challenges consist of miscalculation of fees, failure to generate multiple billing notices and delinquent billing payments. Billing notices are automatically created by the HAL system, and currently, the system is unable to accommodate the calculation of all types of fees. This leads to incorrect billing notices being mailed and an estimated $450,000 loss in revenue for certain license types (e.g. physicians, multiple limited permit holders). In some cases RHB is not aware of the incorrect billing until after the licensee calls or payments are received. Also, the current system does not enable the generation of all required multiple billing notices, such as delinquent billing notices or duplicate billing notices. For example, if RHB does not receive a payment from a facility or a licensee, the system will not generate subsequent billing notices. This results in lost revenue of approximately $1,000,000 in delinquent billing. In addition, limitations in the HAL system prohibit RHB from issuing licenses and renewal notices for radiation machines and licensees in a timely manner. Several times during the year, renewal notices are not generated by HAL or not distributed to the licensees as required, resulting in loss of timely payments and the need for RHB to create manual workarounds. These manual workarounds result in extra work and the potential for entering the incorrect fee amount. Further effects of the lack of standard accounts-receivable functionality include:

- there are an unknown number of licensees not paying bills.
- over 30 percent of payments received by RHB are received past the due date.

A fully detailed study of the underlying system-based errors causing these problems has not been conducted or funded.

Staffing (Program Technician and Management Services Technician positions) to support the fee collection, application processing and license/registration/certification processes within the Radiologic Health and Food and Drug Branches have been justified in several approved Budget Change Proposals in recent years (PS-08 in FY 06-

07; PS-21 and PS-22 in FY 07-08; and EH-06 in the FY 08-09 Governor's Proposed Budget).

When these billing problems and payment processing problems occur, preventing a licensee from providing health care, Californians suffer from reduced access to healthcare.

The state unnecessarily limits the regulated entities' available payment options, delaying payments and issuance of licenses, reducing Californians' access to healthcare

Since licenses are not issued until appropriate fees are paid, any delay in the payment process necessarily delays Californians' access to health care. However, RHB requires all payments to be in check or money order form, limiting customers' options, due solely to the state's own processing limitations. Reasonable customer expectations – based on the prevalence of modern payment methods in virtually every aspect of today's society – are not fulfilled. This is a compound problem that increases the state's workload and delays public health outcomes even while it limits customers' options and fails to meet even basic modern expectations. As a result of the system limitation, a significant manual cash management process exists whereby payments are received; associated to the proper program's applicant or licensee; and manually logged, batched, and sent to CDPH Accounting for deposit. Standard accounts-receivable functionality does not exist, so that when checks are received for an incorrect amount (for which the check is returned) or are dishonored due to non-sufficient funds, this results in additional work steps to resolve and obtain proper payment, requiring program staff to conduct multiple contacts to clarify data with the applicant. To summarize:

- Fees billed are often not correct due to various system limitations
- Payments received are often not correct
- Delays and back-and-forth contacts are created
- Reasonable customer expectations (which could easily be met) are left unmet
- This delays the issuance of the license, and Californians' access to healthcare is reduced accordingly.

An estimated $21 million per year is processes this way, collected by RHB via checks and money orders, and handled by manual processes.

3.1.5 Drinking Water Operator Certification Program

Program Background

The Drinking Water Operator Certification Program (OCP) assures that drinking water treatment and distribution system operators have the required knowledge and experience to safely operate drinking water systems as required by the federal Safe Drinking Water Act (SDWA). There are nearly 30,000 water treatment and water distribution operators certified by the OCP, which is an increase of over 5,500 certified operators in three years (an increase of eight percent per year). To ensure the safety of the public water supply, certified operators:

- Ensure water treatment and distribution facilities are properly maintained.
- Drinking water is provided essential treatment such as filtration and disinfection.
- Ensure safe drinking water quality is maintained as it is conveyed to consumers through piping, reservoirs, and pumps.

Approximately 10,000 new applications are received each year, plus approximately 10,000 recertification applications. The operators must be recertified every three years.

Governing Legislation

The OCP is governed by state legislation as follows:

- California Health and Safety Code, Sections 106875-106910; Operator Certification Program: Water Treatment Plants and Water Distribution Systems.

Major Processes:

Certify Water Treatment and Water Distribution Operators: This process involves the receipt and processing of paper-based certification applications from drinking water systems treatment operators and drinking water distribution operators; reviewing and validating examination results, education contact hours; and issuing certificates.

- ***Perform Cashiering:*** This process involves receiving payments from OCP customers, recording payments into the respective system, and addressing overpayments, underpayments, and dishonored checks.
- ***Reconcile Deposits:*** This process involves reconciling OCP-prepared cash deposits to the State's accounting system.
- ***Water Operator Exam Application:*** This process involves the receipt and processing of paper-based examination applications from drinking water systems treatment operators and drinking water distribution operators; reviewing and validating education and contact hour requirements and issuing examination notices to applicants before the examination.
- ***Renew Water Treatment and Water Distribution Operator Certificates*****:** This process involves sending out certificate renewal notices, receipt and processing of paper-based renewal applications from drinking water systems treatment operators and drinking water distribution operators; reviewing and validating examination results, education contact hours; and issuing wallet card certificate renewals.
- ***Water Operator Certificate Enforcement:*** This process involves drinking water systems treatment operators and drinking water distribution operators who either fail to pay fees, fail to complete continued education requirements, or are subject to sanctions stemming from an incident at the request of the Field Office.

Current Observations:

The following observations affect the ability of OCP to accomplish its mission:

Certifications are delayed due to length of processing time

The submittals received by the OCP for water operator certification are entirely paper-based. The examination and certification applications include numerous documents and correspondences. Additional documents and correspondences associated with an application submittal or existing permit are received sporadically throughout the review and approval process. In addition, all certification change requests, address changes, name changes, and employer continuing education updates are submitted on paper. Paper-based processes have resulted in extensive manual processing steps and the inability to process all submittals received within the designated target timeframes (generally 10 days) due to:

- The multitude of steps related to receiving, opening, sorting, and distributing mail.
- Submitted forms are incomplete, or not completed correctly, and require OCP to either contact the customer or return the submittal. This can go back and forth several times.
- OCP staff must access multiple systems/sources to review and validate the data included in the submittal.
- Back-and-forth contacts with customers to resolve questions or inaccuracies in the paper application and/or payment amount.
- New errors in re-submitted documents, requiring additional follow-up contacts with customers.
- Delays due to the back-and-forth contacts, especially when the customer or State staff are out due to illness, vacation, etc.
- Misplaced and lost submittals and related documents.

When applications are not processed in a timely fashion, operators do not receive their certification. As a result, they cannot work, and Californians' access to safe water is diminished.

The state unnecessarily limits the available payment options, delaying payments and issuance of certifications, reducing Californians' access to safe drinking water

Since certifications are not issued until appropriate fees are paid, any delay in the payment process necessarily delays Californians' access to safe drinking water. However, OCP requires all payments to be in check or money order form, limiting customers' options, due solely to the state's own processing limitations. Reasonable customer expectations – based on the prevalence of modern payment methods in virtually every aspect of today's society – are not fulfilled. This is a compound problem that increases the state's workload and delays public health outcomes even while it limits customers' options and fails to meet even basic modern expectations. As a result of the system limitation, a significant manual cash management process exists whereby payments are received; associated to the proper program's applicant or licensee; and

manually logged, batched, and sent to CDPH Accounting for deposit. Standard accounts-receivable functionality does not exist, so that when checks are received for an incorrect amount (for which the check is returned) or are dishonored due to non-sufficient funds, this results in additional work steps to resolve and obtain proper payment, requiring program staff to conduct multiple contacts to clarify data with the applicant. To summarize:

- Fees billed are often not correct due to various system limitations
- Payments received are often not correct
- Delays and back-and-forth contacts are created
- Reasonable customer expectations (which could easily be met) are left unmet
- Californians' access to safe drinking water is diminished accordingly

This inefficient process is both unnecessary and increasingly unacceptable in view of simple online payment methods available today in nearly every aspect of life. An estimated $1.5 million per year is collected by OCP via checks and money orders, and handled by manual processes.

Single technical support resource puts state program at risk

OCP's FileMaker database system is the Department's tool to assure that drinking water system operators meet the legal requirements and have the necessary expertise to deliver safe drinking water to more than 35 million Californians. This system is supported by a single technical resource (person) with no backup staff. There is little technical documentation in place and few technical experts in the industry available to hire to replace the current technical resource should he suddenly become unavailable. When system issues occur, they cannot be addressed if the individual is out, or unavailable, which impacts OCP staff's ability to continue their regulatory oversight activities; they either have to cease certain activities altogether, or spend extra time and effort on workarounds until the system issue is resolved. This situation places Californians at risk by weakening California's oversight of its drinking water.

3.1.6 Safe Drinking Water Systems

Program Background

The Safe Drinking Water Systems program (SDWS) within the Division of Drinking Water and Environmental Management (DDWEM) provides direct oversight including the permitting, inspection, and enforcement of approximately 2,500 small water systems (those with less than 200 service connections) in 23 counties and delegates responsibility to local environmental health jurisdictions (also known as Local Primacy Agencies) for oversight of the small water systems in the remaining 35 counties. These water systems are billed annually and fees are collected by the program. The DWP is also allowed by statute to bill up to $1,000 of time spent on enforcement activities against the water system. This is currently invoiced manually. A billing and fee collection system to carry out these functions would enable the program to be more responsive to the water utilities and direct staff to other essential activities.

Governing Legislation

SDWS is governed by state and federal legislation as follows:

- California Health and Safety Code, Part 12: Drinking Water, Chapter 4: California Safe Drinking Water Act; Sections 116270 – 116751.
- California Health and Safety Code, Part 12: Drinking Water, Chapter 4.5: Safe Drinking Water State Revolving Fund Law of 1997; Sections 116760 – 116762.60.
- California Health and Safety Code, Part 12: Drinking Water, Chapter 5: Water Equipment and Control; Sections 116775 – 116880.
- California Health and Safety Code, Part 12: Drinking Water, Chapter 7: Water Supply; Sections 116975 – 117130.

Major Processes:

- ***Permit Water Treatment facilities***: This process involves the receipt and processing of paper-based permit applications from water systems facilities; reviewing inspection results and issuing permits.
- ***Perform Water Systems facilities Inspection:*** As part of the permit process, water systems facilities undergo initial permit inspections, as well as periodic inspections thereafter. This process describes the steps associated with a facilities inspection.
- ***Issue Water Systems Billing Notices:*** SDWS sends billing notices to both Large Water Systems (LWS) and Small Water Systems (SWS). This process describes the steps associated with issuing billing notices for all drinking water systems.
- ***Perform Cashiering:*** This process involves receiving approximately 4,677 annual payments from SDWS customers, recording payments into the respective system, and addressing overpayments, underpayments, and dishonored checks.
- ***Reconcile Deposits:*** This process involves reconciling SDWS prepared cash deposits to the State's accounting system.

Current Observations:

The following observations affect the drinking water safety of all Californians:

Drinking water safety is threatened by backlogs of inspections and renewals

The state currently has a backlog of over 2,000 inspections (two years' worth) and approximately 500 public water systems are waiting for renewals (nearly 8 months' worth). Notwithstanding CDPH's current practice of redirecting staff to prioritize highest-risk systems for renewal/inspection to minimize public health impact, the backlogs continue to grow. This means that the safety of drinking water is placed at additional unacceptable risk. Public water systems that are not currently permitted may not be fully complying with water system safety requirements, thereby resulting in potential health risk to consumers.

Californians' access to water is diminished by delays in processing

Paper-based processes have resulted in extensive manual processing steps and the inability to process all submittals received within the designated target timeframes (generally 30 days in statute) due to:

- The multitude of related to receiving, opening, sorting, and distributing mail.
- Submitted forms are incomplete or not completed correctly and require SDWS to either contact the customer or return the submittal. This can go back and forth several times.
- SDWS staff must access multiple systems to review and validate the data included in the submittal.
- Back-and-forth contacts with customers to resolve questions or inaccuracies in the paper application and/or payment amount.
- Handoff of the submittals between units because different units are required to review specific subsections of the submittal (e.g., review of water system permit applications).
- New errors in re-submitted documents, requiring additional follow-up contacts with customers.
- Delays due to the back-and-forth contacts, especially when the customer or State staff are out due to illness, vacation, etc.
- Misplaced and lost submittals and related documents.

The above steps combine to create a processing method that unnecessarily delays the issuance of permits to public water systems, for no reason other than the state's lack of an adequate processing system. In more than half of all instances, the state is not making the 30-day timeframe cited in the previous paragraph. These delays only further compound the backlog.

The state unnecessarily limits the public water systems' available payment options, delaying issuance of permits, reducing Californians' access to safe drinking water

Since permits are not issued until appropriate fees are paid, any delay in the payment process necessarily delays Californians' access to drinking water. However, SDWS requires all payments to be in check or money order form, limiting customers' options, due solely to the state's own processing limitations. Reasonable customer expectations – based on the prevalence of modern payment methods in virtually every aspect of today's society – are not fulfilled. This is a compound problem that increases the state's workload and delays public health outcomes even while it limits customers' options and fails to meet even basic modern expectations. As a result of the system limitation, a significant manual cash management process exists whereby payments are received; associated to the proper program's applicant or licensee; and manually logged, batched, and sent to CDPH Accounting for deposit. Standard accounts-receivable

functionality does not exist, so that when checks are received for an incorrect amount (for which the check is returned) or are dishonored due to non-sufficient funds, this results in additional work steps to resolve and obtain proper payment, requiring program staff to conduct multiple contacts to clarify data with the applicant. To summarize:

- Fees billed are often not correct due to various system limitations
- Payments received are often not correct
- Delays and back-and-forth contacts are created
- Reasonable customer expectations (which could easily be met) are left unmet
- Californians' access to safe drinking water is diminished accordingly

An estimated $11.2 million per year is processed this way, collected by SDWS via checks and money orders, and handled by manual processes.

Single technical support resource puts regulatory function at risk

The primary systems used by California drinking water regulators are based on an antiquated technology (Focus) supported by a single technical resource (person) with no backup. This is a high-risk situation, made even worse because there is little technical documentation in place and few technical experts in the industry available to hire to replace the current technical resource should he suddenly become unavailable. When system issues occur, they cannot be addressed if the technical resource is out or unavailable, which impacts SDWS staff's ability to fulfill their regulatory mission; they either have to cease certain business process activities altogether or spend extra time and effort on workarounds until the system issue is resolved. This situation puts the SDWS Program at significant risk for loss of data or worse system failure, and adds to the backlogs of inspections and renewals mentioned above, diminishing Californians' access to safe drinking water. The EOL system will replace the functionality of Focus, which poses this risk.

3.1.7 Medical Waste Management Program

Program Background

The Medical Waste Management Program (MWMP) protects the public and the environment from potential infectious exposure to disease-causing agents. The MWMP permits medical waste treatment facilities, transfer stations, and alternative technologies and registers medical waste generating health providers. Program staff inspects permitted facilities and investigates and takes enforcement action against facilities that are out of compliance with regulatory requirements. The MWMP regulates the generation, handling, storage, treatment, and disposal of medical waste by providing compliance oversight as dictated by the Medical Waste Management Act (California Health and Safety Code Sections 117600 - 18360). MWMP's primary activities consist of the following:

- Permits and inspects all medical waste off-site treatment facilities and medical waste transfer stations. The Department's MWMP is the local enforcement authority in 25 counties statewide, including Los Angeles County.

- Registers 18 different types of healthcare facilities that generate medical waste.
- Permits treatment and transport facilities that handle medical waste from off-site sources.
- Authorizes businesses that haul medical waste from generators, and provides exemptions for limited quantity hauling for smaller operators.
- Acts as the local enforcement agency in 27 local jurisdictions that elected to have the state implement the large quantity generator inspection program within their jurisdictions.
- Assists generators of medical waste in minimizing waste generation through training and facilitating implementation of its Hospital Pollution Prevention Program.

There are approximately 6,000 medical waste generators which consist of 5,000 small quantity generators, 750 Large Quantity Generators, 30 Common Storage Facilities, and 30 Small Quantity Generators with onsite treatment that need annual renewal. There are over 50 treatment and transport facilities, 95 businesses that haul medical waste from generators and approximately 750 limited quantity hauling exemptions for smaller operators.

Governing Legislation

- Medical Waste Management Act (MWMA) (California Health and Safety Code, Sections 117600 – 118360) governs the management of medical waste in all jurisdictions of the state.
- California Code of Regulations Title 22, Division 4 Environmental Health, Chapter 21 details Minimum Standards for Permitting Medical Waste Facilities.
- California Code of Regulations Title 8, Chapter 4 (Division of Industrial Safety), Sub-Chapter 7 (General Industry Safety Orders), Group 16 (Control of Hazardous Substances), Article 109 (Hazardous Substances and Processes) details Blood Borne Pathogen Standards.

Major Processes:

- ***Transfer Station/Off-Site Treatment Facility/Alternative Technology New Permit:*** This process includes application review, fee processing and facility inspection required to verify applicant sites meet permitting requirements.
- Alternative technologies device permitting requires more extensive testing to demonstrate device effectiveness.
- ***Transfer Station/Off-Site Treatment Facility/Alternative Technology Permit Renewal:*** This process includes permit renewal activities. Permit renewal occurs every five years.
- ***Complaints/Incidents Process:*** This process includes the recording and assignment of reported complaints and incidents to MWMP staff to investigate. The process is triggered by calls from the public or facility/landfill employees reporting a spill or unsafe illegal practice.

- ***Enforcement Process:*** An inspection or investigation resulting from a reported complaint or incident may result in an enforcement action. Enforcement actions involve the investigative inspection of sites out of compliance and the documentation of corrective actions required for sites in violation of the Medical Waste Act. An enforcement action may result in fines or penalties and subsequent administrative or court hearings.
- ***Waste Generation Facilities/Trauma Scene Practitioners New Registration Process:*** This process includes activities to register medical waste generators. Providers and practitioners detail their medical waste handling and disposal procedures.
- ***Waste Generation Facilities/Trauma Scene Practitioners Registration Renewal Process***: This process includes annual registration renewal activities.
- ***Authorize Waste Hauler Process:*** This process authorizes waste haulers to haul waste under authorized conditions. Available waste haulers are presented within a web published listing. Waste haulers self-report waste hauling activities.

Current Observations:

The following observations are impairing the ability of MWMP to effectively manage medical waste in California:

Public health and safety are at risk due to inspection delays

Many current processes require numerous manual steps and delays. For example, only manual processes are available to handle registration renewals and track facility compliance activities such as initial application, payment, and corrective actions. An impact of this is that there are presently 1,000 health care facilities awaiting renewal; these facilities are currently operating under temporary licensure pending their application processing. Without the appropriate timeliness of CDPH review due to processing delays, the public's heath is placed at risk.

The state unnecessarily limits the regulated entities' available payment options

MWMP requires all payments to be in check or money order form, limiting customers' options, due solely to the state's own processing limitations. Reasonable customer expectations – based on the prevalence of modern payment methods in virtually every aspect of today's society – are not fulfilled. This is a compound problem that increases the state's workload and delays public health outcomes even while it limits customers' options and fails to meet even basic modern expectations. As a result of the system limitation, a significant manual cash management process exists whereby payments are received; associated to the proper program's applicant or licensee; and manually logged, batched, and sent to CDPH Accounting for deposit. Standard accounts-receivable functionality does not exist, so that when checks are received for an incorrect amount (for which the check is returned) or are dishonored due to non-sufficient funds, this results in additional work steps to resolve and obtain proper payment, requiring program staff to conduct multiple contacts to clarify data with the applicant. To summarize:

- Fees billed are often not correct due to various system limitations
- Payments received are often not correct

- Delays and back-and-forth contacts are created
- Reasonable customer expectations (which could easily be met) are left unmet.

An estimated $2.0 million per year is processed this way, collected by the MWMP via approximately 2,166 checks and money orders, and handled by manual processes.

State revenue is likely being lost

Billing errors cause by the state's FileMaker Pro database are often discovered by staff. Due to the lack of a system to invoice correctly, and the manual processes used for identifying and correcting these mistakes, we can only speculate about the errors never noticed. An unknown amount of state revenue each year is never billed or received.

3.2 Business Objectives (Problem and Opportunity)

A modern, workflow-oriented, web-based, customer-friendly system to replace the current tangle of systems would offer substantial benefits to patients, the healthcare community, the general public, and CDPH – in short, benefits to all of California. Such a system would allow the State government to:

- Obtain needed information to support both incident/emergency responses and day-to-day regulatory needs
- Carry out its regulatory mission more efficiently and effectively
- Provide expected service levels to customers – primarily the regulated entities, as well as the general public and other governmental agencies
- Avoid unnecessary increases in program budget due to steadily declining efficiencies and future increased IT support needs for antiquated and failing systems.

Table 2 summarizes the business problems identified in section 3.2, along with causes, effects, and the associated business objectives.

Note: Magnitude information (numbers of laboratories, schools, etc.) are provided above, in the program descriptions. Table 2 addresses the cross-program needs, thus the specific metrics are omitted in this table. For example, it could be awkward or misleading to count the number of regulated entities by adding the number of radiation machines to the number of medical waste haulers, etc.

Table 2: Business Objectives

Problem	
Problem 1: The public health and safety of Californians are at risk because the current system environment is highly fragmented within each program.	
Causes and Effects	**Business Objectives**
Causes: • Systems are built on outdated technology and have begun to fail • Staff lack a single repository that accommodates all of its programs and license types • Many current systems are "point" solutions that fail to address the full workflow and lifecycle of regulated entities • Some program data is not captured in any automated systems **Effects:** • Incident/emergency response is impaired because geographic location factors, assignment of appropriate staff, and determining potential impact on local area is performed manually and without modern GIS tools • Staff has created a variety of non-integrated databases and spreadsheets, resulting in duplicate data entry and redundancy • Program inspectors are unable to obtain data for routine functions • Inconsistent technical support	1.0 **Improve CDPH's ability to protect public health and safety by instituting a standardized and full-featured platform for all licensing and licensing-related functions.** 1.1 Maintain all programmatic data related to regulated entities 1.2 Link current processes together (license renewal, enforcement actions/ correspondence/inquiries) and record all data connected with a single site/licensee 1.3 Support business process workflow, not simply recording of data 1.4 Implement a system with sufficient data storage capabilities to allow retention and retrieval of all appropriate data 1.5 Provide common tools for data retrieval, analysis, and reporting 1.6 Implement a system that is accessible by all staff that require access

Business Objective 1 is supported by the following Functional Requirements which are listed in Section 3.3: Business Functional Requirements: L-001, L-002, L-004, L-005, L-006, L-007, L-012, L-014, E-001, E-004, E-005, E-006, E-007, E-008, E-011, E-012, B-001, B-004, B-009, G-001, G-004, G-022.

Problem	
Problem 2: Staff's ability to protect the public and serve customers' needs for modern processing methods are impacted by current non-web-based systems.	
Causes and Effects	**Business Objectives**
Causes: • Current system does not accept electronic submission of applications and other documents • Current system does not provide electronic payment options • No public access is provided for non-confidential licensee information **Effects:** • Customers are burdened with state's paper-based methods • Staff have difficulty in meeting standard timeframes related to data requests and processing steps • About $49.9 million per year is collected via check and money order • Customers do not have access to their licensing and billing data, resulting in time spent by staff to address questions • Customers receive no automated notifications of impending record requirements such as renewal • Additional time is spent by staff, to address by phone, fax or mail, questions received from the public	2.0 **Provide a modern means of customer communi-cations for regulatory functions, including online interactions with licensees.** 2.1 Provide customers with on-line capability to electronically apply, make payments, inquire, and submit additional information and documents 2.2 Provide the public access to non-confidential licensing data via the web

Business Objective 2 is supported by the following Functional Requirements which are listed in Section 3.3: Business Functional Requirements: L-001, L-002, L-003, L-004, L-005, L-006, L-007, L-008, L-009, L-011, L-012, L-015, E-001, E-011, B-001, B-005, B-006, B-008, B-009, B-010, B-016, B-017, G-002, G-005, G-007, G-008, G-010, G-018, G-020, G-023, G-024, G-032, I-001, S-004.

Problem	
Problem 3: Redirection of skilled program staff time away from regulatory work toward system issues, thereby limiting programs' effectiveness.	
Causes and Effects	**Business Objectives**
Causes: • All licensing, enforcement, and billing data information regarding a licensee is not shared across programmatic systems • Current systems provide no ability to process fees electronically, and do not reconcile billed amounts **Effects:** • Public health is placed at risk because program staff are re-directing time to develop and maintain databases and spreadsheets • Working records used by staff are retrieved from paper files • Staff are reliant on emails, phone calls, and physical visits to various colleagues to share customer information • Files are stacked on office countertops and are lost, requiring stakeholder resubmission • Staff must manually tally items and calculate the related bill • Staff manually compile data to respond to customer ad hoc requests	3.0 **Provide a modern means of internal workflow for regulatory functions.** 3.1 Provide customers with on-line capability to electronically apply, make payments, inquire, and submit additional information and documents 3.2 Automate record management across all licensing programs from the creation of a record, tracking and reporting, through record archival and storage 3.3 Support program-specific financial requirements for billing, refund processing, payments processing, and revenue reconciliation; work with CDPH accounting appropriately 3.4 Enable electronic payments 3.5 Eliminate duplicate data entry into multiple systems 3.6 Eliminate manual/paper processing and reduce associated costs

Business Objective 3 is supported by the following Functional Requirements which are listed in Section 3.3: Business Functional Requirements: L-001, L-002, L-003, L-004, L-005, L-009, L-010, L-011, L-012, L-013, L-016, L-017, E-001, E-002, E-003, E-004, E-005, E-006, E-007, E-008, E-009, E-010, E-012, B-001, B-002, B-003, B-004, B-005, B-006, B-007, B-010, B-011, B-012, B-013, B-014, B-015, B-018, G-001, G-003, G-004, G-006, G-009, G-010, G-011, G-012, G-013, G-014, G-017, G-019, G-020, G-021, G-022, G-023, G-024, G-025, G-026, G-027, G-032, I-002, S-003.

<table>
<tr><th colspan="2">Problem</th></tr>
<tr><td colspan="2">Problem 4: Legislative and regulatory mandates and policy directives are difficult to meet with current systems.</td></tr>
<tr><th>Causes and Effects</th><th>Business Objectives</th></tr>
<tr><td>Causes:
Current systems do not have flexibility to support programs in addressing new regulatory and legislative requirements
Public health needs (and the statutes and regulations that support those needs) are continuously evolving and changing
Programs serve an increasing number of customers
Current system environment is not scalable or flexible, making it difficult to modify existing systems to accommodate required changes
Staff lacks access to data that could demonstrate accountability and help support planning, analysis, policy definition, and decision-making
Effects:
New requirements are not being adequately addressed in a timely manner
Delayed processing of applications, renewals, and inspections within required timeframes
Licensees not paying their fees on time – or at all
Inaccurate billing according to regulations</td><td>4.0 Provide flexibility to adapt to a changing statutory, regulatory, and policy environment.

4.1 Provide a system that can be adjusted as needed, based on new business rules, and complies with CDPH, DTS, and State Administrative Manual standards</td></tr>
</table>

Business Objective 4 is supported by the following Functional Requirements which are listed in Section 3.3: Business Functional Requirements: L-004, L-014, L-016, L-017, L-018, E-001, E-002, E-011, E-012, G-004, G-015, G-016, G-030, G-031, G-033, G-034, I-001, I-002, S-001, S-002, S-004.

Problem	
Problem 5: Limited technical support poses high risk.	
Causes and Effects	**Business Objectives**
Causes: • Some core systems are supported by a single resource with no backup • In some cases, systems technologies are over 30 years old and there are few experts in the industry available for technical support • Staff have not been trained to maintain systems **Effects:** • Some programs face high risk as technical support resources become unavailable • Maintenance for some systems is irregular and infrequent, or lacking • Many system errors are not corrected; staff utilize manual work alternatives	5.0 **Provide adequate technical support for current and future business needs.** 5.1 Provide a system based on industry-supported technology 5.2 Provide adequate staffing, through initial vendor support, and subsequently through adequate staff support, with sufficient technical training and knowledge transfer

Business Objective 5 is supported by the following Functional Requirements which are listed in Section 3.3: Business Functional Requirements: G-006, G-007, G-028, G-029, G-032, G-033, G-034, S-001, S-002, S-003.

3.3 Business Functional Requirements

In view of the strong need to better protect the public, the participating programs have developed a common, unified list of functional requirements for the new system. Table 3 identifies the business functional requirements and maps each requirement to the respective category and priority. The categories are as follows:

Licensing – The normal workflow requirements for processing and approving applications and renewals. This applies to licensing, registration, certification, and permitting processes.

Enforcement – The workflow requirements for conducting enforcement activities.

Billing – All billing and financial function requirements

General – General system requirements

Interface – Requirements relating to interfaces with other systems

Security – Requirements for protection of data from unauthorized access or modification.

The full set of Functional Requirements will be developed during the RFP development phase, with full involvement of all CDPH programs participating in this solution.

Table 3: Business Functional Requirements

ID	Functional Requirement	Category	Priority
L-001	Provide the ability to enter and maintain application and licensing data related to all regulated entities, including: • Facilities • Machines and devices • Materials • Professionals • Corporations (manufacturers, etc.) • Schools and other education providers • Continuing education • Low level radioactive waste generators • Vehicles • Reciprocity • Licensing exemptions	Licensing	High
L-002	Provide the ability to enter and maintain data external but related to licensees (e.g., environmental data associated with a facility's location, water sources)	Licensing	High

ID	Functional Requirement	Category	Priority
L-003	Provide the ability to accommodate all machine types/uses	Licensing	High
L-004	Provide the ability to accommodate all licensing types (operator, school, radioactive materials, license commodities) with multiple types of licenses and/or levels of license certification	Licensing	High
L-005	Provide the ability to enter and maintain data specific to licensing type (e.g., minimum Continuing Education Unit (CEU) requirements based on radiation machine operator type)	Licensing	High
L-006	Provide multiple options of different media/modes for applicant submission	Licensing	High
L-007	Provide the ability for authorized customers (operators, licensees) to enter licensing data (e.g., new applications, renewal applications, amendments, address changes, ownership transfer, continuing education unit data) via a secure website	Licensing	High
L-008	Provide a checklist of additional/missing documentation required with the new or renewal license application	Licensing	Medium
L-009	Provide the ability for licensees to submit required reports on-line (e.g., treatment facility self-reporting of volume and weight)	Licensing	High
L-010	Automatically calculate minimum financial surety amounts due based on licensing data	Licensing	Medium
L-011	Provide the ability upon change of ownership to trigger a new application process and associated fees, and disposition the old record, as appropriate	Licensing	Medium
L-012	Provide robust tracking mechanisms for all licensing functions (e.g., application, inspections, criminal background)	Licensing	High
L-013	Provide the ability to track and maintain list of all licensing amendments and conditions including history thereof for all licensing requirements	Licensing	High
L-014	Provide the ability to generate licenses, registrations, certificates, and cards for all license types	Licensing	High

ID	Functional Requirement	Category	Priority
L-015	Provide the ability for operator licensees to print temporary license data via a secure website	Licensing	High
L-016	Provide the ability for CDPH to retain image data of a generated license, registration, or certificate	Licensing	Medium
L-017	Provide linkage to any imaged documentation associated with a licensee, such as site layouts, photos, etc.	Licensing	Medium
L-018	Provide the ability to generate standard legislatively or other external stakeholder required reports (e.g., low level radioactive waste (LLRW) annual reports required by SB 2065, multiple HSC sections)	Licensing	High
E-001	Provide the ability to enter and maintain licensee enforcement data: • Inspection • Enforcement actions taken • Complaints/Allegations • Violations • Deficiencies • Investigations • Emergency response activities	Enforcement	High
E-002	Provide the ability to enter and maintain data related to complaints/allegations/violations/deficiencies received on non-licensees	Enforcement	High
E-003	Provide the ability to enter and maintain geocode and site location data for all licensees	Enforcement	Medium
E-004	Provide the ability to enter and maintain geocode and site location data for all incidents and emergency responses	Enforcement	Medium
E-005	Automatically identify inspections due based on licensee type, date of last inspection, renewal date, site visit cycle, and relative risk and priority of licensee up to a six year horizon	Enforcement	High
E-006	Assign inspections to staff based on program type with override capability	Enforcement	Medium
E-007	Automatically assign inspections to supervisor or staff based on inspection type with override capability	Enforcement	Medium

ID	Functional Requirement	Category	Priority
E-008	Assign appropriate inspectors/investigators/ supervisors based on geographic location of the inspector and the inspection site using GIS data with override capabilities	Enforcement	Medium
E-009	Provide electronic inspection report templates with multiple inspection types	Enforcement	High
E-010	Provide the ability for on-line creation of enforcement documentation (e.g., inspection and investigation forms, embargo notices, and sample receipts)	Enforcement	High
E-011	Provide electronic notice of violations (NOV), NOVRUD, Form 5010 templates and maintain NOV data	Enforcement	High
E-012	Provide the ability to track all inspections, deficiencies, allegations, complaints, investigations, violations, incidents and emergency responses	Enforcement	High
B-001	Provide the ability to enter and maintain billing and payment data related to all regulated entities and sub-entities for which separate billing is required	Billing	High
B-002	Provide standard fee and sub-fee tables for all program/license types	Billing	High
B-003	Provide standard fee tables for all fee types (e.g., penalties, late fees)	Billing	High
B-004	Automatically calculate payment due based on program/license/certificate type, fee type, and license expiration date (e.g., complex rules-based fee calculations - dynamic algorithm)	Billing	High
B-005	Provide billing reconciliation function and maintain a running balance for each entity as applicable	Billing	High
B-006	Allow capability to generate a single itemized bill for customers with multiple license types	Billing	High
B-007	Automatically generate billing notices for outstanding payments based on expiration date and pre-defined intervals (e.g., 60 days, 30 days, and 15 days)	Billing	High

ID	Functional Requirement	Category	Priority
B-008	Track data related to various payment types, including checks, electronic funds transfer, debit cards, and credit cards	Billing	High
B-009	Provide payment options for authorized customers (including electronic payments via a secure website)	Billing	High
B-010	Provide the ability to update records with payments received	Billing	High
B-011	Provide the ability to scan received remittance slips and checks into the system, recognizing, at a minimum, customer identifier, payment amount due, and date of scan	Billing	Medium
B-012	Provide the ability to track overpayments and apply overpayment credits to a customer's account	Billing	High
B-013	Provide the ability to track refunds	Billing	High
B-014	Provide the ability to track dishonored checks	Billing	High
B-015	Provide assistance to track orphaned checks	Billing	Medium
B-016	Provide ability for customers to receive/print a receipt	Billing	High
B-017	Provide the ability for authorized customers to review their billing and payment information via a secure website	Billing	High
B-018	Provide the ability to generate standard fiscal reports including, but not limited to, batched check reports, reconciliation reports, accounts receivable reports, aging reports, and deposits	Billing	High
G-001	Provide on-line system-wide access for personnel located in headquarters, regional offices, and remote sites (e.g., VPN access)	General	High
G-002	Accommodate on-line web access to licensee data to multiple levels of authorized external stakeholders including the public and the licensee	General	High
G-003	Provide multiple levels of user authorizations	General	High

ID	Functional Requirement	Category	Priority
G-004	Provide on-line access to at least ten years of licensee data including, but not limited to, license, enforcement, billing, and payment data. For some programs, historical date since inception is required	General	High
G-005	Provide the ability for the public to perform searches as appropriate on licensees (e.g., key on company name) and obtain basic, non-confidential license data/status via the Internet	General	High
G-006	Provide a minimum of 18 hours/7 days intranet availability	General	High
G-007	Provide a minimum of 18 hours/7 days internet availability	General	High
G-008	Support telephonic access to license information	General	Low
G-009	Provide a permanent identification number (unique identifier)	General	High
G-010	Provide robust search capability (e.g., by address, name, owner, license number, director)	General	High
G-011	Maintain data relationships required to associate multiple related entities (e.g., facility to machine)	General	High
G-012	Maintain multiple contacts and multiple contact information for each regulated entity	General	High
G-013	Provide ability for remote staff to enter data via an intranet	General	High
G-014	Provide context sensitive 'Help function'	General	High
G-015	Employ use of rules based flags for invalid entries, pick lists (drop down boxes), spell check, prompt screens, and similar tools to insure data integrity	General	High
G-016	Provide ability to customize field names and field size	General	Medium
G-017	Provide the ability to record comments	General	High
G-018	Provide standard on-line fill-in forms and templates (e.g., register a complaint, apply for a license)	General	High
G-019	Provide the ability to obtain workload statistics using data in the system (e.g., number of days to review an application)	General	High

ID	Functional Requirement	Category	Priority
G-020	Provide the ability to generate standard reports, letters, and forms – via an intuitive report writer tool	General	High
G-021	Provide the ability to perform ad hoc queries, generate ad hoc reports as well as “canned” reports	General	High
G-022	Provide ability to lookup GIS location characteristics (e.g., terrain) for a particular geocode/address	General	Medium
G-023	Provides for document access, management, and storage via imaging (e.g., image paper records, manage regulation library)	General	High
G-024	Provide the ability to track incoming and outgoing correspondences between programs and customers	General	High
G-025	Provide an on-line tickler or flagging capability for staff that identifies assigned workload and status	General	High
G-026	Provide ability to flag a particular safety risk associated with a licensee	General	High
G-027	Tracks/monitors non-compliance with process timeframes and create alerts at the appropriate levels	General	High
G-028	Full system documentation is provided: User documentation, technical support documentation, etc.	General	Medium
G-029	Full training is provided, for users, “power” users, technicians, and administrators	General	Medium
G-030	Provide the system flexibility to add data elements needed to address changes in regulation and requests by external stakeholders	General	High
G-031	Flexible/highly configurable by trained administrators; system requires little or no-in house programming support	General	Medium
G-032	System must have an easy to use graphical user interface, operating within a standard web browser	General	High
G-033	Comply with CDPH, DTS, and State Administrative Manual system standards	General	High

ID	Functional Requirement	Category	Priority
G-034	Provide a minimum of one year of vendor staff maintenance and operation (M&O) of the new system, measured from the date of the last CDPH program implemented. Provide two optional additional years of vendor staff M&O. Provide all necessary technical training and documentation to allow CDPH staff to take over full support following the required first year of M&O, at state's option.	General	High
G-034	Configurations made in-house by CDPH will not eliminate CDPH's ability to upgrade at next vendor release	General	High
I-001	Allow users the ability to view scanned documents in the existing repository, to be made available to the other participating programs to scan and view their relevant documents.	Interface	Medium
I-002	Allow the ability to import information from outside service providers (e.g., training institutions, testing vendors)	Interface	Low
S-001	Meet all state and CDPH requirements for data, network, and desktop security	Security	High
S-002	Allow for flexible administrator defined access levels (e.g., by role) to functions, processes, and data	Security	High
S-003	Provide an audit trail for all data entry and data changes, including date, time, and user identification	Security	High
S-004	Provide ability to use electronic signatures for possible future enhancement	Security	Low

4.0 BASELINE ANALYSIS

This section provides an overview of the existing technical environment and infrastructure that supports the specified five programs, and the current technology standards[3] defined by the CDPH Information Technology Services Division (ITSD).

This section is organized as follows:

4.1 Major Business Activities

4.2 Current Method

4.3 Technical Environment

4.1 Major Business Activities

The range of entities that CDPH licenses, certifies, or registers is a diverse array that includes healthcare facilities, laboratories, food and drug product manufacturers, medical waste generators, bottled water distributors, X-ray machines, and occupations as diverse as laboratory directors, water treatment system operators, and X-ray machine operators, through the following five CDPH programs:

- Food and Drug Program
- Radiation Safety Program
- Drinking Water Operator Certification Program
- Safe Drinking Water Systems Program
- Medical Waste Management Program

An overview of each participating program is shown in Section 3: Business Case.

As described in that section, the five programs exhibit similarities within their common functions, and today those common functions are supported by a tangled mixture of technological platforms. Many of these platforms have become outdated and are difficult to maintain, supported by only a small number of staff, or reliant on dwindling skill sets due to retirements and obsolescence of technology. In fact, some systems now have no skilled staff remaining to support the system. In addition, numerous stand-alone MS Access and MS Excel systems are created as work-around temporary solutions.

[3] Source: CDPH Information Technology Hardware and Software Standards Volume 1, May 31, 2007.

Process flowcharts of the major business processes of each program are shown in Appendix D: Current Process Flowcharts.

The current licensing business activities and related processes of the five programs are as follows:

Food and Drug Program (through the Food & Drug Branch, FDB)

The Food and Drug Branch assures that foods, drugs, medical devices, and certain other consumer products are safe and not adulterated, misbranded, or falsely advertised. The Branch also ensures that drugs and medical devices are effective; enforces laws related to food, drug, and medical device manufacturing through licensing, inspections, and effective industry and consumer education. In addition, the Branch provides education to businesses to understand the public health basis for regulatory requirements and encourages businesses to voluntarily correct deficiencies; and uniformly enforces regulatory requirements to prevent unfair competition.

Business activities and the associated regulated entities:	Processes performed for each regulated entity:							
	Application/ approval	Inspection or proficiency testing	Renewal	Inquiry/lookup	Maintain historical information	Complaint investigation	Billing	Enforcement
License, regulate and enforce standards for food processing facilities	✓	✓	✓	✓	✓	✓	✓	✓
License, regulate and enforce standards for drug and medical device manufacturing facilities	✓	✓	✓	✓	✓	✓	✓	✓
License, regulate and enforce standards for Home Medical Device Retail (HMDR) facilities	✓	✓	✓	✓	✓	✓	✓	✓
Certify that food, drug, medical device and cosmetic products are safe for export to other states and countries	✓	✓	✓	✓	✓	✓	✓	✓

Radiation Safety (through the Radiologic Health Branch, RHB)

RHB's mission is to enhance and protect public health, safety, and environmental quality by regulating the use of and exposure to radiation. RHB enforces radiation

control laws and regulations designed to protect the public, radiation workers, and the environment.

Business activities and the associated regulated entities:	Processes performed for each regulated entity:							
	Application/ approval	Inspection or proficiency testing	Renewal	Inquiry/lookup	Maintain historical information	Complaint investigation	Billing	Enforcement
Register radiation machines (including reconcile report of assembly)	✓	✓	✓	✓	✓	✓	✓	✓
Certify radiation machine operators	✓	✓	✓	✓	✓	✓	✓	✓
Certify mammography facilities and machines	✓	✓	✓	✓	✓	✓	✓	✓
Certify schools/clinical sites	✓	✓	✓	✓	✓		✓	✓
Perform radiologic technology school inspection	✓	✓	✓	✓	✓	✓	✓	✓

Drinking Water Operator Certification Program (OCP)

The Operator Certification Program assures that drinking water system operators (individuals) have the minimum knowledge and experience required by the federal Safe Drinking Water Act (SDWA).

Business activities and the associated regulated entities:	Processes performed for each regulated entity:							
	Application/ approval	Inspection or proficiency testing	Renewal	Inquiry/lookup	Maintain historical information	Complaint investigation	Billing	Enforcement
Certify drinking water treatment system operators	✓	✓	✓	✓	✓	✓	✓	✓
Certify drinking water distribution system operators	✓	✓	✓	✓	✓	✓	✓	✓

Safe Drinking Water Systems

This program provides direct oversight including the permitting, inspection, and enforcement of small water systems (those with fewer than 200 service connections), in 23 counties and delegates responsibility to local environmental health jurisdictions (also known as Local Primacy Agencies) for oversight of the small water systems in the remaining 35 counties. These water systems are billed annually and fees are collected by the program. CDPH is also allowed by statute to bill up to $1,000 of time spent on enforcement activities against the water system.

Business activities and the associated regulated entities:	Processes performed for each regulated entity:							
	Application/ approval	Inspection or proficiency testing	Renewal	Inquiry/lookup	Maintain historical information	Complaint investigation	Billing	Enforcement
Permit and inspect large and small Public Water Systems (PWS)	✓	✓		✓	✓	✓	✓	✓
Delegate regulatory activities to Local Primacy Agencies (LPAs)								

Medical Waste Management Program

The Medical Waste Management Program (MWMP) protects the public and the environment from potential infectious exposure to disease-causing agents through the regulation and oversight of the generation, handling, storage, treatment, and disposal of medical waste in accordance with the Medical Waste Management Act (MWMA). MWMP's primary activities consist of the following:

Business activities and the associated regulated entities:	Processes performed for each regulated entity:							
	Application/ approval	Inspection or proficiency testing	Renewal	Inquiry/lookup	Maintain historical information	Complaint investigation	Billing	Enforcement
Permit off-site treatment facilities, alternative medical waste treatment technologies, and medical waste transfer stations	✓	✓	✓	✓	✓	✓	✓	✓
Permit healthcare facilities to treat waste	✓	✓	✓	✓	✓	✓	✓	✓
Register healthcare facilities that generate medical waste	✓	✓	✓	✓	✓	✓	✓	✓
Register trauma scene practitioners	✓	✓	✓	✓	✓	✓	✓	✓
Authorize medical waste haulers	✓			✓	✓			

4.2 Current Method

This section provides an overview of the current methods used by the programs in carrying out their licensing and state certification regulatory responsibilities.

4.2.1 Current Systems

The inventory of the systems currently in use is shown in Section 3: Business Case. The sheer complexity of the inventory is one indicator of the tangled, disparate nature of the environment.

4.2.2 Food and Drug Program Major Systems and Limitations

Food and Drug Program systems include:

Licensing System

The Licensing System is the core system for the Food & Drug Branch. It was originally converted into MS Access from 13 different systems in 2004 based upon the drug,

medical device and Home Medical Device Retailer databases created in 2002/2003. It tracks license, renewals, fees, and billing for food processors, drugs, medical devices and Home Medical Device Retailers. The database also provides general information on a company's compliance history, corporate structure, updated contact information and GPS coordinates. Some limited Prescription Drug Marketing Act (PDMA) information is also recorded.

Food Inspection Activity Tracking

In the early 1990s the California Legislature passed a more stringent food processor registration and inspection law. To comply with this new statute, a homegrown database was developed to track food inspection assignments and dates. This system was developed in "Clipper" – a technology popular for a short time in the 1990s.

Drug and Device

In 2001 the Food and Drug Branch acquired the Home Medical Device Retailer program from the Board of Pharmacy. Initially, a database was created in MS Access to track licenses, renewals and fees for this new program, and additionally, the Drug and Medical Device Manufacturer programs databases were also created in MS Access in 2002/2003 from a failing Clipper system. The databases were created for drug, medical device and HMDR for licensing, inspection and enforcement information.

Exemptees

The Exemptees database was developed in MS Access to track Home Medical Device exemptee information. A licensed exemptee or pharmacist is required for HMDR facilities that dispense prescription medical devices or medical oxygen.

Export

The Export database was developed in MS Access in 2000 as a result of new state legislation authorizing the department to issue export certificates for foods, medical devices, drugs and cosmetics that are shipped outside of California. The database is used to track application status and issuance of official certificates.

Complaint

The Complaint database was developed in MS Access in the early 1990s using the information on the Food and Drug Branch complaint form to create one repository for food, drug and medical device complaints and enforcement actions. Reports are generated from the system and sent to the field offices for follow-up on complaints. The reports are also used to track metrics and to check for complaint patterns.

Figure 2 provides a conceptual view of Food and Drug Program current systems environment.

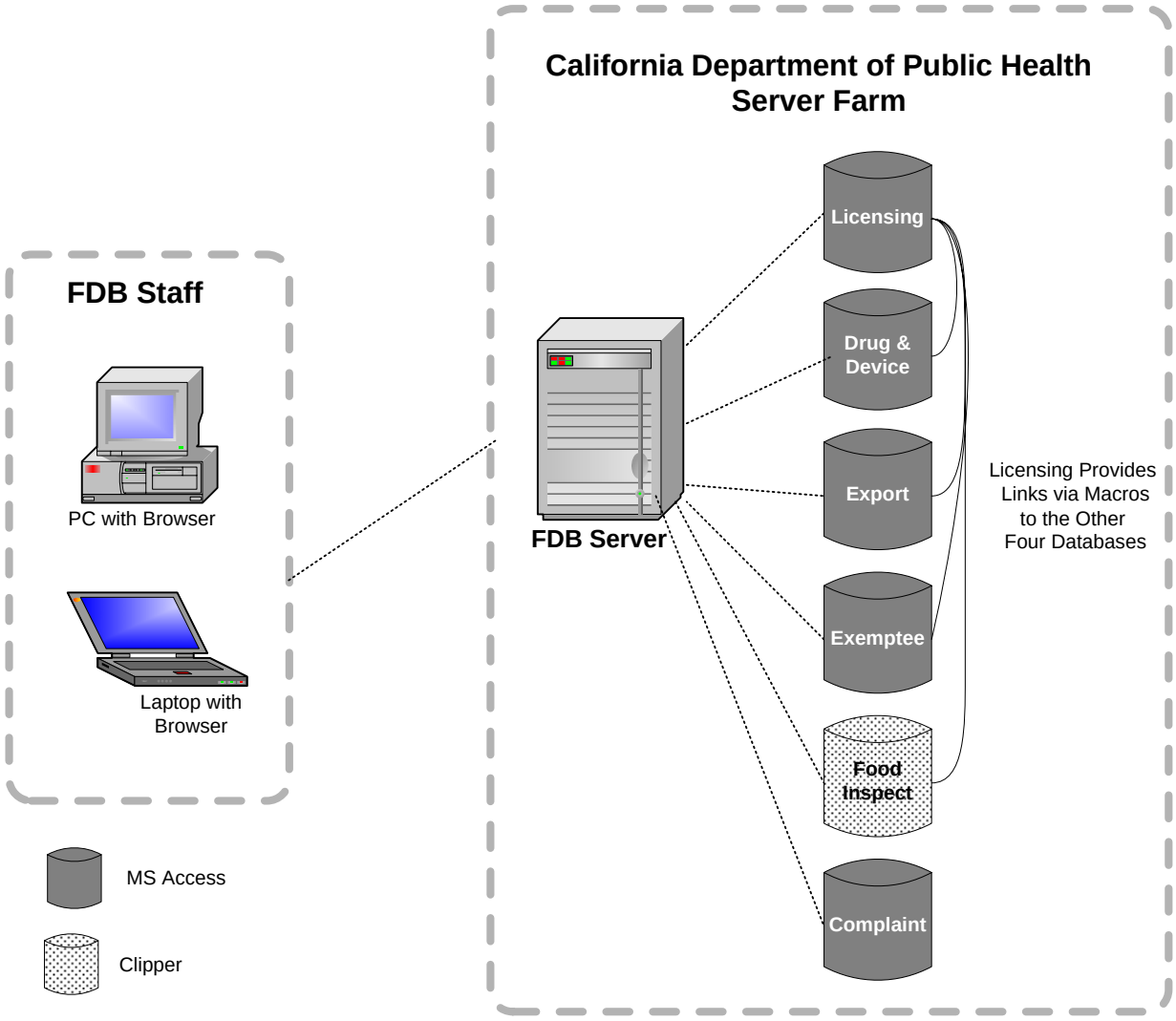


Figure 2: Food & Drug Program Current Systems Environment

The current limitations of the Food & Drug Program's systems include:

High-volume functions are all handled through manual processes and paper files, creating delays and increasing State costs

Processing applications, preparing renewals, and related functions are all core, high-volume functions of FDB's program. These are all handled through manual processes and paper files. Current systems do not support online completion of applications, e-mail of renewal and late notices, and other high-volume functions.

Lack of a workflow management system

There is no "processing" system which would integrate the workflow of activities throughout the licensing process.

Lack of electronic payment capabilities

A significant limitation of the current systems is billing and payment processing including the lack of an Internet-enabled or EFT payment option. Currently FDB is only able to accept checks and money orders and cannot accept electronic payments of any type. Neither staff nor customers can obtain updated payment status information. A web-based payment option (or at least EFT) for FDB, through a 3rd party vendor along with a status lookup feature, implemented as part of an enterprise system, would significantly address these current limitations and provide expected service to FDB's customers.

Long-outdated technology and complete lack of technical support

The Food Inspection Activity Tracking database was developed in "Clipper," a long-outdated technology popular in the early 1990s for some data capture and reporting purposes. Very few professionals are familiar with this technology, and there is no support staff remaining within CDPH. The homegrown system was developed by a non-IT-trained individual who has since retired. It is not documented or supported, and is in disrepair.

Security, privacy and confidentiality of data are not a significant issue currently within FDB's systems.

4.2.3 Radiation Safety Major Systems and Limitations

Radiation Safety systems include:

Health Application Licensing (HAL) System

The main system used to support RHB's radiation machine program is the HAL system. This antiquated, 3270 emulation mainframe system was acquired by CDPH from the California Department of Consumer Affairs (DCA) in 1987 when health-related licensing and billing functions were transferred to RHB. At that time, the objective of HAL was to track certifications associated with radiation machine operators; track registration of radiation machines; and track related billing and payments. The HAL system was implemented with the expectation that a series of manual processes would compensate for the lack of system features and functionality. Today, the HAL system continues to

serve as the repository for license and billing data related to radiation machines, with relatively few enhancements or major improvements since 1987.

California Mammography Information System (CAMIS)

To comply with federal and state legislation, RHB must maintain registration and inspection data related to mammography machines. RHB uses a MS Access database called the California Mammography Information System (CAMIS) to track data related to mammography machines; however, mammography machines and their respective operator data is also maintained in the HAL system to accommodate billing and payment processing.

RAM2000 and MAIL2000

Because HAL lacks the ability to track data related to radioactive materials, RHB has developed two core MS Access databases to address this program. The RAM2000 and MAIL2000 databases are used to track applications, licenses, correspondence, billing, and payment data related to the radioactive materials program.

5010 Tracking Database and Notice of Violation (NOV) Tracking Database

All enforcement-related processes are manual and paper-based. This includes tracking of inspections, allegations, complaints, investigations, violations, incidents, and emergency response data. There are two forms RHB uses in its enforcement function: Form RH5010 (to log an investigation) and the notice of violation (NOV) form. To provide some minor assistance, RHB has created two MS Access databases to track each of these forms (i.e., Form 5010 Tracking database and NOV Tracking database).

Radiologic Technician MS Access Database

RHB maintains Radiologic Technician School Approval data within an MS Access database created by the program manager. The database captures approved school information and related clinical sites within an estimated 1,000 records.

Generally Licensed Devices (GLD)

RHB registers all “generally licensed devices” that contain radioactive materials. GLD is an MS Access database that tracks this registration data. It is a stand-alone database that resides on the RHB LAN server and all data entry is manual. It contains over 200,000 registration records for approximately 20,000 sources (contractors).

Low Level Radioactive Waste Tracking System (LLRWTS)

To comply with federal and state legislation, RHB must track all shipments and storage of low level radioactive waste from generators (hospitals, labs, universities, military installations, etc.). LLRWTS is an MS Access database that tracks this data; up to 350,000 records per year. It is a stand-alone database that resides on the RHB LAN server and all data entry is manual.

Figure 3 provides a conceptual view of RHB’s current systems environment.

Radiation Safety Current Systems Environment

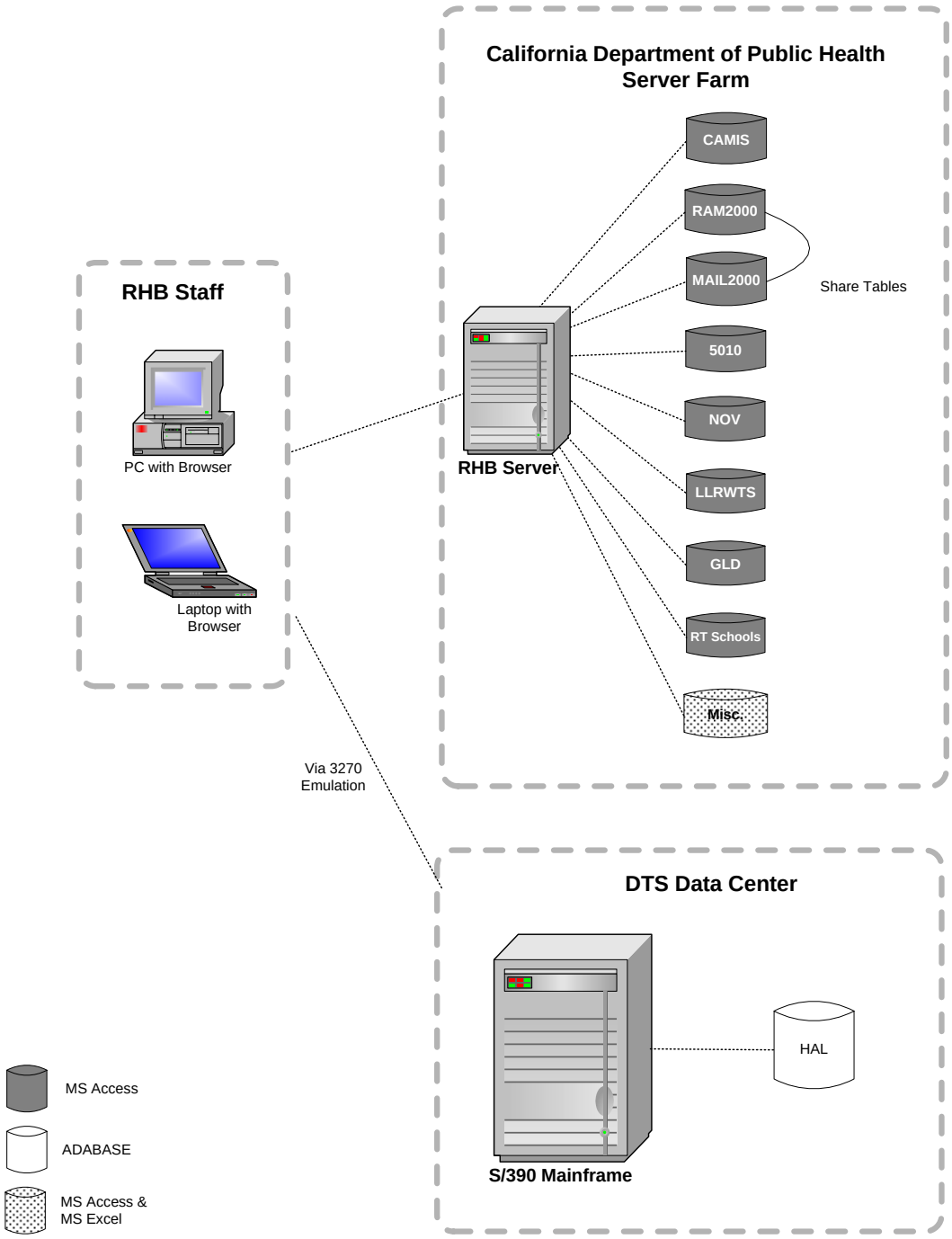


Figure 3: Radiation Safety Current Systems Environment

Radiation Safety systems limitations include**:**

RHB's systems are not web-enabled

One of the most significant shortcomings of the existing systems is that they do not provide RHB's customers online capability to submit applications, changes, or renewals via the web. As a result, customers must submit all information to RHB via paper-based forms which are cumbersome and often incomplete or incorrect.

Lack of electronic payment capabilities

A significant limitation of the current systems is billing and payment processing – including the lack of an Internet-enabled or EFT payment option. Currently RHB is only able to accept checks and money orders and cannot accept electronic payments of any type. Neither staff nor customers can obtain updated payment status information. A web-based payment option (or at least EFT) for RHB, through a 3rd party vendor along with a status lookup feature, implemented as part of an enterprise system, would significantly address these current limitations and provide expected service to RHB's customers.

Modifications to the HAL system are time-consuming and costly

The HAL system resides on an antiquated mainframe platform of Natural and COBOL, with an ADABAS database and 3270 emulation user interface. The HAL system is used by three organizations within CDPH and is currently supported by a shared pool of ITSD staff (i.e., RHB does not have dedicated resources). ITSD resources are limited and few ITSD staff are knowledgeable of the HAL system and the antiquated technology in which it operates. Minor modifications are extremely challenging because changes have a rippling impact to other lines of code in the system. Also, the database structure cannot be easily expanded to accommodate mandated changes. RHB's service requests are considered in the context of service requests and needs of the other two organizations using the HAL system. Today, a minimal number of service requests submitted by RHB are addressed by ITSD due to the lack of ITSD resources and priority given to requests submitted by the other organizations.

External stakeholders are affected because RHB is unable to respond adequately to external requests for information

There is no ad hoc reporting capability within the HAL system. RHB is unable to respond adequately to external requests for information (agency, media, etc.). HAL does not support the business processes needed by the program.

RHB lacks systems to support several of its programs and functions

RHB lacks a single, integrated system that can support all of RHB's programs and related regulatory requirements. Today, RHB's systems essentially maintain minimal licensing and billing data for the highest-volume license types. The HAL system does not provide the ability to track less common licenses, such as limited permits, certifications for therapists, etc. The HAL system has limitations that cause it to not be usable for two of RHB's three major programs: radiologic technology schools and radioactive materials.

Currently, RHB lacks a system that supports several processes including inspections, complaints, allegations, incidents, emergency response, enforcement actions, reporting, workload assignment, and statistical analysis. These processes are managed by paper forms, proliferating manual processes and limiting access to data. Similarly, the RAM2000 and MAIL2000 databases also have limited features and functionality, requiring significant manual processes and paper handling.

Current systems are not integrated

None of RHB's systems are integrated, requiring RHB to operate its programs in silos. RHB has developed a variety of multi-user and stand-alone, single-user MS Access databases and MS Excel spreadsheets to assist in tracking data. Because the systems are not integrated, RHB staff must perform duplicate data entry into multiple systems, resulting in extra processing time, reliance on paper forms to key data into various systems, data redundancy, and enhanced probability of data error.

Lack of data integrity

RHB lacks a single data repository used by all systems. By using multiple data repositories, it is difficult to achieve data consistency. All of the systems have limited data edits and logic checks, resulting in incomplete and inaccurate data to be maintained in the databases. Furthermore, the systems have inadequate calculation features or calculate fees incorrectly. As a result, RHB staff is required to calculate fees due, penalties, etc. using a separate spreadsheet or adding machine, and then entering the total amounts into the systems. The manual calculation and transfer of totals leads to data entry errors and miscalculation of fees due. On occasion, the HAL system miscalculates fees due that are not identified until after billing notices have been distributed. This results in manual updates to the HAL system and the labor-intensive task of initiating a refund and reconciling the accounting records.

Inability to obtain statistical data

RHB is unable to perform statistical analysis or provide internal and external stakeholders data regarding the programs in which it manages. This is due to the lack of a central data repository, lack of report writing tools, and the lack of confidence in the integrity of the data maintained. As a result, it is difficult for RHB to demonstrate accountability for its operations.

Inadequate security features

All of RHB's systems lack an adequate role-based security architecture that would manage access to software modules, screens, and data, based on security roles. As a result, only a few RHB staff have authorization to enter data into the systems, resulting in the creation of central data entry groups within RHB. For some systems, RHB staff need read-only access to the data. In order to address data accessibility issues in this environment, copies of the system's databases have been created that are read-only and provided to RHB staff (e.g., RAMRead and MAILRead). Therefore, while adequate security is currently being provided for RHB data, this is done by a workaround method rather than through adequate role-based security built into the systems.

Radiologic Technician MS Access database has no support

This database has no IT support and no scheduled backup. It requires program manager time to complete manual updates and quality control reviews.

Systems lack an archiving feature

None of the current systems have defined or implemented an archiving function. All records are retained indefinitely. As new licenses continue to be issued, amendments continue to be created, sites continue to be inspected, and correspondences continue to be recorded, the increase in database size and complexity causes increasing delays and risk of system problems.

Privacy and confidentiality of data are not a significant concern currently within RHB's systems, beyond the fact cited above regarding the lack of appropriate role-based security features.

4.2.4 Drinking Water Operator Certification Program Major Systems and Limitations

Drinking Water Operator Certification systems include:

Water Operator Certification Tracking System

This database system is a client/server system that runs on FileMaker v5. The initial installation in 1999 was designed to track registration and certification of water treatment plant operators. In 2001, the program was expanded to incorporate water distribution operators to comply with EPA requirements. With this expansion came new regulations that changed the fee structure and processes, and added a new requirement for tracking continuing education credits. The database is a scripted application, designed to automate tasks in the following general categories: Applications, Renewals, Exams, and Certificates. The system tracks approximately 17,000 treatment plant operators and 25,000 distribution system operators.

OCP Miscellaneous Tools

In addition to the core tracking system, the OCP program uses a variety of stand-alone, single-user MS Excel spreadsheets developed by program staff to track miscellaneous data and perform calculations.

Figure 4 provides a conceptual view of Drinking Water Operator Certification Program current systems environment.

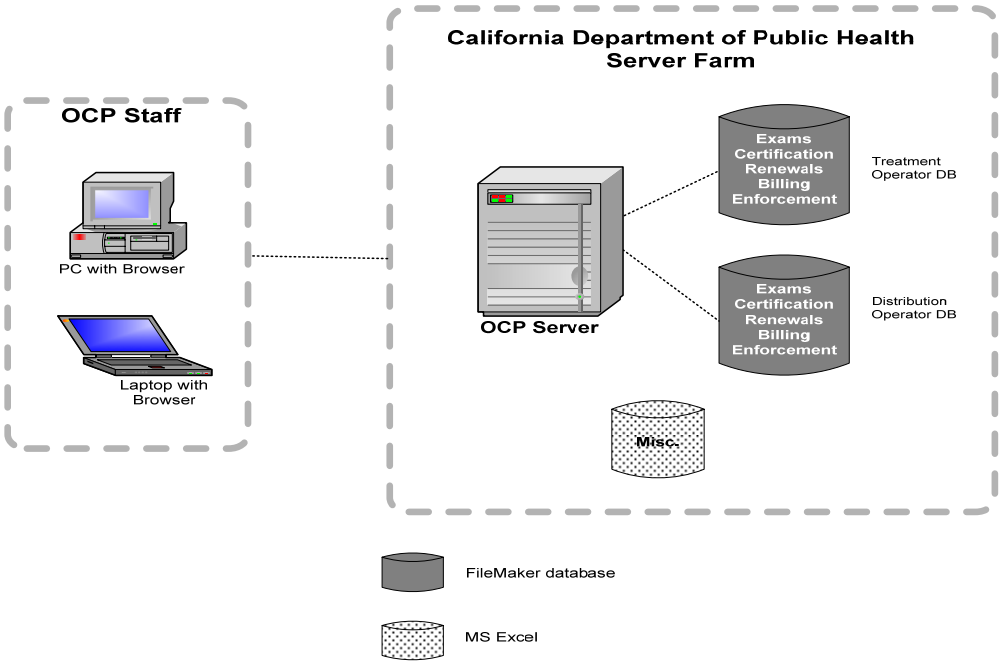


Figure 4: Drinking Water Operator Certification Program Current Systems Environment

Drinking Water Operator Certification Program systems limitations include:

Customers are forced to experience delays and rework because OCP system is not web-enabled

The most significant shortcoming of the existing system (FileMaker) is that it does not provide OCP's customers online capability to submit applications, amendments, changes, renewals, or payments via the web. As a result, customers must submit all information to OCP via paper-based forms which are cumbersome and often incomplete or incorrect. Furthermore, OCP is only able to accept checks and money orders and cannot accept electronic payments of any type.

In addition, only 40% of incoming applications are complete. A web-enabled system could catch these errors immediately, giving the applicants an opportunity to correct the problems immediately, rather than waiting many days for a letter back from the state.

Loss of efficiency due to current processes being cumbersome and inefficient

In the current FileMaker database, screens and navigation are difficult to understand and train. A significant amount of staff overtime is logged as a result. Without the ability to upgrade the processes embedded in this database, OCP is unable to achieve efficiencies that would be possible with a more modern system.

Limited technical support

OCP's FileMaker database system is supported by a single retired annuitant resource with no backup. There are few FileMaker technical experts in the industry which puts the OCP at significant risk should the current technical resource become unavailable. This Retired Annuitant is the same resource shared by the Medical Waste Management Program, which concentrates the state's risk.

However, it's notable that the OCP Database is quite stable and functions quite adequately in the uses for which it was designed. The support individual has proved adept at making any changes necessary. Replacement of this database could be done in the latter phases of a multi-program phased implementation.

Security, privacy and confidentiality of data are not a significant issue currently within OCP's systems.

4.2.5 Safe Drinking Water Systems Major Systems and Limitations

Licensing/permitting-related systems within the Safe Drinking Water Systems program include:

Permits Inspections Compliance Monitoring & Enforcement (PICME) System

The Permits Inspections Compliance Monitoring & Enforcement (PICME) system was created in 1993 to meet the California drinking water reporting requirements of the United States Environmental Protection Agency (EPA). It is an IBM mainframe database residing at DTS. PICME contains permits (conditions), inspections (codes, high level history), compliance (violation history) enforcement (violations, provisions), contacts (addresses, phone numbers, email, titles), and facilities sources (water treatment sources, facilities specifications and flows) data by public water system entity, by district. PICME 'contacts' data (name, billing address, etc.) is sent to a Focus database residing on the SDWS Local Area Network (LAN) for billing purposes. Some of this contact data is also loaded into a FileMaker database on the LAN for Permits tracking.

Permit Tracker

The Permit Tracker is a FileMaker client/server database application that resides on the SDWS LAN. It is used by only one employee in a SDWS district to manage/track water systems permits for that district.

SDWS Miscellaneous Tools

In addition to the core systems, the SDWS program uses a variety of stand-alone, single-user MS Excel spreadsheets, MS Access and Filemaker databases developed by program staff to track miscellaneous data and perform calculations.

Figure 5 provides a conceptual view of SDWS' current systems environment.

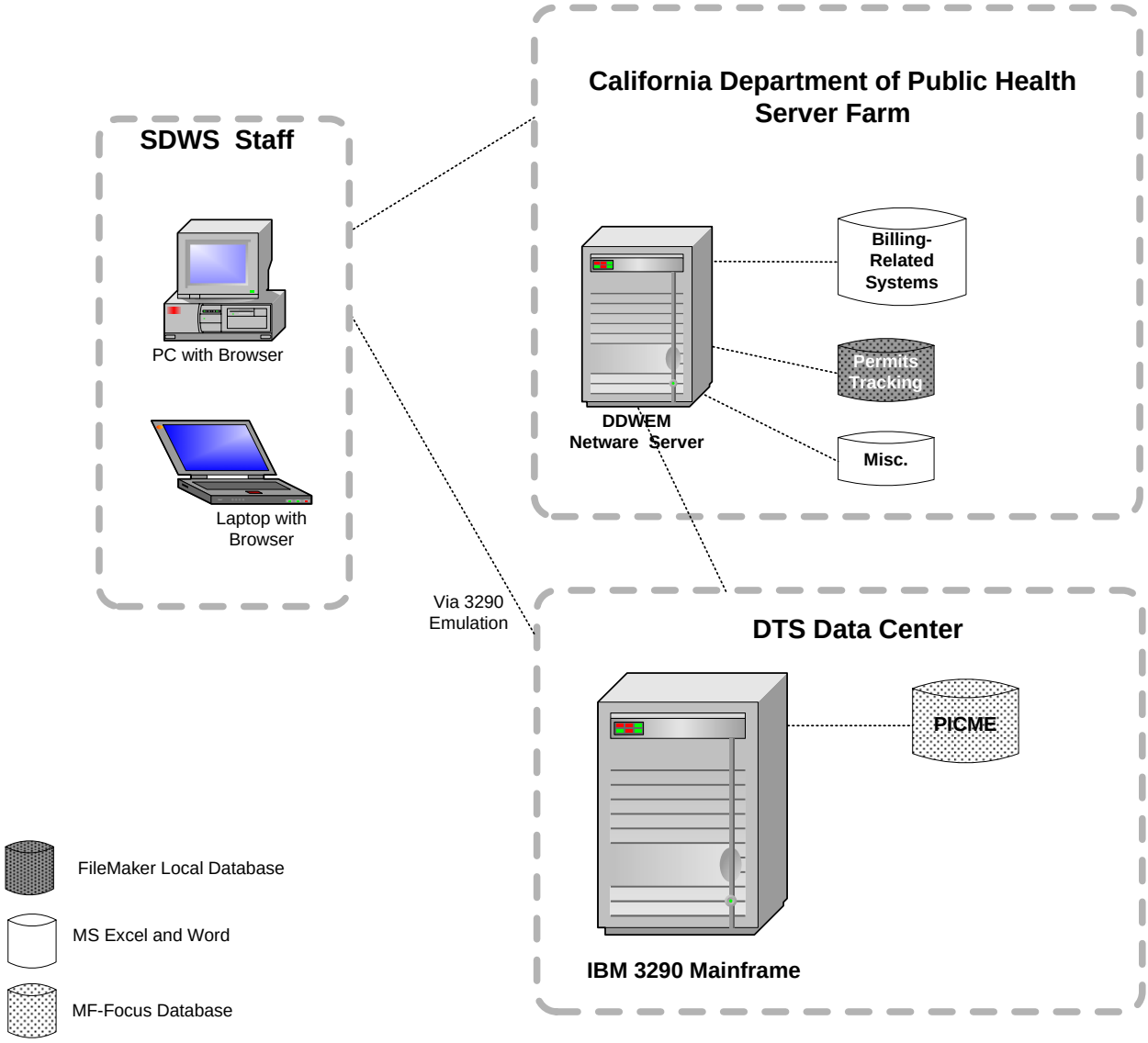


Figure 5: SDWS Current Systems Environment

SDWS' current system limitations include:

SDWS' systems are not web-enabled

One of the most significant shortcomings of the existing systems is that they do not provide SDWS' customers online capability to submit applications, amendment requests, changes, or payments via the web. As a result, customers must submit all information to SDWS via paper-based forms which are cumbersome and often incomplete or incorrect. Furthermore, SDWS is only able to accept checks and money orders and cannot accept electronic payments of any type. As the number of water

systems increases, this efficiency problem puts more of a burden on SDWS staff, causing a diversion of effort away from regulatory activities.

SDWS systems are out of date and do not meet the business need

The core SDWS systems reside on an antiquated platform of Mainframe Focus. Focus is a programming language that is over 30 years old and the systems are performing complex functions and reaching integration/interface levels beyond their intended capability. Since the Focus databases are large and complex, even minor modifications are extremely challenging because changes have a rippling impact to other lines of code in the system. Also, the database structure cannot be easily expanded to accommodate legislative or policy changes.

Limited technical support

SDWS' antiquated Mainframe-Focus databases are supported by a single technical resource with no backup. There are few Focus technical experts in the industry, which puts the SDWS Program at significant risk should the current technical resource become unavailable.

Current systems are in danger of collapse

The current billing system was created and is now maintained by one person. It is fragmented, has been modified repeatedly over time, and is now in danger of collapse. There has been no cross-training because of time and expense constraints. There is an overall personnel and technology risk.

Current systems are not integrated

None of SDWS' systems are integrated, requiring SDWS to operate its functional areas in silos. SDWS has developed a variety of multi-user and stand-alone MS Excel spreadsheets to assist in tracking data. Because the systems are not integrated, SDWS staff must perform duplicate data entry into multiple systems, resulting in extra processing time, reliance on paper forms to multiple individuals to key data into various systems, data redundancy, and greater probability of data error.

Lack of data integrity

SDWS lacks a single data source used by all systems. By using multiple data sources, it is difficult to achieve data consistency. All of the systems have limited data edits and logic checks, resulting in incomplete and inaccurate data to be maintained in the databases. Furthermore, the systems have inadequate calculation features or calculate fees incorrectly. As a result, SDWS staff is required to calculate fees due, penalties, etc. using a separate spreadsheet or calculator, and then entering the total amounts into the systems. The manual calculation and transfer of totals leads to data entry errors and miscalculation of fees due. On occasion, the SDWS Billing System miscalculates fees due that are not identified until after billing notices have been distributed. This results in manual updates to the Billing System.

Security, privacy and confidentiality of data are not a significant issue currently within SDWS' systems.

4.2.6 Medical Waste Management Program Major Systems and Limitations

Medical Waste Management Program systems include:

MWMP FileMaker Pro System

A Filemaker Pro system supports MWMP processes and fifteen staff and specialists. The system, designed and maintained by a single MWMP staff member, handles permitting, authorizing or registering common storage facilities, large and small quantity generators, transfer stations, small quantity generators onsite treatment, trauma scene practitioners, and waste haulers. This Filemaker Pro system includes 11,000 records.

Figure 6 provides a conceptual view of Medical Waste Management Program current systems environment.

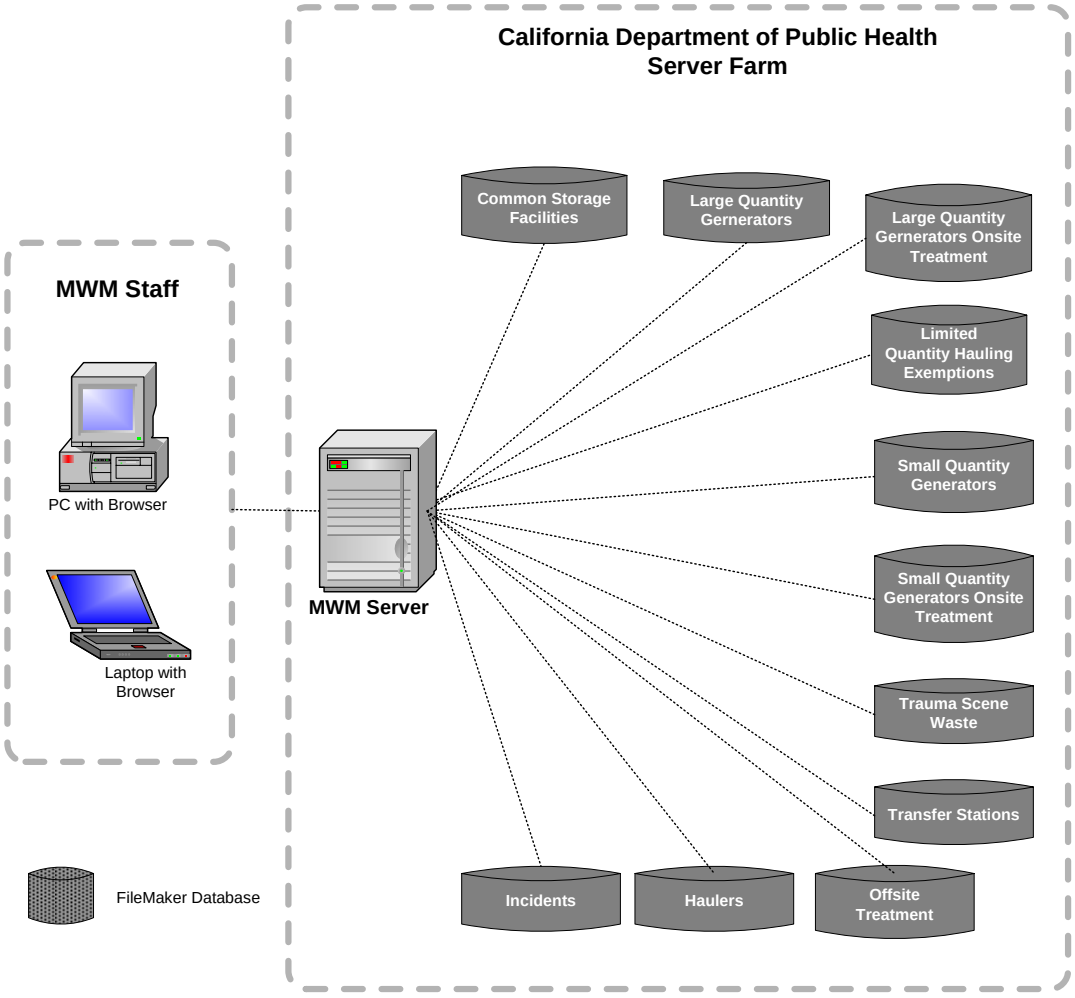


Figure 6: Medical Waste Management Program Current Systems Environment

Medical Waste Management Program systems limitations include:

Lack of electronic payment capabilities

A significant limitation of the current systems is billing and payment processing including the lack of an Internet-enabled or EFT payment option. Currently MWMP is only able to accept checks and money orders and cannot accept electronic payments of any type. Neither staff nor customers can obtain updated payment status information. A web-based payment option (or at least EFT) for MWMP, through a 3rd party vendor, along with a status lookup feature, implemented as part of an enterprise system, would significantly address these current limitations and provide expected service to MWMP customers. Staff hours are directed away from regulatory program responsibilities toward routine cashiering functions

The current system has failed to generate bills on several occasions, and encounters many problems related to financial transactions. For example, dishonored checks are difficult to track, and sometimes are not reconciled for many months. "Orphan" checks are sometimes received which can be difficult or impossible to allocate to their proper account. In these situations, program staff hours are directed away from regulatory program responsibilities to manually crosswalk payment amounts with generated bills to ensure all applicable bills have been generated.

Ability to properly carry out the regulatory requirement is impaired because the technology platform is outdated and fragile; technical support staffing is inadequate

The FilemakerPro application was designed and is supported by a single retired annuitant located in Richmond and available to MWMP staff one day a week. This one day is not adequate in providing time to maintain current records (e.g., identification of duplicate records, correction of damaged records), or to repair scripting issues that are raising the error rate. No other MWMP staff have expertise in current FilemakerPro scripts, and staff's expertise in ad hoc report development is limited.

FilemakerPro application and supporting LAN place limits on record size

The FilemakerPro application is currently approaching its maximum record size of approximately 10,000 records. In addition, the application is not provided adequate LAN partition space. MWMP staff utilize personal partition space or expansion hard drives to store site digital photos transmitted with permit applications or captured during site inspections.

System data recovery is limited

The FilemakerPro application data is backed up on a weekly basis and there is no ability to retain a history of application changes.

Security, privacy and confidentiality of data are not a significant issue currently within MWMP's systems.

4.3 Technical Environment

All five of the participating programs fall within CDPH's Center for Environmental Health and report to the Chief Deputy Director of Policy and Programs. Organizational charts are provided in Appendix E: Participating Programs Organizational Structures**.** Program management and staff have been eagerly awaiting this solution for years; and in fact, several individual programs have attempted to initiate on-line functions in recent years. Programs are quite motivated to obtain the improvements in effectiveness and efficiency of the future system. The organizational and managerial environment is ready for this long-awaited improvement.

It can be difficult to estimate the expected operational life of a proposed solution, particularly when a specific software solution has not yet been selected. However, it's not unusual for a well-functioning and well-supported IT system to remain operational well in excess of 10-15 years. This would be a reasonable minimum standard when evaluating software solutions for the current business need.

A key financial constraint is the reliance on Special Funds for this solution. It is CDPH's expectation that no General Fund dollars will be expended for this new system, nor increases in regulatory fees charged by the participating CDPH programs.

While the proposed Enterprise-wide On-line Licensing system is not specifically mandated by legislation, the project directly supports the programs' compliance with their respective governing statutes, and will strongly address the Governor's directive to provide state government services through online channels wherever appropriate. Important policy constraints exist which will guide any system replacement effort, including: the federal Health Information Portability and Accountability Act (HIPAA); the different state and federal laws governing the various programs on their ability and/or authority to implement an enterprise-wide solution; Payment Card Industry (PCI) standards for funds transfer; and general information security considerations, which are addressed below. The implementation process will be conducted with full participation of the Department's Information Security Office (ISO) toward ensuring that these important security considerations are fully addressed in the new system.

The proposed system also directly aligns with the State's IT Strategic Plan, Goal # 2 which states, "Implement common business applications and systems to improve efficiency and cost-effectiveness."

Availability of personnel resources for development and operation of current applications is limited, as described in the sections above.

4.3.1 Network Infrastructure

CDPH has developed a sophisticated network infrastructure that fully supports a server-based technology environment as well as provides direct access to the DTS data center. CDPH utilizes a DTS Ethernet wide area network (WAN) and local area network (LAN) that serves CDPH users in Sacramento and various regional offices throughout the State. The CDPH WAN provides access to the many applications used by CDPH staff. Within this network, there are three different security zones that provide accessibility to CDPH systems and tools:

- Intranet Zone
- Extranet Zone
- Internet Zone

Each of these zones provides a unique security profile that allows appropriate access and protection to data and applications. The location of a system within the various zones is based upon who will access the system. Internal CDPH staff utilize the Intranet Zone; authorized off-site staff (e.g., counties, staff not currently on-site, etc.) utilize the Extranet Zone; and the public utilizes the Internet Zone.

Intranet Zone

The Intranet Zone is the internal CDPH network that is accessible only by authorized CDPH staff. The Intranet Zone is typically used by CDPH staff directly connected to CDPH's internal private network. By logging into the LAN, staff has automatic access to the CDPH Intranet Zone, providing access to local servers as well as the designated environment at the DTS data center.

Extranet Zone

The Extranet Zone is an area of the network used primarily by non-CDPH staff who perform functions on behalf of CDPH or to support CDPH.

The Extranet Zone is configured as a three-tier environment with separate web, application, and database servers. It has its own Active Directory Forest and Domain and consists of several tiers that are logically and physically protected from each other. All communication is encrypted. The Extranet Zone is accessed through the public Internet or through a direct dial-up connection with an authentication method, such as a user id/password or certificate.

Internet Zone

The Internet Zone is that area of the network accessible by the public. This zone protects internal CDPH resources at the network and application layers. The purpose of the Internet Zone is to support public access, via the Internet, to CDPH-selected non-confidential information. Verified identity of the individuals is usually not required. This zone is the least secure and will not contain or allow access to any data not authorized for public dissemination.

CDPH's current Internet website (http://www.cdph.ca.gov) resides in this zone. Today, this website provides the public with general program information, CDPH contact information, forms (in .pdf documents), links to other websites, and some limited lookup functions.

4.3.2 Desktop Configuration

The current desktop configuration is shown in Appendix C: Hardware and Software Standards.

4.3.3 Technology Standard: Software

This section defines the current CDPH technology standards related to software.

Desktop/Laptop Software Standards

The current software standards are shown in Appendix C: Hardware and Software Standards.

Programming Software Standards

The current programming software standards are shown in Appendix C: Hardware and Software Standards.

Server Software Standards

The current server software standards are shown in Appendix C: Hardware and Software Standards.

4.3.4 Technology Standard: Hardware

This section defines the current CDPH technology standards related to hardware.

Server Hardware Standards

The current server hardware standards are shown in Appendix C: Hardware and Software Standards.

Network Topology and Equipment Standards

The current network topology and equipment standards are shown in Appendix C: Hardware and Software Standards.

4.3.5 Technology Standard: Security

Appendix B: CDPH Information Security Standards, SR-1, identifies the current security standards for all CDPH systems.

4.3.6 Project Management Standards

ITSD's Project Management Office (PMO) defines project management standards and oversees the management of all IT projects. The standards are aligned with the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK) and the State of California's Statewide Information Management Manual (SIMM).

5.0 PROPOSED SOLUTION

For this business-based procurement solution, the CDPH proposes the implementation of an enterprise-wide licensing system to address current system limitations, directly impacting the CDPH ability to effectively carry out responsibilities for minimizing health and safety risks to California residents. CDPH proposes to conduct a business-based procurement to select a vendor to provide an information technology solution that will address the business needs and functional requirements identified in Section 3: Business Case.

Figure 7 depicts a process-level view of the proposed solution. This figure can be contrasted with the many diverse processes currently carried out by the five programs (as shown in Appendix D). The streamlined nature of this proposed solution, along with the improved interaction with regulated entities, results in the improved public health and safety as well as improved efficiency of operations as shown in Section 8.

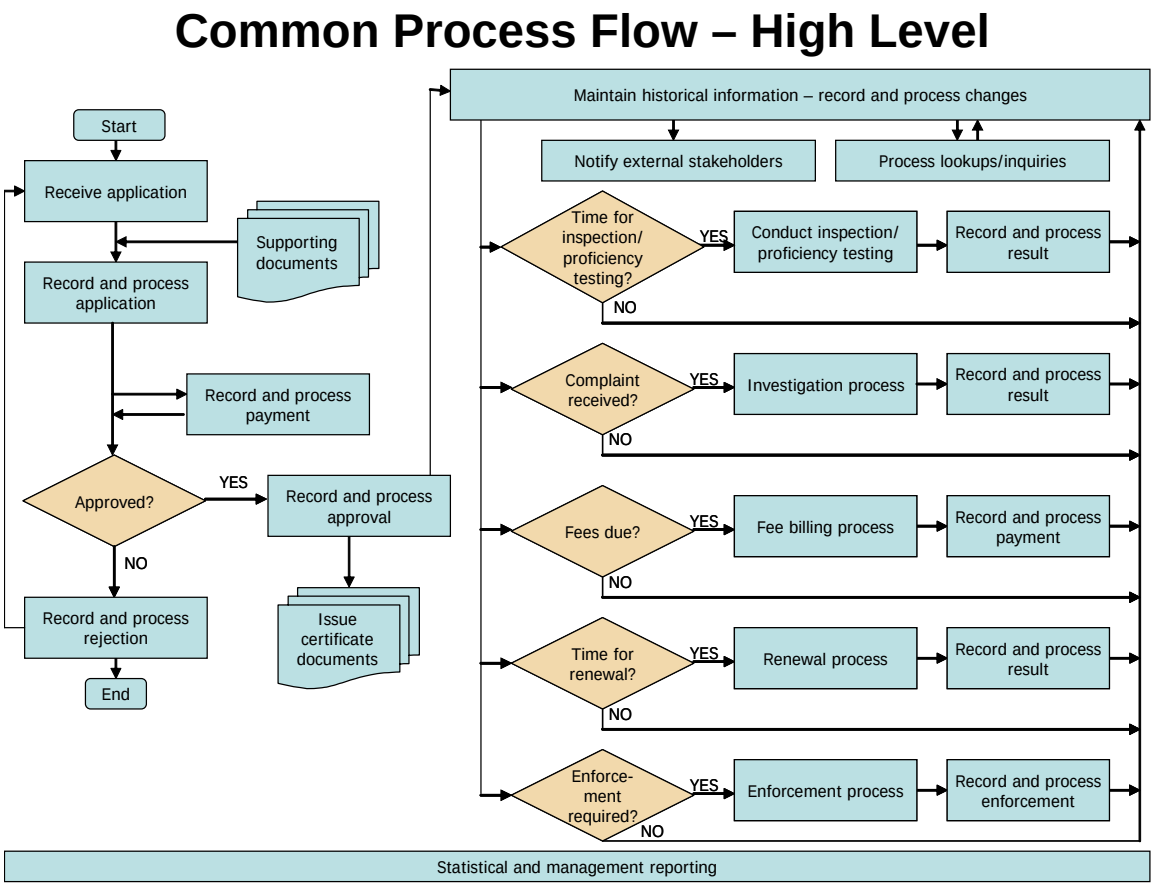


Figure 7: EOL Common Process Flow

This section presents the proposed business-based procurement solution and identifies alternative solutions that were considered.

The remainder of this section is organized as follows:

5.1 Solution Description

5.2 Rationale for Selection

5.3 Other Alternatives Considered

CDPH chooses to conduct a business-based procurement for the following key reasons:

- CDPH's needs are complex and cross multiple licensing programs.
- Vendor product offerings exist which appear to be very close fits to CDPH's needs.
- The competitive procurement phase, using detailed CDPH requirements, and thorough product demonstrations from all interested vendors, will afford the State much greater visibility into the comparative strengths and pricing structures of the competing vendor software solutions.

This solution proposed by CDPH is aligned with the California Service-Oriented Architecture (Cal-SOA) approach[4] defined by the California CIO in conjunction with the Enterprise Leadership Council which was established to provide over-arching, enterprise-wide governance. The Council notes[5] that "[t]he capacity to share data among the revenue departments, and for the revenue departments to cross-check data held by other departments, contributes to appropriate enforcement and collections." CDPH is eager to work collaboratively with other departments to make the solution available for their licensing-related needs.

In other words, this Enterprise-wide On-line Licensing project proposed by CDPH accomplishes one of the key fundamental steps in fulfilling the SOA vision; namely, it "[b]uild[s] a foundational technology infrastructure in one or more data centers to support Cal-SOA."[6]

5.1 Solution Description

Specific problems cited in Section 3, Business Case include:

[4] California Service-Oriented Architecture ("Cal-SOA"), J. Clark Kelso, California Chief Information Officer, December 28, 2007.

[5] Ibid, p. 1.

[6] Ibid, p. 3.

- Numerous risks to Californians' public health and safety are caused by the current antiquated and fragmented licensing-related systems.
- Staff's ability to protect the public and serve customers' needs and demands for modern service levels are impacted by current paper-based, non-web systems.
- Redirection of public health resources (program staff time) away from public health duties toward system issues, limiting programs' effectiveness.
- Current systems make it difficult to meet regulations and legislative mandates as well as policy directives.
- Limited technical support poses high risk of system failures.

The proposed solution is a web-based, off-the-shelf software product with a centralized database that will contain licensing, enforcement, and billing data for CDPH's applicable licensing programs. The solution is scalable and will not interfere with existing CDPH efforts.

Most importantly, the proposed solution will directly address many of the operational challenges that have led to the public health risks described in this document.

The CDPH proposes this solution to integrate systems, on an enterprise-wide basis, for significant business improvements in both external interactions (with regulated entities, the public, other government agencies) and internal processing efficiencies. This enterprise-wide system is anticipated to provide broad and secure access for CDPH users and, where appropriate under existing security rules, the general public. The system will also provide multi-program data retention and archiving which will help to provide valid data for emergency response assistance, statistical analyses, and other purposes.

This system integration is possible because of the similarities between CDPH Program functions. EOL is intended to provide a web-based, off-the-shelf integrated solution that supports the application and approval processes for certification, registration and licensing; inspection and proficiency testing; complaints/investigations; renewals; enforcement; billing; and the maintenance of historical information. Each CDPH program cited in this feasibility study carries out these functions.

A key aspect of this overall solution is the business process improvements (sometimes called reengineering). The importance of these process improvements can be seen by comparing the current program-specific, fragmented process flowcharts in Appendix D with the streamlined, common high-level process flow shown in Figure 7 above. The specific process improvements will be identified early in the implementation phases, through combined efforts of CDPH program staff (experts in the public health mission of their programs) as well as vendor staff (experts in the capabilities of their software and the uses derived by prior similar clients), all under the close oversight of CDPH executive leadership and 3rd-party oversight vendors.

In this business-based procurement, CDPH seeks a solution which would eliminate all five programs' utilization of all systems detailed in Section 3.1.2, depending on vendor solution functionality to be identified during the procurement phase.

In addition to meeting CDPH Program requirements, the envisioned solution will operate in a manner consistent with CDPH's current regulatory and policy structure; will be scalable to accommodate potential future expansion within CDPH; and will comply with the standards defined by the State of California's Department of Technology Services (DTS). The test/training and production servers will reside at the State's Department of Technology Services (DTS) and the development server will reside at the CDPH facility.

The proposed solution will enable the following levels of user access:

- CDPH professional access (read/write)
- CDPH read-only access
- Customer-access (secure for submitting information, renewals, etc.)
- Public read-only access

The proposed solution will provide CDPH with the ability to maintain licensing, enforcement, and billing data in a central repository and effectively manage the associated workflows.

CDPH users will access the proposed solution through the existing DTS and CDPH wide area network (WAN) and local area network (LAN) network infrastructure. The regional offices will access the proposed solution via the existing DTS and CDPH secure websites.

The customer access will provide a secure Internet site whereby authenticated customers will be able to apply for a new license, submit renewals or changes related to an existing license, submit payments, and review their license and billing data.

The public access will enable the public to query on and view non-confidential information via the Internet. A web portal component will be integrated with CDPH's existing portal on CDPH public website; however, the search engine will be much more robust, and non-confidential license data for all programs participating in this solution will be available.

Figure 8 provides a conceptual view of the proposed solution. Please note that this is a conceptual view, and the actual solution will conform to all applicable standards.

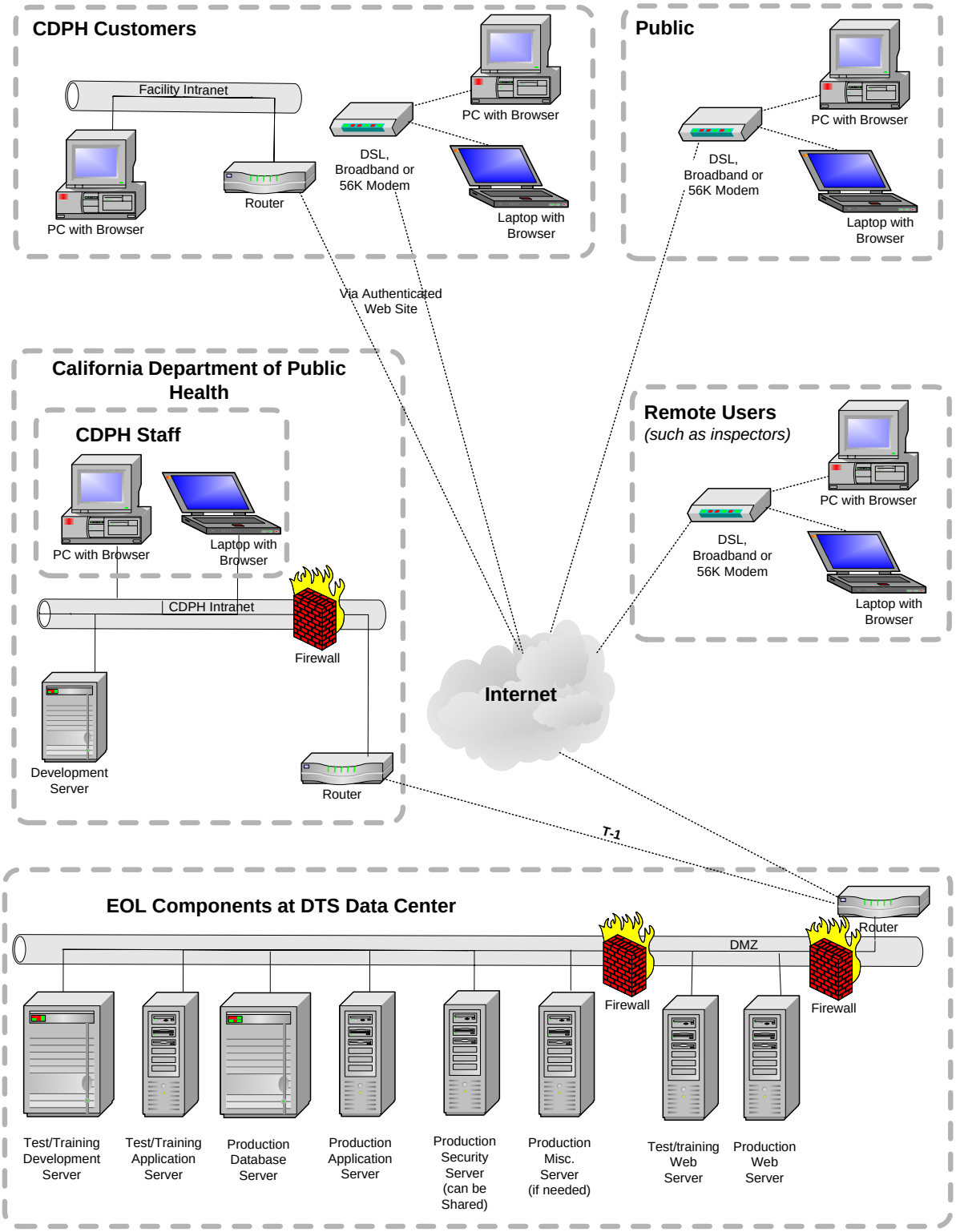


Figure 8: EOL Conceptual View

5.1.1 Proposed Hardware

The following section describes the proposed hardware required for the business-based procurement solution, to be refined through the competitive procurement process.

The proposed solution is expected to leverage CDPH's current investment in desktop configuration, printers, network and communications hardware. The current standard desktop configuration for CDPH users is an HP/Compaq model DC7700 or Gateway model E4610D desktop PC with Microsoft's Windows XP Professional 2002 and Office 2003 software. CDPH currently has a sufficient number of printers and will utilize them as part of the proposed solution.

The EOL development server will reside at CDPH/ITSD allowing CDPH IT staff and vendor easier access to the development environment and more flexibility in making ongoing configuration changes. The development server will be partitioned to simulate a three-tier architecture. The EOL test/training and production servers would reside at the DTS Gold Campus Data Center. The test-training environment will also be partitioned to serve as a staging environment. The proposed solution will require the purchase of web, database, and application servers for the development, test/training, and production environments. To allow for CDPH's evolving environment at DTS (e.g., establishment of CDPH security servers), an additional server is included in the costing of this proposed solution. If the additional hardware is needed, it will conform to the DTS and CDPH platform currently supported. The proposed solution will also utilize the existing DTS and CDPH WAN and LAN network infrastructure.

Table 4 describes CDPH's current hardware configuration standards. These represent a guideline for vendors; exceptions where necessary can be authorized by the CDPH CIO. The full set of hardware and software standards is provided in Appendix C.

Table 4: Current Standards (Proposed Minimum EOL Hardware Configuration)

Category	Description
Server Type	Dual Core processor
Operating System	Microsoft Windows Server 2003 SP1 (or R2 SP2)
Processor	Minimum of 3.0 GHz each
RAM Memory	2 GB SDRAM or 4 GB SDRAM
Controller	PERC 4e/Di disk controller RAID 5 Minimum of 128 MB Battery Backup Write and Read Cache (BBWC)
Storage	64 GB Internal Hard Drive Three 36/72 GB pluggable Ultra-SCSI hard drives, or five 36/72 ultra SCSI hard drives for a Raid 5 + 1 hot spare configuration

Category	Description
Network Interface Card	Dual 10/100/1000 MBPS network interface cards
Power Supplies	Redundant hot plug power supplies
Fans	Redundant cooling fans

5.1.2 Proposed Software

The following section describes the proposed software required for the business-based procurement solution. This software solution will be refined through the competitive procurement process.

The proposed solution will result in the implementation of an off-the-shelf software product that provides comprehensive licensing, enforcement, and billing functions and meets all of CDPH's business needs identified in Section 3: Business Case. Both commercial off-the-shelf (COTS) and modifiable off-the-shelf (MOTS) solutions are available which incorporate current industry practices and have been successfully implemented in other organizations, reducing risk to the State. Many available the off-the-shelf packaged solutions can work with add-on software products such as geographic information systems, which interface with the core database and application structure. An off-the-shelf software product solution is scalable and would enable future expansion.

As part of FSR development, CDPH conducted a market study, as follows: Several off-the-shelf products were identified which could potentially meet CDPH's business need, based on current knowledge, research, and discussions with other customers both within the State of California government and other regulatory bodies outside California. These solutions can each be implemented in phases, further reducing project risk. Table 5 lists the market vendors of applicable solutions identified.

Table 5: Potential Off-the-Shelf Solutions

Vendor Solution	Package Type
Vendor Solution A (name redacted)	MOTS
Vendor Solution B (name redacted)	COTS/MOTS
Vendor Solution C (name redacted)	MOTS
Vendor Solution D (name redacted)	MOTS
Vendor Solution E (name redacted)	MOTS
Vendor Solution F (name redacted)	MOTS
Vendor Solution G (name redacted)	COTS/MOTS

CDPH anticipates that the full procurement process, to be conducted in a fully-competitive environment, will quite possibly result in discovery of other potential off-the-

shelf vendor solutions beyond the seven vendor solutions discovered as part of this preliminary market study.

5.1.3 Proposed Technical Platform

EOL is expected to be a three-tiered, web-enabled solution that will use a web server, database server, and application server, in accordance to CDPH and DTS standards. The test/training and production environment will be located at the DTS Gold Campus Data Center in Rancho Cordova, California. The development environment will be located at the CDPH East End Complex in Sacramento, California. The servers will adhere to the State standards for security, firewall, password authentication, hardware, software, and web.

The CDPH users will access the proposed solution through their existing DTS and CDPH WAN and LAN network infrastructure. The regional offices will access the proposed solution through the existing DTS and CDPH secure user authenticated websites. The CDPH customers of the proposed solution will be able to access the system through the public Internet, but via a secure portal that will require a login authentication. The public will access non-confidential data via the public Internet.

Table 6 identifies the current network protocol standards. As described above, CDPH's CIO can authorize exceptions where warranted, thus providing flexibility to accommodate vendor solutions that may be appropriate.

Table 6: Current Standards (Proposed EOL Network Protocols)

Type	Description
Transmission Control Protocol/Internet Protocol (TCP/IP)	Used to connect the EOL host environment to the Internet
Secure Sockets Layer (SSL)	Used to manage the security of file and message transmissions from the Internet to the EOL environment
Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)	Used to transmit individual data messages securely over the Internet through encryption/decryption Used to transmit user's EOL User ID and password to gain access to the EOL environment
SSH Transfer Protocol (SFTP)	Used to exchange files between EOL and other servers/systems in a secure manner (if needed)

5.1.4 Development Approach

The Systems Integration vendor will be responsible for all software and database configurations required to implement the EOL off-the-shelf solution. The proposed development approach and methodology will be submitted by potential Systems Integration vendors during the procurement phase. The proposed approach and methodology must adhere to standards defined by the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK) and the Statewide Information

Management Manual (SIMM), as well as applicable standards defined by the Institute of Electrical and Electronics Engineers (IEEE). CDPH will retain the roles described in Section 6, including proper governance, oversight, and direct participation of subject matter experts.

5.1.5 Data Migration/Integration Issues

A variety of data will be migrated into the new system from CDPH's existing systems, including databases in ADABAS, Filemaker, Clipper, Focus, MS Access, MS Excel, and other miscellaneous tools that are used by CDPH. Table 7 identifies the CDPH sources for data to migrate. Data maintained in a variety of miscellaneous stand-alone spreadsheets, not listed in this table, may also be migrated.

Table 7: Data Sources for Migration/Integration

Data Source
▪ Health Application Licensing (HAL) System
▪ Food Inspection Activity Tracking
▪ California Mammography Information System (CAMIS)
▪ Various MS Access 2003 databases (FDB, Radiation Safety)
▪ Permits, Inspections, Compliance Monitoring & Enforcement (PICME)
▪ Permits Tracking
▪ Operator Certification Database
▪ Miscellaneous MS Access and MS Excel tools

Note: This table refers to data in the respective systems, not the systems themselves.

The major tasks associated with data migration are as follows:

Data Cleansing

CDPH's existing systems, databases, and spreadsheets contain data that are redundant, incomplete, formatted incorrectly, or out of date. Data cleansing activities will be used to detect and correct any inconsistent data before the data can be migrated to EOL. If the business rules can be defined, automated data cleansing processes can be used; in some cases, involvement of CDPH subject matter experts may also be required to assist in examining some data for cleansing.

Reconciliation of Inconsistent Data

CDPH has identified certain inconsistencies among data across the systems. CDPH's staff will identify which data is the most accurate to prevent inaccurate data from being migrated to the proposed solution. CDPH will establish a process to handle any data exceptions through automation or manual reconciliation.

Repair of Incomplete Data

CDPH's current systems do not contain sufficient edits to ensure that data are correctly saved into the databases for a license or payment. The lack of proper edits results in

incomplete data. It is anticipated that CDPH's staff will determine whether incomplete data should be manually entered into the new system or if they would prefer to do manual cleanup of the data in the current system before any data migration will be able to occur. CDPH's staff will define procedures to resolve this issue. Once the data has been reviewed and corrected, it will be considered as part of the data migration to the proposed solution.

Data Migration

CDPH's data migration process will convert data from different formats (including ADABAS, FileMaker, Clipper, etc.) to the proposed solution's data format. To enable successful data migration from one system to another, it is anticipated that CDPH's staff will be required to assist in the definition of the data mapping rules and data relationships to enable the data migration process to be completed. It is also anticipated that CDPH's staff will be required to assist in establishing a process that will handle any data exceptions through automation or manual reconciliation. CDPH's staff will also be required to define which data and how much historical data will be migrated.

The Systems Integration vendor is responsible for conducting the data migration and integration effort. During the systems design activities, the vendor will develop a detailed Data Cleansing and Conversion Plan. At a minimum, the Data Cleansing and Conversion Plan must address the following:

- Migrate sufficient data to enable on-line application processing.
- Migrate sufficient data to enable on-line license renewals.
- Identify opportunities for automated data conversion (i.e., script).
- Identify where manual data conversion is necessary and the participants.
- Define data clean-up tasks that must occur to enable data migration.
- Define a validation approach to confirm data accuracy prior to migration.

Data Integration

Specific external systems with which the EOL system will interoperate are described in Section 5.1.7 below.

5.1.6 Procurement Approach

CDPH will procure a variety of products and services as part of the EOL project. The project will use procurement methods approved by the Department of General Services (DGS), including the California Multiple Award Schedules (CMAS) or Master Services Agreement (MSA) for service less than $1,500,000 and the traditional procurement (via RFP) process for services greater than $1,500,000.

Table 8 identifies the products or services that will be procured and the planned procurement method. Additional information regarding the procurement approach is provided in Section 6, Project Management Plan of this document, and in the Information Technology Procurement Plan (ITPP) Section 3, Acquisition Methodology.

Table 8: Products and Services to Procure

Product/Service and Description	Expected Range	Expected Procurement Method
Acquisition Services: Responsible for development of the solicitation document required to solicit the Systems Integrator	< $ 500,000	CMAS
Project Management Services: Responsible for the overall management of the EOL project and coordinating and overseeing project activities performed by vendors, as well as by CDPH and DTS	< $1,500,000	CMAS or MSA
Project Oversight Services – Independent Project Oversight Contractor (IPOC): Responsible for ensuring that the project is managed according to defined State and industry standards and best practices.)	< $1,500,000	CMAS or MSA
Project Oversight Services – Independent Verification and Validation (IV&V): Responsible for monitoring the EOL project to ensure that products conform to RFP requirements (verification) and that they satisfy the intended user needs (validation)	< $1,500,000	CMAS or MSA
Systems Integration (including software): Responsible for all aspects of the EOL development, test/training and production environments including, but not limited to, software, configurations, data migration, reports, training, documentation, implementation and ongoing support via a maintenance contract	> $1,500,000	Traditional (RFP) business-based

Procurement of Acquisition Services

Vendors selected to perform acquisition services cannot bid on any of the remaining procurements. The approach to procuring acquisition services includes:

- Planning and Project Management Branch (PPMB) Planning and Oversight Section (POS) will develop a solicitation document.
- PPMB will distribute the solicitation document to a minimum of ten qualified vendors, including a minimum of two small and/or Disabled Veteran Business Enterprise (DVBE) businesses.
- Bidders will be required to submit a proposal and may be required to participate

in an interview process.

- PPMB will work collaboratively with CDPH to establish an evaluation and selection team consisting of CDPH project management (program and technology services), and ITSD staff as appropriate.
- PPMB, in consultation with CDPH project management, will select the winning bidder and award the contract based on applicable rules.

Procurement of IPOC Services

The procurement of IPOC services will be separate and distinct from the other procurements. The Vendor selected to perform this service cannot bid on any of the remaining procurements. The procurement approach includes:

- Planning and Project Management Branch (PPMB) Planning and Oversight Section (POS) will develop a solicitation document.
- PPMB will distribute the solicitation document to a minimum of ten MSA-qualified vendors, including a minimum of two small and/or Disabled Veteran Business Enterprise (DVBE) businesses if available.
- Bidders will be required to submit a proposal and may be required to participate in an interview process.
- CDPH will establish an evaluation and selection team consisting of program, PPMB, and other ITSD staff as appropriate.
- PPMB, in consultation with CDPH project management, will select the winning bidder and award the contract based on applicable rules.

Procurement of IV&V Services

The procurement of IV&V services will be separate and distinct from the other procurements. The Vendor selected to perform this service cannot bid on any of the remaining procurements. The procurement approach includes:

- Planning and Project Management Branch (PPMB) Planning and Oversight Section (POS) will develop a solicitation document.
- PPMB will distribute the solicitation document to a minimum of ten MSA-qualified vendors, including a minimum of two small and/or Disabled Veteran Business Enterprise (DVBE) businesses if available.
- Bidders will be required to submit a proposal and may be required to participate in an interview process.
- CDPH will establish an evaluation and selection team consisting of program, PPMB, and other ITSD staff as appropriate.
- PPMB, in consultation with CDPH project management, will select the winning bidder and award the contract based on applicable rules.

Procurement of Project Management Services

The procurement of Project Management services will be separate and distinct from the other procurements. The Vendor selected to perform this service cannot bid on any of the remaining procurements. The procurement approach includes:

- Planning and Project Management Branch (PPMB) Planning and Oversight Section (POS) will develop a solicitation document.
- PPMB will distribute the solicitation document to a minimum of ten MSA-qualified vendors, including a minimum of two small and/or Disabled Veteran Business Enterprise (DVBE) businesses if available.
- Bidders will be required to submit a proposal and may be required to participate in an interview process.
- CDPH will establish an evaluation and selection team consisting of program, PPMB, and other ITSD staff as appropriate.
- PPMB, in consultation with CDPH project management, will select the winning bidder and award the contract based on applicable rules.

Procurement of Systems Integration Services

The System Integration vendor will provide both software and services, requiring a single “prime” vendor with the potential for subcontracted vendors. The procurement of System Integration services will be separate and distinct from the other procurements. Vendors selected to perform this service cannot bid on any of the other procurements.

The approach for each of these procurements includes:

- The Acquisition Services vendor, retained by CDPH, will develop a Request For Proposals (RFP) solicitation document, and any related required documents, that will follow approved methodologies for protecting the State’s investment and to satisfy the specific needs of the State’s procurement process. The RFP will be approved by PPMB and DGS.
- DGS, on behalf of CDPH, will publish the RFP in the California State Contracts Register and any other appropriate channels.
- CDPH will conduct a Bidder’s Conference, in accordance with the standards defined by DGS.
- After the distribution of the RFP, vendors will be provided the opportunity to submit questions to CDPH. This will help increase the chance for vendors to submit responsive proposals.
- The procurement process will consist of two phases. The first phase is the submission of a draft proposal that enables CDPH to assess bidders and further clarify CDPH’s needs and the vendor’s proposed approach. The second phase will include submission of a final proposal
- Confidential discussions with the vendor may be conducted as part of the draft proposal submissions. If so, CDPH will develop and review with DGS evaluation

factors and values and communicate these to potential bidders within the solicitation document.

- CDPH will establish an evaluation and selection team consisting of CDPH program and CDPH technology support staff, as well as representatives of PPMB and DGS.
- CDPH will award a contract to the vendor whose solution meets the specifications of the RFP and provides the "best value" to the State. With guidance from the DGS, CDPH will follow all of the procurement processes and procedures to ensure compliance with the appropriate guidelines to conduct a competitive and fair procurement. Contract services will be procured using an agreed upon procurement vehicle/mechanism between DGS and CDPH, to ensure alignment with current procurement guidelines in place at that time.

5.1.7 Technical Interfaces

EOL will be required to interface to CDPH existing scanned document repositories. RHB will use a document scanning system to provide staff online access to issued licenses, registrations, and certificates and reduce the need to locate and rely on paper files to perform work functions. The software will be required to be installed as part of CDPH's standard desktop configuration for those needing to review the scanned licenses.

5.1.8 Testing Plan

The Systems Integration vendor, in coordination with CDPH, will be required to develop and administer a Testing Plan. The Testing Plan will include traceability to the functional requirements. At a minimum, the Testing Plan will address the following areas of testing:

Unit Testing

Unit testing is verification of the accuracy and completeness of the system's individual software modules, objects, functions, and procedures. Unit testing is performed by the development team.

System Testing

System testing is verification that the system components work together as designed as well as that the new system integrates seamlessly with existing systems and data stores. System testing is performed by the Systems Integration development team.

Performance/stress testing

Performance/stress testing is verification that the software and hardware operate together in a manner that meets the expected average and peak performance requirements. Performance/stress testing is dependent on scripting as test scripts mimic the expected production environment. Performance/stress testing is performed by the Systems Integration development team.

Regression Testing

Regression testing is verification that implementation of new modules or functionality does not adversely impact system components already deployed and in production. Regression testing is performed by the Systems Integration team and validated by designated users.

User Acceptance Testing

User acceptance testing is verification that the completed system operates in accordance with the system requirements based on a structured testing process. User acceptance testing is coordinated by the Systems Integration vendor and performed by designated users.

5.1.9 Resources Requirements

Table 9 identifies the CDPH resource requirements for this project.

Table 9: Proposed Solution – CDPH Resource Requirements

Role	One-Time Resource Requirements	Ongoing Resource Requirements
Governance Sponsor	Chief Deputy Director CDPH Operations	N/A
Executive Sponsor	Deputy Director Center for Environmental Health	N/A
EOL Project Director	Appointed by Deputy Director, Center for Environmental Health	N/A
PPMB/PMO Project Director	Center for Environmental Health	N/A
PPMB Oversight Contract Manager	ITSD PPMB	ITSD PMO (during maintenance period)
Infrastructure	ITSD DTS	ITSD DTS
Programmer (data conversion)	ITSD CDPH Programs (during data conversion) DTS	ITSD
Database Administration	ITSD CDPH Programs	ITSD
Help Desk	N/A	CDPH Programs

Role	One-Time Resource Requirements	Ongoing Resource Requirements
Business Subject Matter Experts (process improve-ments, requirements, data cleansing, data conversion)	CDPH Programs	N/A

5.1.10 Training Plan

The implementation of the new system will directly impact the business processes and tools used by CDPH staff. The Systems Integration vendor will be responsible for the development and execution of all training efforts. The vendor's proposed training approach and methodology will be included in the proposals submitted during the procurement phase. At a minimum, the training approach must include user and systems training. The vendor-provided classroom training will be available to all expected users. The selected Systems Integration vendor, in coordination with CDPH, will be required to develop a detailed Training Plan during the Design phase of the project.

At a minimum, the Training Plan must include the following information:

- Types of training (e.g., technical, business, etc.)
- Format of training (e.g., classroom, web-based, etc.)
- Target participants
- Location of training
- Training materials
- Frequency of training

The Training Plan must also address any training that would be necessary for licensees or other external parties – for example, how to submit a renewal application. This training could be fulfilled by online help and/or tutorials, as appropriate to the task.

5.1.11 Ongoing Maintenance

Hardware Maintenance

DTS would host and support all the test/training and production servers and WAN network infrastructure, including any required maintenance and infrastructure upgrades. CDPH would host and support the development server, as well as the LAN. Certain hardware and software components of the solution may include maintenance contracts with the appropriate vendors. An agreement between DTS and ITSD will be used for clearly defining expectations and responsibilities between them.

Software Maintenance

Under a software maintenance and support contract, the Systems Integration vendor would provide EOL maintenance for two years following the cutover date of the final implementation phase, with an option to renew for two subsequent years. Upon

conclusion of the maintenance and support agreement, CDPH Program IT staff and ITSD would be responsible for any maintenance tasks. During the vendor maintenance period, CDPH Program IT staff would be responsible for quality assurance; participate in knowledge transfer sessions and code reviews; assist with testing, and deployments; maintain user security; develop and maintain standard and ad hoc reports; and serve as level one help desk. Before the end of the vendor maintenance period, the vendor must provide all documentation and training to turn over support smoothly to CDPH staff. An agreement between DTS and ITSD will be used for clearly defining expectations and responsibilities between them.

5.1.12 Information Security

CDPH's current systems have limited security restrictions. The CDPH Information Security Officer (ISO) has been involved in this project's definition of security requirements and supporting infrastructure and will continue this involvement to carefully define EOL security controls. Appendix B: CDPH Information Security Standards, SR-1 provides the basis for this definition.

The proposed solution's information security environment will conform to the DTS, CDPH, and State of California security policies and standards. The CDPH ISO will oversee the definition of EOL system security. Security components will be implemented at both a system-wide and at a user-level.

CDPH will define the level of security access they require for the data stored in the proposed solution. CDPH's staff will require security access roles to be defined that will be aligned with their data access needs. Many of CDPH's core systems, MS Access databases, and other tools contain private information that will be reviewed against State and CDPH privacy and confidentiality guidelines. CDPH's staff will determine which security access roles will have access to create, update, and view this data.

System-wide security elements will include:

- Compliance with www.ca.gov portal standards.
- Secure Sockets Layer (SSL) encryption to encrypt data transactions that include personal and credit card information.
- Physical access to server and network equipment at DTS is restricted and is only accessible through card key access by authorized staff.
- All logical access to EOL information will be through system and application-level security, and will utilize group policy objects for security administration.
- Data ownership group policy objects to authorize user access to specific data elements on a need-to-know basis only. This will prevent unauthorized users from creating, reading, updating, or deleting sensitive EOL data for which they are not primarily responsible.
- HTTPS will be used for accessing a secure Web server.
- Implement an "n-tier" architecture that provides secure zones for each tier (or layer) of the application including the database, application, and presentation

layers. Communication between each of the layers will be via secure protocols.

Where applicable, security will limit access based on an authorized User ID and password, as well as security roles. At a minimum, the following security control access features will be implemented:

- Forced log-off of inactive users.
- Termination of a user's session after unsuccessful logon attempts.
- Locking of a user's master record after repeated failed logon attempts.
- Expiration of passwords after a specified period.
- Required password changes at regular intervals.
- Minimum password lengths.
- Prohibited use of certain passwords, such as using the same character string for the user log on and password.
- EOL will be required to provide a unique user name and strong password for secure user authentication in a role based security model.

In addition, the solution will comply with the Payment Card Industry (PCI) Data Security Standard (current version is 1.1, released September 2006), as applicable to the electronic payment component of the solution.

5.1.13 Confidentiality

As described previously, the proposed solution's information security environment will conform to the DTS, CDPH, and State of California security policies and standards. The CDPH ISO will oversee all aspects of data confidentiality during the EOL project (for example, details of pending investigations of alleged violations, or data on specific inspection results which may not be public record).

CDPH's current expectation is that no Health Insurance Portability & Accountability Act of 1996 (HIPAA) protected health information (PHI) will be included in the EOL database. In the event that CDPH discovers that any data to be included is in fact PHI, role-based security will ensure that only authorized CDPH staff have access to this information. The ISO will be involved to assure adherence to all applicable Federal HIPAA and State privacy and security statutes.

For data requiring safeguards, EOL will use Secure Socket Layer (SSL) 128-bit encryption and server validation via registered server certificates retained by DTS (i.e., VeriSign certificates). Sensitive data will be encrypted.

5.1.14 Impact on End Users

The new EOL system will provide end-users within CDPH the ability to better carry out responsibilities for minimizing health and safety risks to California residents.

Current CDPH licensing systems are problematic. Among the many challenges:

- Systems built on outdated technology and are not designed to meet the current business requirements.
- Systems do not support CDPH ability to adequately address some regulatory and legislative requirements in a timely manner.
- Systems do not provide staff with the tools to efficiently respond to incidents/emergencies.
- Many systems face high risk as technical support resources for outdated technologies become unavailable.

The proposed EOL solution technologies will alleviate these operational challenges and obstacles within the department. EOL will significantly impact the manner in which most of CDPH's staff performs their functions by automating many processes, eliminating manual work steps, and eliminating stand-alone worksheets and databases. Additionally, a new system will benefit all Californians by providing improved tools for CDPH to respond to incidents or emergencies.

Today, CDPH operates in silos for many activities. This is driven by the lack of a central data repository and the lack of access to data. EOL will provide a central data repository and workflow system, improving CDPH's application, renewal, enforcement and payment processing. In addition, EOL will enable CDPH to expand its use of the Internet to facilitate business with its customers and its external stakeholders.

5.1.15 Impact on Existing Systems

As stated above, in this business-based procurement, CDPH will seek a solution to eliminate CDPH's utilization of nearly all systems detailed in Section 3.1.2. CDPH and the Systems Integration vendor will plan the phased decommission of all systems to be eliminated; these systems will continue operations until CDPH is ready to exclusively access EOL. ITSD and CDPH Program IT staff will continue to support systems planned for elimination until decommissioning.

5.1.16 Consistency with Overall Strategies

The proposed solution is aligned with the following state-wide, Executive Branch-wide, and department strategies.

Healthcare Improvement Initiative

In March 2007, the Governor issued Executive Order S-06-07 which was intended to move forward California's efforts to adopt health information technology, increase transparency of quality and pricing information, and increase accountability in public and private health care delivery systems. CDPH implementation of an enterprise-wide solution which provides data access and reporting capability directly supports the direction to increase public health accountability.

e-Government Initiative

In September 2000, the Governor issued Executive Order D-17-00 to implement electronic technologies that would allow the people of California to receive government

services and interact with State government. More recent State of the State addresses by that Governor and California's present Governor have continued to emphasize the commitment to providing on-line services. By offering web-based features for CDPH customers and the public, the proposed solution is further advancing the Governor's direction.

California Public Records Act

The California Legislature has stated that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state. The California Public Records Act, Government Code section 6250 and seq., requires that public records be available to the public upon request. By providing the ability for the public to verify licensee data and status, the proposed solution supports the public's right to know as required in the California Public Records Act.

California State Information Technology Strategic Plan

This plan includes the objective to operate as a seamless enterprise, delivering consistent, cost effective, efficient, reliable, accessible and secure services that satisfy the needs of its diverse public and private customers. By operating on scalable, current technology and streamlining processing to leverage the features and functionality offered by the proposed solution, EOL is aligned with California's information technology strategic direction. The proposed system also directly aligns with the State's IT Strategic Plan, Goal # 2 which states, "Implement common business applications and systems to improve efficiency and cost-effectiveness."

Cal-SOA Vision

Consistent with the overall IT Strategic Plan cited above, and as mentioned at the outset of this section, the EOL solution is aligned with the Cal-SOA Vision articulated by the state's Chief Information Officer and Enterprise Leadership Council, by making use of the simple, stated principle "build once, use often" and providing the resulting system as an available solution for other departments with similar functions of licensing, registration, and certification.

Strategic Plan Alignment

The proposed solution is aligned with the most recent published departmental strategic plan, by enabling CDPH to meet several strategic goals including enhancing programs, services, and communications with current and emerging technology; consolidating, coordinating, and integrating CDPH programs; ensuring easy access to information; improving business practices; and implementing information technology and Internet-based systems to support business process and transactions.

5.1.17 Impact on IT Infrastructure

The business-based procurement will identify infrastructure requirements for the new EOL system and related impacts. The current expectation is that these requirements will be based on vendor specific characteristics. It is unknown whether DTS may offer a Customer Owned Equipment Management Service (COEMS) offering at the time of the implementation. If so, the pricing of such an offering might be attractive to CDPH. After

the implementation, the System Integration vendor will be responsible for providing maintenance and support for at least one full year following the implementation date, with an add-on option of two additional years.

5.1.18 Data Center Consolidation

In accordance with current State of California strategy, the test/training and production environments of the proposed solution will reside at the State's DTS Gold Campus Data Center located in Rancho Cordova, California.

5.1.19 Impact on Data Center

The proposed solution will comply with the hardware, software, network, and security standards defined by DTS. DTS has the necessary infrastructure and support required to provide comprehensive 24x7 services. In addition, housing the EOL test/training and production environments at DTS and providing one full year of maintenance by the Systems Integration vendor, with an option for two additional years of maintenance, will allow CDPH to reduce its risk by transitioning to state IT support in a controlled timeline.

DTS services to be provided for EOL include:

- Hardware procurement, installation and maintenance for test/training and production servers.
- Software procurement, installation, and maintenance for test/training and production servers (operating system, system utilities, databases, and web software).
- Performance monitoring and alerting.
- Secure network connectivity.
- Environmentally controlled and secure facility.
- Reliable power supply with full uninterruptible power supply (UPS) and generator backup.
- System backup, recovery, and off-site storage.
- Security systems, including virus protection, data encryption, and intrusion detection.
- Internet protocol (IP) addresses and domain name system (DNS) registration.
- Restricted file transfer protocol (FTP) access for content management.

The Systems Integration vendor, working with CDPH and DTS will determine the data back-up cycles, archiving standards, and operational recovery of the system in the event of a disaster. Costs associated with DTS services are included in the ongoing operation and maintenance cost detailed in Section 8.0: Economic Analysis Worksheet.

5.1.20 Backup and Operational Recovery

The new system will adhere to the backup and operational recovery requirements identified by CDPH and DTS. Specific procedures related to backup and operational

recovery will be further addressed by the Systems Integration vendor in the EOL Operational Recovery Plan (ORP). The EOL ORP will be developed in accordance with State Administrative Manual (SAM) Section 4843, Operational Recovery Planning and at a minimum include the information identified in the Department of Finance Operational Recovery Plan Documentation for Agencies Preparation Instructions, SIMM Form 65A.

The EOL test/training and production environment will reside at the DTS and will comply with the existing standards defined and services offered by DTS.

5.1.21 Public Access

With the proposed solution, the public will be able to review non-confidential license data through various on-line search functions on CDPH Program websites. Data will include basic licensee name (when applicable), license status, license expiration date, and date license was first issued. No confidential information will be made available to the public.

Authenticated CDPH customers will be able to review their license information through a secure portal via the Internet. In addition, authenticated customers will be able to submit applications, license change requests, address changes, license renewal data, and make payments through a secure web portal.

5.1.22 Costs and Benefits

Costs

The expected costs of the EOL project include one-time costs of approximately $5 – 6 million and continuing annual costs of approximately $0.4 – 0.5 million before savings to be realized (plus continuing existing annual costs of approximately $0.5 million).

Table 10 summarizes the estimated total costs for the proposed solution. Detailed information regarding cost is provided in Section 8.0: Economic Analysis Worksheets.

Table 10: Proposed Solution – Estimated Cost

Estimated One-Time New Costs	Estimated Annual New Costs
Approximately $ 5 – 6 million	Approximately $ 0.4 – 0.5 million

Benefits

The overall anticipated benefits of EOL include:

- Reduced health and safety risks for Californians.
- Reduced burdens placed on companies, individuals, and other regulated entities.
- Greater ability to respond to emergencies, terrorist incidents, or other public health threats.

- Greater level of service provided by the state government to constituencies.
- Improved internal efficiencies of State of California operations.
- Reduced risk of internal challenges (system outages, malfunctions) and external challenges (loss of income by professionals, media exposure, litigation).
- Compliance with Governor's and CDPH's initiatives to provide on-line services in the State.
- Ability for CDPH to better meet legislative and other requirements.
- Replacement of outdated technologies in the participating programs with new technologies designed to meet current business requirements.
- Single data repository that contains license, enforcement and billing data for 100% of all CDPH programs.
- Ability to provide statistical data to internal and external stakeholders demonstrating CDPH's accountability.
- Elimination of duplicate data entry.
- Improved data quality.
- Elimination of silo, stand-alone "systems".
- Reduction of paper documents (receipt, processing, storage, retrieval).
- Automated generation of billing notices.
- Reduction in processing time.
- Ability to offer customers online access to their data and electronic payment via the Internet.
- Public access to non-confidential license data via the Internet.
- Reduction of risk due to lack of technicians knowledgeable in outdated technologies.

As for the strictly financial benefits, above and beyond the public health and safety benefits, the five programs combined have estimated net cost savings greater than $900,000 per year due to elimination of much of the workload currently being expended on the manual, time-intensive processes cited in this report. This is net savings, after considering the redirection of the $0.5 million per year, cited above.

These savings would more than offset the ongoing annual costs of the new system, cited above.

Table 11 identifies the estimated financial benefits expected as a result of the proposed solution:

Table 11: Proposed Solution – Estimated Financial Benefits (Per Fiscal Year)

Program and Category	Estimated New Revenue	Estimated Annual Savings
Food and Drug Program	$0	$295,831
Radiation Safety Program	$0	$550,785
Drinking Water Operator Certification Program	$0	$8,411
Safe Drinking Water Systems	$0	$29,635
Medical Waste Management Program	$0	$19,338
Total Annual Estimated Financial Benefits	**$0**	**$904,000**

5.2 Rationale for Selection

Three potential solutions were evaluated for the EOL project. These were:

- Off-the-Shelf Software Product.
- Custom-Developed Software Solution.
- Modify the e-Licensing Management System (ELMS) currently in use in a different program within CDPH (not one of the programs participating in this EOL solution).

The off-the-shelf packaged solution was selected for the following reasons:

- Addresses the business problems and functional requirements identified in FSR Section 3: Business Case.
- Enables future scalability and a phased deployment.
- Leverages best practices already incorporated in the software through other customers with the same or similar missions (i.e. public health agencies).
- Reduces system development time and cost.
- Aligns with the State's and CDPH' strategic directions.
- Reduces risk to the State by making the Systems Integration vendor fully responsible for the software environment.
- Reduces project risk because the proposed solution has been successfully implemented in other government licensing agencies.
- Reduces risk associated with organizational changes to ITSD that may result from the CDPH reorganization.
- Allows CDPH to leverage existing off-the-shelf packaged interfaces to third-party adjunct software (e.g. report writer, GIS, etc.).

Upon completion of the alternative analysis, each alternative was compared against each other within the context of eight criteria. Each alternative was assigned a rank, from one to three, based on how well the alternative met the criteria. Table 12 indicates

that the proposed solution ranked best for most of the criteria individually, and by far the best overall.

Legend
3 = Best addresses the criterion 2 = Neither best nor worst 1 = Worst solution for this criterion

Table 12: Alternatives Considered Comparison

Criteria	Proposed Solution	Alternative 1	Alternative 2
	Off-the-Shelf Software Package	Custom-Developed Software	Modify ELMS for All Programs
Meets Business Objectives	3	2	1
Functional Requirements	2	3	1
Project Risk	3	1	2
Technical Risk	3	2	1
One-Time Development Costs	3	2	1
On-Going Costs	3	1	2
Schedule	3	2	1
Alignment with Strategic Direction	3	2	1
Total	**23**	**15**	**10**

5.3 Other Alternatives Considered

This section provides information on the other alternative solutions considered, but not selected.

5.3.1 Alternative 1: Custom-Developed Software Solution

This alternative would create a new web-based solution that adheres to DTS and CDPH technology standards. The solution would be developed specifically to meet CDPH's identified business needs by providing licensing, enforcement, and billing modules for back office processing; a secure Internet module for use by CDPH's customers; and an Internet portal for queries by the public.

A custom solution would require CDPH to design a new system from a blank sheet. This solution would be fully customized to CDPH's operations and processes and may not

prove to be usable or scalable for future CDPH needs and other CDPH programs. CDPH has not implemented a custom system solution and is not knowledgeable of the software development process or best practices. It would require a greatly extended timeframe from CDPH staff to participate in the development of a custom solution. Overall project risk would be much higher.

Advantages and Disadvantages

Table 13 identifies the advantages and disadvantages with Alternative 1:

Table 13: Alternative 1 – Advantages and Disadvantages

Advantages	Disadvantages
▪ Development of screens and process flows customized to meet CDPH's needs ▪ Fully meets all of CDPH's functional requirements ▪ Complies with DTS and CDPH technology standards	▪ More costly than off-the-shelf packaged solution ▪ Longer implementation timeframe; longer time before savings are realized ▪ Increased risk due to vendor's reliance on CDPH for information to design the system; CDPH is not knowledgeable of software development best practices and standards ▪ Does not encourage CDPH to streamline and standardize business processes using industry best practices ▪ Involves greater amount of CDPH staff time ▪ Limits scalability for use by other CDPH organizations ▪ Limits flexibility to address future legislative changes for CDPH and future CDPH needs ▪ Increased risk of project failure

Conclusion

This alternative was not selected due to the project risks of a first time implementation, the probability of not being delivered on time or on budget, the inability to leverage best practices, the amount of CDPH program staff time that would be required to design the system, and the potential for limited scalability and flexibility to satisfy future CDPH needs.

5.3.2 Alternative 2: Modify ELMS

In 2004, CDPH's Licensing and Certification (L&C) unit implemented a custom-developed solution to track healthcare facility licenses and citations. The eLicensing Management System (ELMS) was developed using Microsoft's .NET with an Oracle database management system on a single server at CDPH. Today, L&C uses ELMS to track licenses and citations issued against the licensees.

ELMS is used for back-office license and citation tracking; however, it does not currently have a customer web-based module nor does it offer electronic payment processing. In addition, ELMS has limited enforcement data tracking capabilities. It currently does not

provide inspection, case management, or enforcement functionality. Essentially, ELMS contains less than 20% of the features and functionality required by the participating CDPH programs.

This alternative would modify ELMS to expand features and functionality to address CDPH's functional requirements and business needs. For example, modifications required would include the ability to manage licenses, certification, and registration related to people, machines, and schools - not just facilities; adding a billing and cashiering module; enhancing the enforcement module to meet CDPH's needs; adding a web-based module for use by CDPH's customers and the public; adding a sophisticated report writing tool; and providing the ability to interface to a scanning system and GIS.

Advantages and Disadvantages

Table 14 identifies the advantages and disadvantages with Alternative 2:

Table 14: Alternative 2 – Advantages and Disadvantages

Advantages	Disadvantages
▪ Provides a foundation for CDPH licensing functionality ▪ Leverages CDPH's prior IT investment	▪ Significant investment required to modify ELMS to meet functional requirements of the other programs ▪ ELMS does not currently interface with any adjunct software that CDPH requires (GIS, ePay, scanning system, etc.); interfaces are costly to develop ▪ Restricted to the database structure which was established to track only facilities ▪ Does not conform to DOF's requirement that production environments reside at a state data center ▪ ELMS architecture is not a three-tier solution and lacks hardware required for an enterprise solution ▪ Increased risk to L&C since CDPH will need to modify their system to expand functionality
	▪ Increased risks due to the potential that a competitive procurement would result in a new vendor (not the vendor that developed ELMS) being retained to update ELMS

Conclusion

This alternative was not selected due to the limited ability of ELMS to meet the various programs' needs, risks associated with significant modification or add-on modules required to meet CDPH's needs, higher costs than the proposed solution, non-compliance with DOF's direction for location of system production environment at State data centers, and the lack of required infrastructure.

Overall Conclusion

The proposed Enterprise-wide solution envisioned by CDPH directly addresses the Enterprise Leadership Council and State CIO's collaborative Cal-SOA approach to technology. This solution as described in this FSR will create an available "cost-effective, flexible application […] in [a] centrally hosted environment" that will "serve common functions and data management needs across the Executive Branch."[7] The solution makes use of the simple, stated principle "build once, use often" that underlies the Cal-SOA approach.

As stated in the Cal-SOA vision, "[i]f we courageously seize the opportunity presented by this massive refresh in our technology infrastructure and business and program applications, we can build a much more responsive, flexible and cost-effective set of systems. If we shrink back from this opportunity, fearful of the changes that will be necessary to develop a meaningful Cal-SOA, we will once again build a series of siloed applications and databases that frustrate efforts to share information and leverage services across the Executive Branch and increase development maintenance costs for individual projects."[8]

CDPH believes that the approach in this FSR directly addresses this imperative by making available a solution for a common business function (licensing, registration, and certification) that can be used by other departments across the Executive Branch.

[7] Op. cit. p. 2.

[8] Op. cit. p. 3.

6.0 PROJECT MANAGEMENT PLAN

The California Department of Public Health, in preparation to undertake an enterprise-level project, recognizes that not only a structured approach to project management is needed to ensure the successful implementation of the proposed solution. The project complexity, and the involvement of multiple CDPH programs and associated stakeholders, will also require consistent executive-level involvement and support, as well as regular and broad communication activities. This document provides an overview of how the Center for Environmental Health Enterprise-wide On-Line Licensing System project will accomplish this programmatic coordination and communication, and overall project management.

Following project approval, the CDPH Information Technology Services Division (ITSD) Planning and Project Management Branch (PPMB) Project Management Office (PMO) will work with CDPH program representatives and the selected project management vendor to develop a Project Management Plan (PMP) that addresses the project schedule, scope, budget, quality, change and issue management, project roles and responsibilities, human resources management, cross-program communications, and risk management. The PMP will be aligned with the Department of Finance's (DOF) Information Technology Project Management Methodology included in the State Information Management Manual (SIMM), as well as the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK).

The remainder of this section is organized as follows:

6.1 Project Manager Qualifications

A qualified and experienced Project Manager is critical to the success of any project. CDPH will assign a PPMB Project Director to work with a procured and qualified contract Project Manager and supporting team. The EOL project requirements for a contract Project Manager include the following minimum qualifications and experience:

- Project Management Professional (PMP) certification from the PMI or equivalent.
- At least five years experience in information technology (IT) project management,

using structured project management techniques and practices, including structured risk management.

- Knowledge and experience in project management concepts and techniques including, but not limited to, communications, change management, issues management, risk management, quality management, schedule management, scope management, configuration management, contract management, procurement management, and cost management.
- At least two years experience with the State of California's procurement and reporting processes working with the State's control agencies.
- At least three years experience in developing collaborative relationships with various project stakeholders, including state control agencies.
- At least five years experience with System Development Life Cycle (SDLC).
- At least five years experience with identifying and documenting business and system requirements.
- Successful coordination of and communication between project teams consisting of both state and vendor staff, and across multiple programs with varying functional requirements.
- Previous experience and success in managing projects similar to the EOL project in terms of solution type (i.e., commercial off-the-shelf or modified off-the-shelf), size, scope, and complexity.
- Knowledge and experience in data management and data conversion.
- Experience in working closely with internal and external stakeholders in order to share information and reach a common goal.
- Experience in developing and maintaining detailed project schedules.
- Experience in working with the State's Department of Technology Services (DTS).
- Experience in performing conflict resolution with stakeholders, vendors, and staff.

The responsibilities of the Project Manager are further described in section 6.5.4, Project Team Roles and Responsibilities.

6.2 Project Management Methodology

The CDPH Project Management Methodology is based on guidelines in SIMM Section 45, Appendix A, Information Technology Project Oversight Framework; SIMM Section 20, Project Management Methodology Guidelines; and PMI's PMBOK Third Edition. The EOL Project Manager will, at a minimum, implement the recommended project management and risk management practices required by DOF's Information Technology Project Framework, industry best practices, and lessons learned from prior CDPH projects. At a minimum, this includes:

- Development and maintenance of the EOL project charter and PMP defining the project goals and objectives, communications plan, roles and responsibilities, project team, scope, and high-level milestones and deliverables.
- Development and maintenance of a detailed project schedule that defines the phases, activities, timeframe, resources, dependencies, milestones, and deliverables, and monitor planned versus actual performance.
- Tracking and managing the project budget.
- Performing resource, quality, and configuration planning.
- Development of business and technical requirements.
- Utilization of a predefined issue management and change management process.
- Utilization of a predefined structured approach for reviewing and approving deliverables.
- Identification and documentation of business, technical, and functional requirements, to serve as a baseline for success criteria.
- User review and acceptance testing.
- Ongoing project performance reviews, corrective actions, and project plan updates.
- Adherence to the DOF reporting requirements for reportable projects, including Monthly Project Status Reports and the Post Implementation Evaluation Report (PIER).

A critical factor will be ensuring that ongoing work will be accomplished during the time that staff is involved in this project. The following preventative and mitigating measures will be taken to ensure continuity of CDPH's critical public health and safety operations during the course of the implementation:

Decisions on the sequencing and phasing of the implementation will be finalized in part based on anticipated program workloads, current vacancy rates, and any seasonal fluctuations in workload.

Expert staff members who are assigned to the project will have completed knowledge transfer and turnover activities to the "backfill" staff who will be filling in during the implementation.

Expert staff members who are assigned to the project will retain at least 25% availability to assist the backfill staff for operational continuity. This percentage is expected to decrease over time.

Implementation timeframes will be set without overly aggressive deadlines, using input from the Systems Implementation vendor (experienced with their own product), as well as the Independent Verification & Validation (IV&V), Independent Project Oversight (IPO), and Project Management consultants, to minimize the risk of "crunch" deadlines which would tend to disrupt operational continuity.

Should a significant public outbreak or other major business disruption occur, the CDPH Project Manager will immediately consult with the established risk escalation chain described in Section 7. The project will remain flexible to delay or suspend portions of the implementation if needed to protect the health and safety of the public.

The CDPH Project Director will continually monitor the success of this approach, and will recommend adjustments on an as-needed basis to ensure operational continuity of CDPH's public health and safety activities.

The remainder of this section provides an overview of the major areas of project management.

6.2.1 Integration Management

Integration management includes the development and execution of the overall project management plan and ancillary plans. Key activities of integration management include:

- Identifying project initiation activities.
- Determining how the project will be executed and managed.
- Determining how communications will occur between CDPH programs and other stakeholders.
- Determining how change will be controlled.
- Defining project phases, major milestones, scheduled tasks and activities, resource allocation with periodic project reporting.
- Defining deliverable/product review and approval and other acceptance criteria.
- Defining project success evaluation criteria and project closeout activities.
- Determining status and other reporting expectations.
- Identifying relationships to other IT or business efforts.

6.2.2 Scope Management

Scope management includes processes to ensure that the appropriate set of work and deliverables are defined and solution implemented that meets the project objectives. FSR Section 3.3, Business Objectives, defines the overall scope of the EOL project. The project charter and PMP will define, in detail, the logical and technical scope, as well as the project parameters. Scope changes will be controlled via a formal change control process, and may require an SPR and DOF's approval.

The following approach will be used to manage the scope of this project:

- The business objectives and functional requirements will be defined and validated at each phase of the project.
- Any proposed change to the project scope and objectives must be analyzed and approved through the change control process. The Executive Sponsor approves significant changes to scope.

- Project scope will be continuously evaluated against time, cost, functionality, and other constraints of the projects.
- Requirements will be evaluated against objectives throughout the effort to ensure that the project satisfies business objectives consistent with defined quality standards.
- All vendor contracts will be managed to contract specifications.

6.2.3 Time Management

The approach to time management includes the techniques to be used to manage the project schedule. Management of the project schedule has a critical impact on the costs, scope and quality of all projects. The project will utilize the following approach to time management:

- The project will be based on the general approach, major phases, and resources described in the FSR.
- The Project Manager, with assistance from the project team, will develop a work breakdown structure (WBS) and project schedule.
- As the WBS is created, the project team will determine relative priorities of the requirements for Steering Committee approval.
- The project schedule will be based on the outputs of the WBS.
- The project schedule will be updated continually during the course of the project until completion.
- Should the development or implementation experience any slippage, the project will have the opportunity to delay non-critical requirements in order to meet the critical requirements.
- The process of making significant changes to the project schedule will be integrated with and managed through the project's defined change management process.
- The project schedule cannot be allowed to exceed the approved baseline schedule without approval from the Steering Committee.
- If the project schedule deviates by ten percent or more, the deviation will be reported to the DOF via a Special Project Report (SPR) for approval.

6.2.4 Cost Management

Cost will be monitored and managed throughout the life of the project based on the approved budget. Project costs include state costs (i.e., interagency agreements, personnel years, backfills, and information technology costs), contractor/vendor resources (i.e., contracts or service level agreements), and hardware and software procurements. Cost Management involves resource planning, cost estimating, cost budgeting, cost accounting, and cost control. The Project Manager will manage the costs of the project using the following approach:

- The project budget will be continually tracked during the life of the project. This budget will show the approved baseline cost estimates, approved revisions to the cost estimate, actual expenditures against the cost estimates and the remaining balance in each cost category.
- The project expenditures cannot be allowed to exceed the approved cost estimates without approval from the Steering Committee and DOF (if expenditures exceed ten percent of the original estimate) or through the CDPH budgetary processes.
- Project costs that change ten percent or more will be reported to the DOF via a SPR for approval.

6.2.5 Quality Management

Quality management involves quality planning, independent validation and verification (IV&V), quality assurance, and quality control. The Project Manager is ultimately responsible for quality management and will use the following tools and techniques for managing project quality:

- Deliverable expectation documents (DED)
- Templates
- Standards and best practices
- Reviews and audits
- Requirement reviews and a requirements traceability matrix
- Design review sessions and walkthroughs
- Defined deliverable acceptance criteria
- Training
- Testing
- Verification and validation

In addition, the IV&V oversight vendors will ensure all contracted vendors use the software development lifecycle processes and industry standards, such as IEEE and PMBOK.

6.2.6 Human Resource Management

Human resource management includes how the project will be staffed and the identification of the qualifications needed for team members to successfully complete the project according to the project timeline and objectives. Human resource management requires the definition of the project team organization, skill identification, staff acquisition, staff duration, knowledge transfer between team members, and team development.

6.2.7 Communication Management

Communication management defines:

- Who will receive project information
- What type of information will each project stakeholder receive
- When the information will be disseminated
- How the information will be disseminated and stored
- Who is responsible for ensuring all communication activities take place and that information is clearly communicated and understood by information recipients

The EOL Project Manager will work in partnership with the EOL Project Director, Executive Sponsor, the EOL project Steering Committee, Program Directors, and other project stakeholders and customers to identify communication requirements and to ensure frequent and clear communication occurs. The EOL Project Manager will develop a formal Communication Plan to ensure all project stakeholders, either directly involved in the project or impacted by the project activities and products, will be kept informed of the project's purpose, progress, issues, and implementations and will identify types, methods, and frequency of communications between all stakeholders.

6.2.8 Risk Management

Risk management involves defining how issues and risks will be identified, qualified, prioritized, quantified, escalated, and managed. Project risks include events that might impact project parameters including schedule, budget, scope, and quality. FSR Section 7 provides an initial Risk Management Plan. Project risks arise and evolve throughout the course of normal project. Due to the complexity of this enterprise-wide project, the CDPH Project Manager will work closely with the EOL Project Director, Executive Sponsor, the EOL project Steering Committee and Program Directors to monitor and resolve issues and to mitigate risks. Although initial risks and mitigating actions have been identified, regular risk assessments will be included in the project schedule.

6.2.9 Procurement Management

Procurement management involves defining how the necessary goods and/or services will be acquired to accomplish the objectives of the project. Procurement management includes procurement planning, solicitation planning, solicitation, source selection, contract administration, and contract closeout. A formal Information Technology Procurement Plan (ITPP) has been developed in support of the EOL FSR.

All procurements required for the project will be conducted in accordance with state laws and the Department of General Services (DGS) procurement rules. The ITPP defines the roles and responsibilities of all those involved in conducting the procurements and contract management. The plan also defines specific procedures for managing invoices, monitoring implications of proposed changes on the related contracts, and how disagreements with vendors will be managed and escalated for resolution.

CDPH will provide a Contract Manager to oversee the procurement process as well as ongoing contracts with the various EOL project vendors. In addition, the CDPH will procure an IV&V vendor to provide verification and validation oversight of acquisition activities and procurement document content. The EOL project team will also include an independent project oversight member from the CDPH PPMB Planning and Oversight Section (POS) during the procurement phase to ensure that procurements not subject to DGS are conducted in a manner aligned with ITSD standards.

The following table identifies the products or services that need to be procured and the planned procurement method. Additional information regarding the procurement approach is provided in ITPP Section 3, Acquisition Methodology.

Table 15: Products and Services to Procure

Product or Service	Description	Procurement Method
Acquisition Services	Responsible for development of the solicitation document required to solicit the Systems Integrator	CMAS
Project Oversight Services (IV&V)	Independent Verification and Validation (IV&V) is responsible for 1) verifying the adequacy of the EOL project RFP presentation of system solution and requirements, 2) monitoring the EOL project to ensure that products conform to RFP requirements (verification) and that they satisfy the intended user needs (validation)	CMAS or MSA
Project Management Services	Responsible for the overall management of the EOL project and coordinating project activities performed by vendors, as well as by CDPH and DTS	CMAS or MSA
Project Oversight Services (IPOC)	Independent Project Oversight Contractor (IPOC) is responsible for ensuring that the project is managed according to defined State and industry standards and best practices	CMAS or MSA

Product or Service	Description	Procurement Method
Systems Integration (including software)	Responsible for all aspects of the EOL project development, test/training and production environments including, but not limited to, software, configurations, data migration, reports, training, documentation, implementation and ongoing support via a maintenance contract	Traditional Business-based

6.3 Project Organization

Figure 9 on the following page represents the organization of the EOL project team. A description of roles and responsibilities is provided in Section 6.5.4, Project Team Roles and Responsibilities.

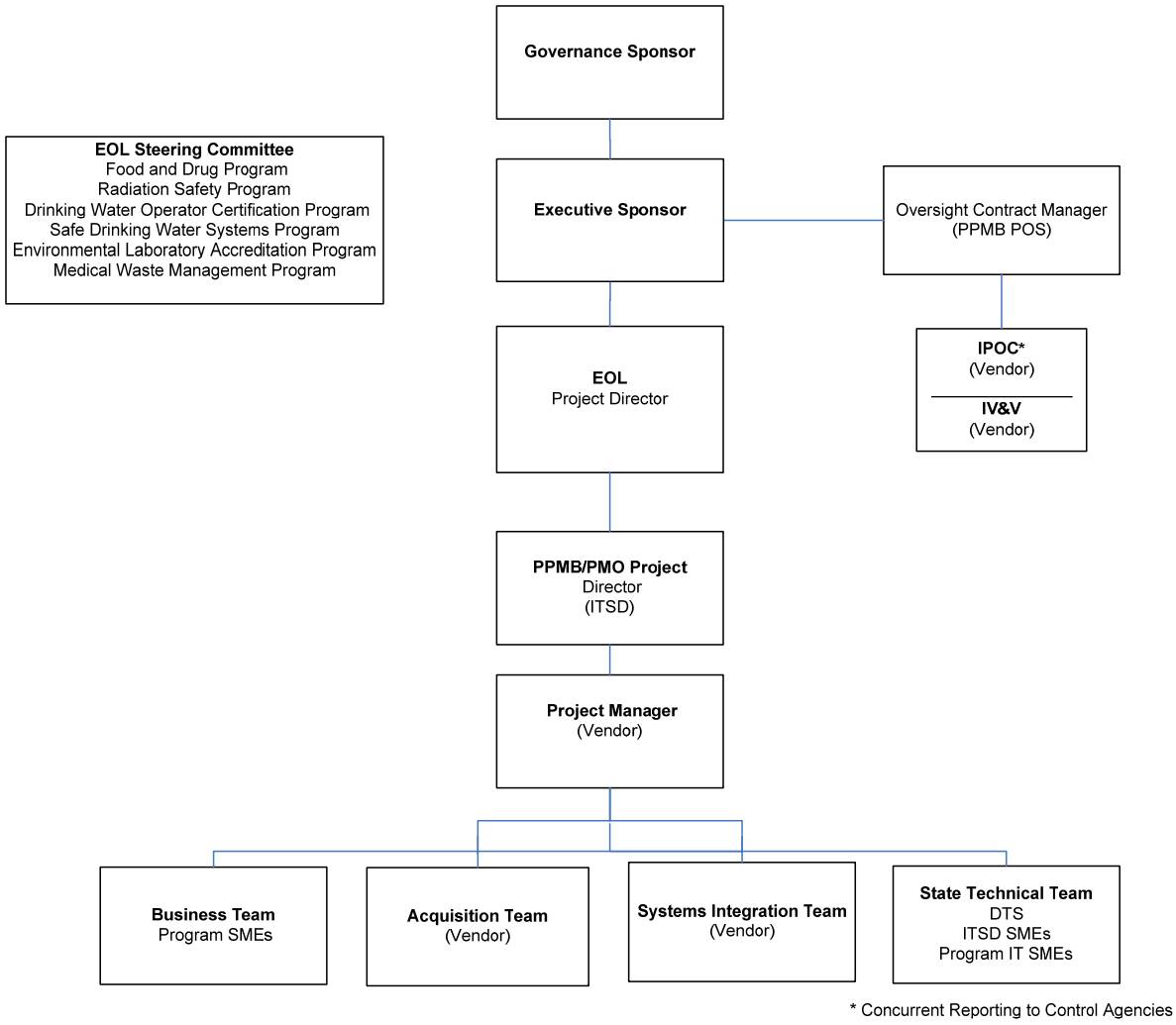


Figure 9: EOL Project Team Organization

6.4 Project Priorities

Managing a project requires balancing of three major components: resources, schedule, and scope. These three components are interrelated. A change in one component may impact and result in a change in another component. DOF requires that the project stakeholders agree on the importance of each of these factors before the project begins by assigning one of the following to each factor:

- Constrained: the factor cannot be changed
- Accepted: the factor is somewhat flexible to the project circumstances
- Improved: the factor can be adjusted

The following table presents the trade-off matrix for this project.

Table 16: Trade-off Matrix

	Degree of Flexibility		
	Low	**Medium**	**High**
Schedule			X
Scope		X	
Resources	X		

The following table presents the project priorities for this project.

Table 17: Project Priorities

Schedule	Scope	Resources
Accepted	Improved	Constrained

6.5 Project Plan

Project planning defines the project activities to be performed, end products to be delivered, and how the activities will be accomplished. The purpose of project planning is to define each major task, estimate the time and resources required, plan for communications, and provide a framework for management review and control. A formal Project Management Plan (PMP) will be developed by the EOL contract Project Manager in coordination with the EOL CDPH Project Director. The PMP will follow the template provided by the CDPH PMO and comply with the PMI PMBOK, the DOF Information Technology Project Oversight Framework, and applicable IEEE standards. The project planning activities and goals include defining:

- Project scope
- Project assumptions
- Project approach and schedule (i.e., phasing)
- Project team roles and responsibilities
- Project communication plan

6.5.1 Project Scope

The logical scope of a project is defined as the enterprise processes and systems that form the logical boundaries for the business areas directly included and impacted. The scope of work is to develop, test, and implement an off-the-shelf web-based solution that will support the business objectives and functional requirements described in FSR Section 3, Business Case. The business processes and respective organizations impacted by the EOL project are identified in the following table.

Table 18: Logical Scope

Function	Impacted CDPH Organizations
Licensing (application, renewal, inquiry, maintenance of historical information)	▪ Radiation Safety Program ▪ Medical Waste Management Program ▪ Food and Drug Program ▪ Safe Drinking Water Systems ▪ Drinking Water Operator Certification Program
Enforcement	▪ Radiation Safety Program ▪ Medical Waste Management Program ▪ Food and Drug Program ▪ Safe Drinking Water Systems ▪ Drinking Water Operator Certification Program
Billing	▪ Radiation Safety Program ▪ Medical Waste Management Program ▪ Food and Drug Program ▪ Safe Drinking Water Systems ▪ Drinking Water Operator Certification Program
Complaint/Investigation	▪ Radiation Safety Program ▪ Medical Waste Management Program ▪ Food and Drug Program ▪ Safe Drinking Water Systems ▪ Drinking Water Operator Certification Program
Inspection or Proficiency Testing	▪ Radiation Safety Program ▪ Food and Drug Program ▪ Safe Drinking Water Systems ▪ Drinking Water Operator Certification Program

The existing systems that are impacted by the EOL project are identified in FSR Section 4.2, Current Method. The EOL Project includes the following major activities:

- Acquisition and installation of any required hardware and software needed to implement the technical solution.
- Configuration of the off-the-shelf software package.
- Conversion of existing data.
- Deployment of the solution to internal and external (i.e., customers) end-users.
- Training of internal end-users and support staff on the new solution.

6.5.2 Project Assumptions

The major project assumptions include:

Scope

- The scope of the EOL project solution is limited to the business processes and users associated with the CDPH organizations identified in Section 3.
- The functional requirements will not substantially change during the project.

Funding

- Funding will be through fee-supported Special Funds.
- No funding will be needed from the state's General Fund.
- No increases in fees charged to regulated entities will be required.

Procurement

- PPMB submits the FSR for this project to DOF and serves as a liaison between CDPH and DOF.
- DOF will review and approve the FSR for this project within sixty days of submission.
- DGS approves the proposed procurement approaches defined in the ITPP for this project.
- DGS will review and approve the proposed procurement approaches defined in the ITPP for this project within sixty days of submission.
- PPMB will review and approve all project-related acquisition documents.
- CDPH will utilize a business-based procurement approach to procure software and integration services.
- CDPH will procure the services of an experienced Acquisition Specialist vendor to develop the Systems Integration RFP in accordance with DGS and DOF standards.
- CDPH will procure the services of an experienced Project Manager, using the CMAS or MSA process. The Project Manager will oversee the development of the System Integration RFP by the Acquisition Specialist and provide the project management services for the duration of the EOL project.
- CDPH will procure IPOC services, using the CMAS or MSA process. The IPOC vendor ensures that the project is managed in accordance with State and industry standards.
- CDPH will procure IV&V services, using the CMAS or MSA process. The IV&V vendor oversees the project from Systems Integration vendor selection through the duration of the EOL project.

- CDPH, DOF, and DGS approval of the Systems Integration RFP may delay vendor procurement, contract award, and project start date.
- There will not be a significant delay due to vendor protest of the awarded Systems Integration services contract.

Project Implementation

- All new hardware and software related to the EOL project must be in accordance with CDPH and DTS technology standards.
- The test/training and production environment for the EOL system will reside at DTS as prescribed by the State Administrative Manual (SAM) section 4982.1; the development environment will reside at CDPH Sacramento headquarters server farm.
- CDPH will contract with the Systems Integration vendor to provide at least one full year of post-implementation maintenance and operations, with an option to extend for two additional years.

Project Management

- Executive sponsorship will continue through project completion, and will include a focus on continuously sustaining consensus of the multiple programs participating in this implementation.
- Regular and broad communication will be a key project management emphasis.
- Issues will be resolved and risks mitigated on a timely basis.

Staffing

- CDPH program expertise is essential to this effort; designated staff will be available to participate in requirements definition, systems design, data clean-up and conversion, user acceptance testing, and training.
- CDPH IT knowledge of existing systems and their involvement in ongoing support makes it essential for designated staff to participate in requirements definition, systems design, data clean-up and conversion, testing, training, and on-going maintenance.
- Suppliers, vendors, consultants, and State staff will perform their EOL project assignments in a competent and timely manner.
- PPMB (POS) will provide a part-time resource to oversee IPOC and IV&V activities.
- PPMB (PMO) will provide a Project Director.
- ITSD will make resources available to build and implement an EOL system development server.
- ITSD will provide a resource to assist in working with the designated DTS data center, as needed.

General

- CDPH programs will support and accept process and procedure changes driven by business transformation in order to leverage the features and functionality of the new system and standardize procedures and documentation.
- Existing systems used by CDPH programs will continue to support program business functions until such time that EOL system is successfully implemented; at which time CDPH programs no longer utilize the legacy systems.
- This project further assumes that CDPH programs will not develop any new stand-alone spreadsheets or databases during the EOL project unless it is deemed by management as absolutely critical and is driven by legislation.
- This project further assumes that CDPH will not perform any modifications or enhancements to current systems during the EOL project unless it is deemed by management as absolutely critical (e.g., driven by legislation, adversely impacting ability to issue billing notices, correcting a serious error, etc.).

6.5.3 Project Approach and Schedule

CDPH will use a phased approach, in order to obtain initial benefits early in the process, and to minimize use of scarce resources, minimize project risk, and accommodate an enterprise-wide implementation.

The following project approach and schedule represent one reasonable approach. As the FSR approval and subsequent procurement phases proceed, particularly regarding approaches recommended by the software vendors based on their specific experience conducting similar implementations for other clients, it's expected that this approach will be adjusted. Since this is a business-based FSR, CDPH expects that vendor-proposed implementation approaches obtained during the competitive procurement process will inform the final selected approach. For example, the online payment (EFT) functionality might be implemented first, for the benefit of all participating programs, before the full implementation of all functionality begins for any individual program. The final selection of approach will remain fully within the state's discretion, and will be fully specified in the Special Project Report (SPR).

Table 19 represents an example sequence of the Enterprise-wide On-line Licensing System implementation project:

Table 19: Project Phases and Schedule

Phase/ Stage	Phase/Stage Name	Estimated Start	Estimated End
Phase 1: Project Planning and Analysis			
Stage 1.1	Project Start-up	7/2/2007	8/24/2007
Stage 1.2	FSR/ITPP Vendor Procurement	8/25/2007	10/9/2007
Stage 1.3	FSR/ITPP Development by Vendor and CDPH	10/9/2007	12/17/2007
Stage 1.4	FSR/ITPP Approval by CDPH	12/18/2007	12/20/2007
Stage 1.5	FSR/ITPP Approval by Control Agencies	12/21/2007	4/1/2008
Phase 2: Procurement Planning			
Stage 2.1	IPOC/IV&V Vendor Solicitation Document Development	3/4/2008	5/1/2008
Stage 2.2	Project Manager Vendor Solicitation Document Development	3/4/2008	5/1/2008
Stage 2.3	Acquisition Specialist Vendor Solicitation and Procurement	4/2/2008	7/2/2008
Stage 2.4	Systems Integration Vendor RFP Development and Approval by CDPH	7/2/2008	9/1/2008
Stage 2.5	Systems Integration Vendor RFP Approval by Control Agencies	9/2/2008	10/2/2008
Phase 3: Vendor Procurement and Selection			
Stage 3.1	IPOC/IV&V Vendor Procurement	5/1/2008	7/1/2008
Stage 3.2	Project Manager Vendor Procurement	5/1/2008	7/1/2008
Stage 3.3	Systems Integration Vendor Procurement	10/3/2008	5/4/2009
Stage 3.4	Systems Integration Vendor Selection	5/9/2009	6/23/2009
Stage 3.5	SPR Development/Approval by CDPH	6/25/2009	8/9/2009
Stage 3.6	SPR Approval by Control Agencies	8/10/2009	10/9/2009

Phase 4: Systems Configuration and Implementation: Radiation Safety Program, Food & Drug Program			
Stage 4.1	Business Process Redesign and System Preparation		
Activity 4.1.1	Business Process Redesign and System Analysis	10/10/2009	1/10/2010
Activity 4.1.2	Systems Configuration / Modifications	1/11/2010	5/14/2010
Activity 4.1.3	Data Conversion	2/11/2010	5/14/2010
Activity 4.1.4	Systems Testing	5/15/2010	8/15/2010
Stage 4.2	Implementation		
Activity 4.2.1	User Acceptance Testing	8/16/2010	9/16/2010
Activity 4.2.2	Implementation (including Training)	9/17/2010	11/15/2010
Activity 4.2.3	Post-Implementation Support (excluding M&O)	11/15/2010	1/14/2011
Phase 5: Systems Configuration and Implementation: Medical Waste Management Program, Safe Drinking Water Systems, Drinking Water OCP			
Stage 5.1	Business Process Redesign and System Preparation		
Activity 5.1.1	Business Process Redesign and System Analysis	11/16/2010	1/14/2011
Activity 5.1.2	Systems Configuration / Modifications	1/15/2011	3/18/2011
Activity 5.1.3	Data Conversion	1/15/2011	3/18/2011
Activity 5.1.4	Systems Testing	3/19/2011	5/20/2011
Stage 5.2	Implementation		
Activity 5.2.1	User Acceptance Testing	5/21/2011	6/21/2011
Activity 5.2.2	Implementation (including Training)	6/22/2011	7/22/2011
Activity 5.2.3	Post-Implementation Support (excluding M&O)	7/22/2011	9/20/2011
Phase 6: Post-Implementation			
Stage 6.1	Initial Maintenance and Operations	11/15/2010	11/15/2011
Stage 6.2	Phase-out of HAL for RHB	11/15/2010	6/15/2011
Stage 6.3	Post Implementation Evaluation Report (PIER)	5/15/2012	6/14/2012
Stage 6.4	Optional Vendor Add-on Maintenance and Operations	11/16/2011	11/16/2013

A Gantt chart view is contained in the figure below.

ID	Task Name	Start	Finish
1	**CDPH Enterprise-wide On-line Licensing Project**	**Mon 7/2/07**	**Sat 11/16/13**
2	**Project Activities**	**Mon 7/2/07**	**Tue 9/20/11**
3	**Phase 1: Project Planning and Analysis**	**Mon 7/2/07**	**Mon 3/31/08**
4	Stage 1.1 Project Start-Up	Mon 7/2/07	Fri 8/24/07
5	Stage 1.2 FSR/ITPP Vendor Procurement	Sat 8/25/07	Tue 10/9/07
6	Stage 1.3 FSR/ITPP Development by Vendor and CDPH	Tue 10/9/07	Mon 12/17/07
7	Stage 1.4 FSR/ITPP Approval by CDPH	Tue 12/18/07	Thu 12/20/07
8	Stage 1.5 FSR/ITPP Approval by Control Agencies	Fri 12/21/07	Mon 3/31/08
9	**Phase 2: Procurement Planning**	**Tue 3/4/08**	**Thu 10/2/08**
10	Stage 2.1 IPOC/IV&V Vendor Solicitation Document Development	Tue 3/4/08	Thu 5/1/08
11	Stage 2.2 Project Manager Vendor Solicitation Document Development	Tue 3/4/08	Thu 5/1/08
12	Stage 2.3 Acquisition Specialist Vendor Solicitation and Procurement	Wed 4/2/08	Wed 7/2/08
13	Stage 2.4 Systems Integration Vendor RFP Development and Approval by CDPH	Wed 7/2/08	Mon 9/1/08
14	Stage 2.5 Systems Integration Vendor RFP Approval by Control Agencies	Tue 9/2/08	Thu 10/2/08
15	**Phase 3: Vendor Procurement Selection**	**Thu 5/1/08**	**Fri 10/9/09**
16	Stage 3.1 IPOC/IV&V Vendor Procurement	Thu 5/1/08	Tue 7/1/08
17	Stage 3.2 Project Manager Vendor Procurement	Thu 5/1/08	Tue 7/1/08
18	Stage 3.3 Systems Integration Vendor Procurement	Fri 10/3/08	Mon 5/4/09
19	Stage 3.4 Systems Integration Vendor Selection	Sat 5/9/09	Tue 6/23/09
20	Stage 3.5 SPR Development/Approval by CDPH	Thu 6/25/09	Sun 8/9/09
21	Stage 3.6 SPR Approval by Control Agencies	Mon 8/10/09	Fri 10/9/09
22	**Phase 4: Systems Configuration and Implementation: RHB, Food & Drug**	**Sat 10/10/09**	**Fri 1/14/11**
23	**Stage 4.1 Business Process Redesgn and System Preparation**	**Sat 10/10/09**	**Sun 8/15/10**
24	Activity 4.1.1Business Process Redesign and System Analysis	Sat 10/10/09	Sun 1/10/10
25	Activity 4.1.2 Systems Configuration / Modifications	Mon 1/11/10	Fri 5/14/10
26	Activity 4.1.3 Data Conversion	Thu 2/11/10	Fri 5/14/10
27	Activity 4.1.4 Systems Testing	Sat 5/15/10	Sun 8/15/10
28	**Stage 4.2 Implementation**	**Mon 8/16/10**	**Fri 1/14/11**
29	Activity 4.2.1 User Acceptance Testing	Mon 8/16/10	Thu 9/16/10
30	Activity 4.2.2 Implementation (including Training)	Fri 9/17/10	Mon 11/15/10
31	Activity 4.2.3 Post-Implementation Support (excluding M&O)	Mon 11/15/10	Fri 1/14/11
32	**Phase 5: Systems Configuration and Implementation: MWMP, DWOCP, SDWS**	**Tue 11/16/10**	**Tue 9/20/11**
33	**Stage 5.1 Business Process Redesign and System Preparation**	**Tue 11/16/10**	**Fri 5/20/11**
34	Activity 5.1.1 Business Process Redesign and System Analysis	Tue 11/16/10	Fri 1/14/11
35	Activity 5.1.2 Systems Configuration / Modifications	Sat 1/15/11	Thu 3/17/11
36	Activity 5.1.3 Data Conversion	Sat 1/15/11	Thu 3/17/11
37	Activity 5.1.4 Systems Testing	Mon 3/21/11	Fri 5/20/11
38	**Stage 5.2 Implementation**	**Mon 5/23/11**	**Tue 9/20/11**
39	Activity 5.2.1 User Acceptance Testing	Mon 5/23/11	Tue 6/21/11
40	Activity 5.2.2 Implementation (including Training)	Wed 6/22/11	Fri 7/22/11
41	Activity 5.2.3 Post-Implementation Support (excluding M&O)	Fri 7/22/11	Tue 9/20/11
42	**Ongoing Activities**	**Mon 11/15/10**	**Sat 11/16/13**
43	**Phase 6: Post-Implementation**	**Mon 11/15/10**	**Sat 11/16/13**
44	Stage 6.1 Initial Maintenance and Operations	Mon 11/15/10	Tue 11/15/11
45	Stage 6.2 Phase-out of HAL for Radiological Health Branch	Mon 11/15/10	Wed 6/15/11
46	Stage 6.3 Post Implementation Evaluation Report (PIER)	Tue 5/15/12	Thu 6/14/12
47	Stage 6.4 Optional Vendor Add-on Maintenance and Operations	Wed 11/16/11	Sat 11/16/13

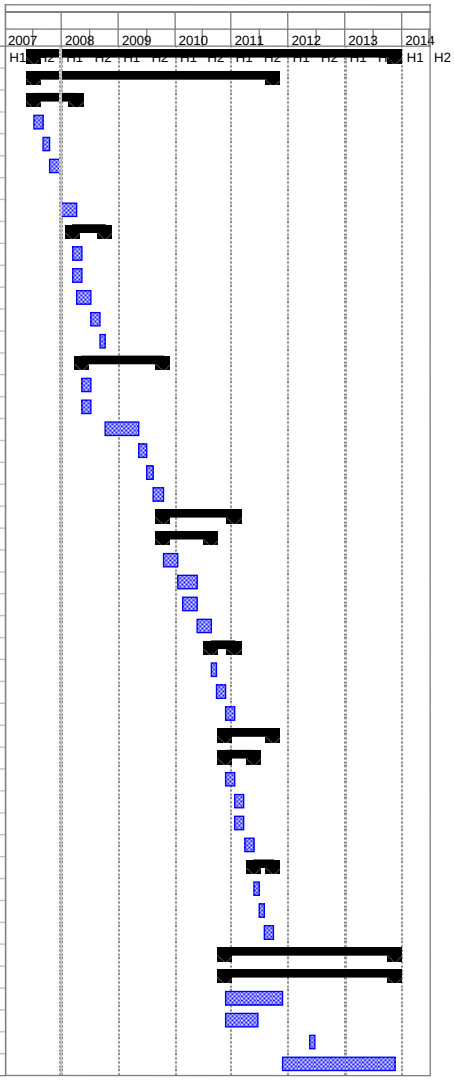


Figure 10: Project Schedule

The major deliverables associated with each phase are identified below.

Table 20: Project Deliverables

Phase	Deliverable
Phase 1: Project Planning and Analysis	▪ FSR/ITPP Vendor Solicitation Document ▪ CDPH Concept Paper ▪ Approved FSR ▪ Approved ITPP
Phase 2: Procurement Planning	▪ Acquisition Vendor Solicitation Document ▪ Contract for Acquisition Specialist Vendor ▪ Approved Systems Integration Vendor RFP ▪ Approved Project Manager Vendor Solicitation Document ▪ Approved IPOC/IV&V Vendors Solicitation Document
Phase 3: Vendor Procurement and Selection	▪ Contract for Project Manager Vendor ▪ Contract for IPOC/IV&V Vendors ▪ Systems Integration Evaluation and Selection Results ▪ Contract for Systems Integration Vendor ▪ Project Management Plan ▪ Special Project Report
Phases 4 and 5: Systems Configuration and Implementation	▪ Updated Project Management Plan ▪ Data Cleansing and Conversion Plan ▪ Testing Plan ▪ Training Plan ▪ Implementation Plan ▪ Systems Maintenance Plan ▪ Logical and Physical Data Model ▪ Systems Design Document (SDD) ▪ Data Mapping and Data Dictionary ▪ Systems & Integration Test Results ▪ Data Conversion Results ▪ User Acceptance Test Results ▪ Functioning EOL System Application ▪ EOL System Database ▪ User Manual ▪ Operational Plan ▪ Operational Recovery Plan ▪ System Manuals ▪ Training Materials and Sessions
Phase 6: Post-Implementation	▪ Maintenance and Operation of System ▪ Documented Help Desk Procedures ▪ Tuned and Optimized System ▪ Tuned and Optimized Database ▪ Post Implementation Evaluation Report

6.5.4 Project Team Roles and Responsibilities

The governance structure described in this section will remain in place throughout the entire duration of the phases shown above; specifically, through the end of vendor maintenance and operations. This means through the end of Stage 6.4, or in the event the state elects not to engage the vendor for the optional stage, then through the end of all other stages, inclusive of the 1-year required vendor maintenance and operations period and PIER reporting. This provision will ensure that appropriate consensus among all participating programs continues to be sought and obtained for all major project decisions.

The following table identifies each key participant and their responsibilities on this project.

Table 21: Project Team Roles and Responsibilities

Role	Responsibilities	Organization
Governance Sponsor	▪ Makes final decisions if Project Steering Committee (with Executive Sponsor as Chair) does not reach consensus	Chief Deputy Director, CDPH Operations
Executive Sponsor	▪ EOL project Steering Committee Chair ▪ Provides executive sponsorship, oversight and guidance ▪ Commits project resources and expenditures ▪ Approves the final scope of the EOL project and resolves scope issues ▪ Approves significant changes to the scope, cost or schedule ▪ Resolves significant issues that the EOL project Steering Committee cannot resolve in a timely manner – including making final decisions if consensus among Program Chiefs is not reached ▪ Provides final approval of project deliverables ▪ Communicates with major stakeholders ▪ Responsible for project acceptance	CDPH Deputy Director, Center for Environmental Health
EOL Project Steering Committee	▪ Primary project decision-making body ▪ Provides business sponsorship, executive oversight and strategy ▪ Advisor to Executive Sponsor ▪ Assists in the identification of business needs and provides business direction ▪ Confirms project goals and scope ▪ Provides strategic guidance and monitors and approves progress at key intervals ▪ Makes decisions on key project issues not resolved by Project Director ▪ Escalates unresolved issues to the Executive Sponsor	CDPH Deputy Director, Center for Environmental Health Chiefs of Participating Programs: FDB RHB DWOCP SDWS

Role	Responsibilities	Organization
	▪ Communicates project status to respective external stakeholders, as needed ▪ Assists in the coordination of efforts between CDPH programs ▪ Ensures overall project success ▪ ---------- ▪ On behalf of their respective programs, the members each: ▪ Allocate subject matter expert resources within their respective programs ▪ Review and provide input on project deliverables ▪ Act as a liaison between program staff and the project management and system integration vendor teams ▪ Participate in the resolution of issues raised by stakeholders ▪ Recommend product acceptance and approval to the Project Director	MWMP PPMB/PMO Project Director
EOL Project Director	▪ Provides guidance and leadership to PPMB/PMO Project Director ▪ Communicates project status to internal stakeholders ▪ Serves as liaison between CDPH and DGS ▪ Provides procurement support ▪ Ensures project progress and deliverable quality ▪ Resolves or escalate issues that cannot by solved by the project team to the EOL Project Steering Committee ▪ Attends EOL project management meetings ▪ Reviews and recommends project deliverables; recommend deliverable acceptance (and invoice approval) to the Executive Sponsor	Appointed by Executive Sponsor (i.e. Appointed by CDPH Deputy Director, Center for Environmental Health)
PPMB/PMO Project Director	▪ Serve as liaison between CDPH and DOF ▪ Manage activities performed by IPOC and IV&V ▪ Develops solicitation documents to procure the project PM, IPOC and IV&V ▪ Resolves or escalates issues	PPMB
EOL Project Manager	▪ Participates in the procurement processes to secure IV&V/IPOC vendor services ▪ Manages IV&V/IPO contract compliance ▪ Coordinates EOL project management meetings	PMPB
Business Team (Subject Matter Experts)	▪ Provide guidance and subject matter expertise ▪ Assist in the identification of business needs and requirements ▪ Assist in analysis of the current operating environment	FDB RHB DWOCP

Role	Responsibilities	Organization
	▪ Create/refine business technical requirements for RFP ▪ Assist in the definition of business processes and business rules and development of new processes ▪ Participate in gap analysis sessions ▪ Assist in data gathering, research and analysis ▪ Assist with data cleansing and data conversion activities ▪ Participate in joint application design (JAD), working sessions ▪ Participate in user acceptance testing ▪ Participate in training	SDWS MWMP
Acquisition Team	▪ Develops initial solicitation documents for CDPH/PPMB review (to procure the Systems Integration vendor) ▪ Defines proposal evaluation and selection procedures ▪ Assists CDPH/PPMB as needed to obtain DGS approval of solicitation documents ▪ Establishes bidder libraries, as required ▪ Facilitates the selection of vendors	Vendor
Systems Integration Team	▪ Overall responsibility for the design, development and implementation phases of the project ▪ Designs and develops EOL system and associated business processes, in accordance with CDPH programs' functional requirements and business needs ▪ Coordinates project scheduling with the Project Manager; develops a plan for phased development and implementation ▪ Conducts project reviews and provides project status ▪ Ensures project implementation and contract deliverables are on time and to RFP specifications ▪ Validates requirements ▪ Leads all gap analysis, prototyping, JAD, and focus group sessions ▪ Conducts system design and development walkthrough sessions ▪ Coordinates with programs and ITSD on system technology architecture and data migration ▪ Designs, develops, tests, and documents system interfaces ▪ Conducts unit and Systems Integration tests ▪ Supports user acceptance testing of the system ▪ Develops system documentation ▪ Develops rollout plan	Vendor

Role	Responsibilities	Organization
	▪ Provides training to authorized users ▪ Manages any sub-contractors utilized for training or system documentation purposes ▪ Participates in change management processes ▪ Participates in risk and issue management processes	
State Technical Team	▪ Builds EOL system development server ▪ Provides the Systems Integration Team with technical information regarding CDPH programs' existing systems, databases, and infrastructure ▪ Validates technical requirements ▪ Assists in performing automated data cleansing and data migration activities ▪ Participates in technical review (as needed) ▪ Assists in interfaces ▪ Assists in systems testing	DTS ITSD Program IT SMEs
Independent Verification & Validation (IV&V)	▪ Serves as an independent expert in regards to determining if project products meet the required level of quality, functionality, and performance ▪ Identifies technical risks and defects and provides recommended mitigation strategies and contingency plans ▪ Executes verification and validation tasks in accordance to IEEE standards (or other industry-accepted IT standards) ▪ Evaluates project deliverables against established standards ▪ Provides information on project issues, risks, and status to the Project Manager, PMO Project Director, Project Director, Steering Committee, and oversight agencies	Vendor
Independent Project Oversight Contractor (IPOC)	▪ Serves as an independent expert in regards to project management and operations ▪ Executes project oversight tasks in accordance with DOF's IT Project Oversight Framework ▪ Reviews all project management processes and assesses compliance with standard project management practices ▪ Reviews risk management practices used on the project, independently identifies and analyzes risks, and makes recommendations on risk response ▪ Develops management reports, including the IPO report submitted monthly to DOF	Vendor

6.6 Project Monitoring

Due to the complexity and overall cost of the project, DOF mandates that the EOL project implements formal project monitoring. Project monitoring activities must encompass the monitoring of the project's schedule, budget, and scope. The process for tracking and reporting on the status of project deliverables, project schedule, and project budget is described in this section.

6.6.1 Overall Project Monitoring

The EOL Project Manager is responsible for overseeing all aspects of the EOL project. CDPH will contract with a vendor to provide a certified Project Manager who has experience in managing a systems development and implementation project. Specific requirements of the Project Manager are defined in Section 6.1, Project Manager Qualifications.

6.6.2 Team Meetings

On a weekly basis, project status meetings will be held. These meetings will be conducted by the Project Manager and will include vendor and EOL project team members. The major areas of discussion will include, but are not limited to, the following:

- Schedule status
- Deliverable status
- Upcoming events (e.g., meetings, interviews, working sessions)
- Risks
- Issues
- Changes
- Scope
- Budget
- Relevant other topics

6.6.3 Project Management Meetings

On a weekly basis, the PMO Project Director and Program Directors, as appropriate, and the Project Manager will meet to review the project. During these meetings, the project status, upcoming events, outstanding issues, and potential project changes will be discussed.

6.6.4 Risk Management Meetings

Monthly, the EOL Project Manager will conduct a meeting focused on the identification and management of project risks. During these meetings, the Risk Register (and related Risk Management Forms) is reviewed and status is provided by the Risk Owner. Additional information on the risk management process is provided in Section 7.0, Risk Management Plan.

6.6.5 Status Reporting

Weekly, the Project Manager will develop and distribute an EOL project status report to the PMO Project Director Project and Program Directors. This report represents the activities performed by all project team members (including vendor and CDPH staff) during the previous week and includes information on accomplishments, activities in progress, upcoming activities, issues, and deliverable status.

On a monthly basis, the Project Manager will prepare the project's monthly Executive Project Status Report and submit it to the PMO Project Director for approval and then to the Executive Sponsor and Project Director. This report summarizes the overall status of the projects schedule, budget, and scope. It includes an updated version of the project work plan, identifying new/changed tasks and percentage of completion for each task.

6.6.6 Steering Committee

The EOL Project Steering Committee will meet monthly or as determined by the committee depending on risks and criticality. The Project Manager presents an overview of the status of the project, completed milestones, upcoming activities, and change control items that need to be addressed by the Steering Committee. Additional topics of discussion will vary based on the status of the project, as well as other events that may influence the project's efforts including risks, issues, legislative impacts, external stakeholder requests, etc. The meetings will be synchronized with major project milestones to ensure the sharing of project information in a timely manner.

6.6.7 Independent Project Oversight Contractor (IPOC)

The EOL project team will include a third-party vendor to serve as IPOC, as required by DOF. The responsibilities of the IPOC are provided Section 6.5.4, Project Team Roles and Responsibilities. At times, the IPOC will work with the IV&V vendor, as needed. The IPOC will report to CDPH POS.

6.6.8 Independent Verification and Validation (IV&V)

The EOL project team will include a third-party vendor to perform IV&V functions for the EOL project, as required by DOF. The responsibilities of the IV&V vendor are provided Section 6.5.4, Project Team Roles and Responsibilities. The IV&V will report to CDPH POS.

6.7 Project Quality

Quality is defined as the delivery of a work product or deliverable that satisfies the requirements and objectives of the project with minimal errors and defects. In order to ensure that the products delivered meet the specified business and technical objectives and requirements and to minimize the risk of receiving a work product or deliverable of poor quality, the following process will be implemented.

6.7.1 Deliverable Expectations Document

A Deliverable Expectations Document (DED) will be completed prior to the start of any major deliverable. Within the DED, the following is identified:

- Deliverable name
- Description of the deliverable
- Deliverable outline
- Planned delivery date
- Deliverable reviewers
- Deliverable sign-off sheet

The Project Manager, Program Directors, and Project Director are responsible for reviewing and approving each DED. The Project Manager will coordinate and conduct walkthroughs on all deliverables. The IPOC and IV&V will be provided draft and final versions of the deliverables, as well as participate in the walkthrough sessions. Program Directors provide input on project deliverables. A deliverable acceptance form will be completed by the Project Manager and forwarded with the deliverable to the Project Director for review. This form certifies the acceptance of the deliverable by CDPH and must be attached to the vendor's invoice in order for the Contract Manager to process the invoice. The Project Director reviews each deliverable and forwards the deliverable and the recommendation for approval to the Executive Sponsor who has final deliverable approval authority.

6.7.2 Project Oversight

Independent project oversight will occur through activities performed by the IPOC and IV&V vendors. The IPOC vendor is responsible for ensuring that the project is managed according to defined State and industry standards and best practices. The IV&V vendor is responsible for monitoring the EOL project to ensure that products conform to RFP requirements (verification) and that they satisfy the intended user needs (validation). The responsibilities of all roles are provided in Section 6.5.4. Project Team Roles and Responsibilities. The areas related to project quality include:

- Quality assurance reviews of the systems integrator's overall approach and deliverables including schedules, but not limited to, requirement confirmation and mapping, gap analysis, systems architecture and design specifications, test plans, test results, and training plans.
- Validation of requirements, including user, system software, hardware, and security.
- Performing requirements traceability throughout each stage of the project's system development lifecycle.
- Independent analysis on critical issues.
- Independent testing of software, as defined in the IV&V statement of work.
- Development of project metrics to monitor project quality.

6.8 Change Management

Change is an inevitable occurrence on any project. A change is defined as any alteration to the scope of the project including requirements, hardware, software, application, network, operations or environment that adds to, deletes from, or in any way modifies the scope, schedule, or cost of the project. In order to effectively manage change, the overall PMP will include a Change Management Plan to define the process, procedures and outputs for all change-related project activities. The plan will identify the parties responsible for identifying, resolving, supporting, and making project changes. The major goal of this Change Management Plan is to ensure changes are made using standardized methods and procedures that minimize negative impacts and maximize positive impacts to the requirements, design, development, implementation, and maintenance of the system.

The Change Management Plan will define the processes and procedures for: reporting an identified need for change; how the change request will be analyzed and documented; how the change will be acted upon for review, approval or denial; and, how the change will be incorporated into the PMP. The plan is designed to:

- Minimize project risk
- Provide documentation for all changes
- Minimize disruption to the project due to rework
- Measure project volatility
- Provide open disclosure of changes
- Communicate changes to stakeholders
- Maximize system/application value
- Minimize unanticipated impacts to schedule and/or budget

The implementation of a change management plan ensures that all changes are evaluated for potential scope, cost, and schedule impacts. The process allows decision-makers the opportunity to evaluate changes in a systematic manner that becomes a component of the overall project risk management strategy. Without a method for evaluating, prioritizing, and implementing changes, schedule delays, poorly defined requirements and/or cost overruns are all potential results for any system development effort. Alternatively, a well-defined and properly utilized change management process reduces risk and increases the likelihood of project success.

The change management process for the EOL project will provide a mechanism for the review and approval of changes or additions to the scope, requirements, or design of the system. This process will allow CDPH and the Systems Integration vendor to jointly discuss, review, prioritize and approve changes to requirements and design through all phases of the project.

The change management process will track all proposed changes to the system software and hardware. All requested changes would be analyzed with respect to cost and benefit. The Project Manager will present change requests to a change control

board (CCB) for approval. This process ensures that changes are documented and applied in a controlled manner with participation from relevant project personnel from initiation through closure.

Approved changes will be included in an updated and approved schedule and assigned to the responsible party for execution. Project documentation will be updated in accordance with the approved document management process. Any change that results in a change in scope, schedule, or costs of 10 percent or more will require an approved SPR.

6.9 Authorization Required

The EOL project requires standard DOF and DGS authorization. Reporting criteria, as defined by SIMM, will be followed throughout the project. The following table identifies the authorization required for the EOL project.

Table 22: Authorization Required

Type	Organization
Feasibility Study Report	DOF
Information Technology Procurement Plan	DGS
Systems Integration Request for Proposal	DGS
Special Project Report	DOF
Appropriation of Funds	DOF
Post-Implementation Evaluation Report (PIER)	DOF

7.0 RISK MANAGEMENT PLAN

Risk management is the systematic process of identifying, analyzing, and responding to project risk. It includes maximizing the probability and consequences of positive events and minimizing the probability and consequences of adverse events to project objectives.[9]

A risk is any factor that may potentially interfere with the successful completion of the project's goals. Every project inherently contains risks. Therefore, the CDPH risk management process identifies, describes, and evaluates potential project risks, defines mitigation strategies (as needed), monitors the identified risks throughout the project, and provides a method to identify new risks during the project.

This Risk Management Plan describes the methods that the Enterprise-wide On-Line Licensing System project team will use to manage risks throughout the life of the project. The remainder of this section is organized as follows:

7.1 Risk Management Approach

7.2 Risk Analysis

7.3 Risk Management Worksheet

7.4 Risk Tracking and Control

7.1 Risk Management Approach

7.1.1 References Consulted

The references used in the development of this Risk Management Plan section include:

Project Management Institute's *Project Management Body of Knowledge* (PMBOK), 3rd Edition, Chapter 11 (Project Risk Management)

Department of Finance (DOF) Information Technology Project Oversight Framework, Section 5 (Risk Management and Escalation Procedures)

DOF State Information Management Manual (SIMM), Section 200.3.11 (Risk Management Plan)

[9] Project Management Institute, *A Guide to the Project Management Body of Knowledge, Third Edition.*

Software Engineering Institute's Technical Report CMU/SIE-93-6, Taxonomy-Based Risk Identification

7.1.2 Goals and Objectives

The goal of risk assessment is to improve the probability of success of the EOL project by providing a roadmap for the ongoing assessment of potential problems and the opportunity to make adjustments to avoid or lessen the impact of those problems before they occur.

The objectives of the risk assessment are the continuous identification, assessment and documentation of:

- The risks faced by the project.
- The estimated probability of each risk.
- The consequences in terms of impact on project schedule, cost, and quality if the risk events should occur.
- The priority of each risk for response action and escalation.
- The owner of each risk.
- The plan of action for responding to each risk.
- The thresholds and procedures for escalating risks.

7.1.3 Scope

This Risk Management Plan includes the risk management activities for the duration of the EOL Project.

7.1.4 Roles and Responsibilities

Table 23 identifies the project stakeholders and their related risk management responsibilities.

Table 23: Risk Management Roles and Responsibilities

Role	Responsibilities
Department of Finance (DOF)	• Review monthly Independent Project Oversight Reports to assess project risk management practices • Provide feedback and direction as needed
EOL Steering Committee	• Final approval of Risk Management Plan • Review escalated medium and high severity risks • Provide direction when needed • Determine if risks have become unacceptable for the project to continue

Role	Responsibilities
ITSD/Planning and Oversight Section (POS)	• Provide general risk management assistance as requested • Review escalated high and medium severity risks • Provide feedback and suggestions as needed • Manage the Independent Project Oversight Contractor (IPOC) efforts • Manage the Independent Verification and Validation (IV&V) efforts
Project Director	• Approve Risk Management Plan • Review escalated high, medium, and low severity risks • Provide direction and feedback as needed
Risk Manager (i.e., EOL Project Manager)	• Overall responsibility for project risk management • Develop the Risk Management Plan • Determine which risk candidates represent actual risks • Participate in periodic risk identification reviews • Assigns Risk Owner(s) • Maintain the Risk Management Forms • Maintain the Risk Register • Escalate risks, as needed
Risk Owners (Project team members, as assigned)	• Assign risk attributes • Propose risk priority • Propose risk response strategy • Develop risk response action plan • Execute risk response actions • Track and report risk status and response activity
Project Team Members	• Identify risk candidates • Assist in quantifying risks • Serve as Risk Owners (as assigned)
Independent Project Oversight Consultant (IPOC)	• Provide an ongoing independent review and analysis of project risk management practices • Independently identify and analyze project risks • Develop Independent Project Oversight (IPO) reports for submission to management and DOF
Independent Verification and Validation (IV&V) Consultant	• Review and evaluate technical risks • Independently identify and analyze technical risks • Coordinate with the Risk Manager and IPOC to ensure that technical risks are tracked and escalated as needed

7.2 Risk Analysis

The continuous cycle of risk management activity is depicted in Figure 11.

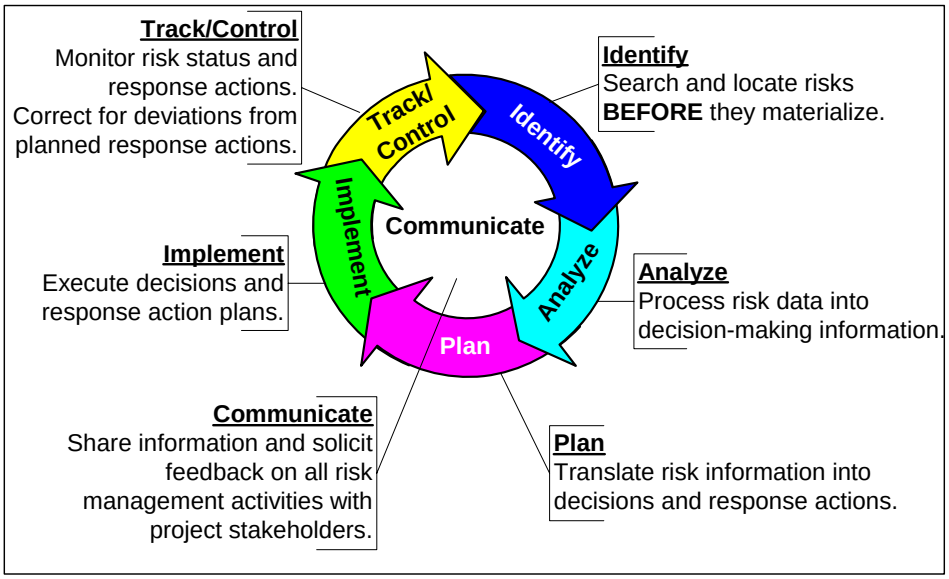


Figure 11: Risk Management Process

Risk management includes the following major components:

- Risk Analysis: Identifying and prioritizing risks.
- Risk Action Planning and Tracking: Developing a plan of action for each identified risk, and tracking progress against the plan.
- Risk Escalation: Providing appropriate visibility of risks to management.

7.2.1 Risk Identification

Risk identification is the process of identifying risk events that could negatively impact project schedule, cost, and/or quality if the event were to occur. It would be impossible to identify all possible risks to the project, therefore emphasis is on identifying risks that are at least somewhat likely to occur and that could have a significant impact on the project. All project team members are responsible for identifying potential risks to the project. Monthly Risk Management meetings include a standing agenda item for raising new risk candidates to the attention of the Risk Manager. Project team members and the IPOC may also communicate risk candidates to the Risk Manager by email, telephone, or ad hoc meetings. Potentially serious risk candidates should be communicated as soon as practical rather than waiting for the next meeting.

One technique the project can use to identify risks is the Software Engineering Institute's (SEI) Risk Taxonomy. Developed by SEI in 1993, this is essentially a checklist used to systematically identify risks. The checklist provides a structured framework of questions regarding the potential software development and project management risks that are commonly present on most projects. The questionnaire could be initially administered by the Risk Manager to the EOL project team and key stakeholders during project start-up.

Sources of Risk

Project risks can come from many and varied sources. Project team members must be vigilant in recognizing and documenting potential risks so that they can be properly evaluated for project impact. Some common risk sources include:

- The technology used on the project.
- The legal and regulatory environment in which the project is executed.
- Relationships between the organizations involved in the project.
- Sufficiency and allocation of project resources.
- Unrealistic or conflicting stakeholder expectations.
- Mandated implementation date.

Risk Determination

The Risk Manager, with participation as needed by applicable project team members, determines which risk candidates constitute actual risks to the project. The following considerations support the determination of "Is it a risk?":

- Timeframe: A risk is a potential future event. Risk events that have already occurred are not risks, but rather represent problems or issues to be managed outside of the Risk Management process. Events that may occur after the project is completed, but not during the project, are not risks to the project.
- Likelihood: What is the estimated probability of the risk event occurring? If there is little or no likelihood of the risk event occurring, the risk may not warrant inclusion in the Risk Management process. An event that is certain to occur is not a risk but rather a problem or issue.
- Impact: What is the estimated impact to the project schedule, cost, or quality if the risk event should occur? Risks with little or no impact may not warrant inclusion in the Risk Management process.

Risk candidates that are judged to meet the three criteria described above are included in the project's Risk Management process.

Risk Attributes

For each risk identified, the risk's attributes should be documented by the Risk Owner. Table 24 identifies the minimum risk attributes to be identified.

Table 24: Risk Attributes

Risk Attribute	Description
Risk Title	A brief sentence or phrase that summarizes the risk.
Risk ID	A unique number used to identify the risk. The Risk ID is assigned sequentially as risks are identified.
Originator	The name and organization of the person who identified the risk.

Risk Attribute	Description
Origination Date	The date that the risk was recognized as a project risk.
Risk Owner	The project team member responsible for responding to the risk and tracking risk status. The Risk Manager assigns the Risk Owner.
Risk Statement	A concise definition of the risk using the sentence structure: Concern • Likelihood • Consequence For example: “Mandated unrealistic implementation date • will likely • lead to significant missing functionality in the system implementation”.
Affected Elements	The project component(s) that will be impacted by the risk, for example schedule, budget, resources, scope, and/or quality.
Risk Context	The risk context elaborates on the risk statement, adding detail and background information as needed to provide a full understanding of the risk.

7.2.2 Risk Prioritization

Risks are prioritized by severity, with high severity risks given the highest priority for response action and escalation. Risk severity is a determined by the probability, impact, and time frame of the risk.

Probability

Risks are assigned a probability rating based on the estimated likelihood of a risk event occurring. Table 25 identifies valid ratings.

Table 25: Risk Probability

Likelihood of Risk Event	Probability Rating
100%	Not a risk (a likelihood of 100% means the risk has already occurred and therefore it is an issue)
66% to 99%	High
33% to 66%	Medium
1% to 33%	Low
0%	Not a risk

Impact

Risks are assigned an impact rating based on the estimated negative impact on project cost, schedule, and/or quality. Table 26 identifies how the ratings are derived.

Table 26: Risk Impact

Criteria	Impact Rating
One or more of the following: • Project cost increase of $50,000 or more • Project schedule increase of 10% or more • Failure to meet required performance • Failure to provide required functionality	High
None of the "High" criteria; however, one or more of the following: • Project cost increase of $25,000 to $50,000 • Project schedule increase of 5% to 10% • Significant discrepancies in desired performance • Significant discrepancies in desired functionality	Medium
None of the "High" or "Medium" criteria; however, one or more of the following: • Project cost increase of less than $25,000 • Project schedule increase of less than 5% • Minor discrepancies in desired performance • Minor discrepancies in desired functionality	Low

Timeframe

Risks are assigned a timeframe rating based on the time period within which action must be taken to successfully respond to the risk. Table 27 identifies valid ratings.

Table 27: Risk Timeframe

Time Period to Respond to Risk	Timeframe Rating
Less than six months	Short
Six months to one year	Medium
More than one year	Long

Risk Exposure

Risk exposure is determined from the probability and impact ratings, and is used along with the timeframe rating to determine severity. The exposure rating for each risk is the intersection of that risk's impact and probability, as presented in Table 28:

Table 28: Risk Exposure Matrix

Impact	Probability		
	High	**Medium**	**Low**
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Risk Severity

Risks are prioritized by severity, with high severity risks given the highest priority for response action and escalation. Risk severity is determined from risk exposure (i.e., probability and impact) and timeframe ratings. It is used to prioritize the risk. Risks with a "High" severity have the highest priority for risk response activity and escalation, followed by "Medium" and then "Low". The severity rating for each risk is the intersection of that risk's exposure and timeframe, as presented in Table 29:

Table 29: Risk Severity Matrix

Timeframe	Exposure		
	High	**Medium**	**Low**
Short	High	High	Medium
Medium	High	Medium	Low
Long	Medium	Low	Low

7.3 Risk Management Worksheet

The EOL project was assessed and several project risks were identified. If the risks are not properly addressed, they will impact the project schedule, budget, and/or overall quality. Table 30 describes these risks in the Department of Finance's prescribed format. It includes the following columns:

- Risk: Risks that may occur during the EOL project.
- Probability: Likelihood of the risk occurring.
- Impact: Estimated negative impact on EOL project.
- Affected Elements: Project component(s) that will be impacted by the risk.
- Preventative Measures: Actions CDPH may take to minimize the potential of the risk occurring.
- Contingency Measures: Actions CDPH may take if the risk does occur.

Table 30: EOL Risk Management Worksheet

#	Risk	Proba-bility	Impact	Affected Elements	Preventative Measures	Contingency Measures
1	CDPH does not have experience in managing or participating in an IT project of this magnitude and cross-program nature.	High	High	Resources Schedule	• Retain the services of a PMP-certified Project Manager vendor. • Retain the services of an IPOC as well as an IV&V vendor. • Seek guidance from POS. • Develop and manage to Project Management Plan aligned with the standards defined by the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK). • Retain an ongoing maintenance contract with the Systems Integration vendor.	• Delay project start until appropriate Project Management and IPOC resources are retained.
2	Scope creep caused by internal or external stakeholders.	High	Medium	Schedule Budget	• Execute project scope management process. • Involve stakeholders in final requirements review. • Communicate project scope within programs and ITSD.	• Escalate scope issues to EOL Steering Committee, Project Director, and Program Directors, as appropriate.

#	Risk	Proba-bility	Impact	Affected Elements	Preventative Measures	Contingency Measures
3	New or changes to existing legislation or statewide budget priorities may impact business needs and functional requirements.	High	Low	Schedule Budget Scope	• Execute project scope management process. • Program Directors monitor upcoming bills and potential legislation that may impact EOL. • Map legislative changes to system modules and project phases to monitor potential impacts.	• Delay project until changes can be integrated into project plan. • Hire contracted resources to assist with the integration of changes. • Create addendum to Systems Integration vendor's contract for additional work.
4	CDPH staff does not accept changes in business processes.	Medium	Medium	Resources	• Ensure stakeholder involvement in analysis and design activities. • Manage on-going stakeholder communication in accordance to a defined Communi-cation Plan. • Ensure sufficient and appropriate training for users. • Escalate issues to Project Director, Steering Commit-tee, and/or Execu-tive Sponsor for their involvement in the resolution. • Conduct focus group session(s) with staff to understand their issues.	• Manage changes through attrition. • Redirect staff to different work activities. • Procure and implement modules of the system that will be supported by the staff.

#	Risk	Proba-bility	Impact	Affected Elements	Preventative Measures	Contingency Measures
5	Inability to standardize on new business processes/new system functionality due to individual and/or program unit interpretation of regulations, guidelines, branch or section policies, etc.	Medium	High	Scope Resources Schedule	• Conduct focus groups with staff to create standard interpretation of regulations, guidelines, policies and practices prior to procurement of the Systems Integration vendor. • Involve stakeholders and end users in analysis and design. • Ensure sufficient and appropriate training for all users. • Escalate issues to Project Director, Steering Committee, and/or Executive Sponsor for their involvement in the resolution.	• Delay project implementation. • Standardize only a subset of all common business processes.

#	Risk	Proba-bility	Impact	Affected Elements	Preventative Measures	Contingency Measures
6	Migration of data from HAL and other legacy systems encounters delays or requires additional resources.	High	Medium	Resources Schedule Budget	• Require that the Systems Integration vendor leads all data conversion activities. • Ensure the project's Data Cleansing and Conversion Plan identifies specific data cleansing and data conversion activities staff. • Retain contractors and/or student assistants to assist in data migration activities. • Ensure sufficient time and CDPH staff is allocated to the data conversion process.	• Do not migrate data from legacy systems during implementation; use legacy in parallel with new until the migration can be completed. • Migrate only portions of data.

#	Risk	Proba-bility	Impact	Affected Elements	Preventative Measures	Contingency Measures
7	CDPH and the participating programs do not have project team resources available when project starts.	High	High	Schedule Resources	• Begin project resource identification/allocation as soon as project funds are approved. • Communicate timing of when subject matter experts are needed. • Involve CDPH management in project team definition. • Escalate issues to Project Director, Executive Sponsor, and Steering Committee.	• Delay the start of the implementation. • Use a phased implementation approach by program.
8	CDPH does not have project facilities available when the project is ready to start.	Low	High	Schedule	• Begin facility search process as soon as funds are approved by the Department of Finance. • Escalate issues to Project Director, Executive Sponsor, and Steering Committee.	• Delay the start of the implementation. • Allow vendor to work off-site.
9	Unable to procure a suitable off-the-shelf product that meets CDPH's business needs.	Low	High	Budget Scope	• Perform market research. • Allow sufficient dollars for customization in project budget plus contingency.	• Stop project. • Reduce scope.

#	Risk	Proba-bility	Impact	Affected Elements	Preventative Measures	Contingency Measures
10	DTS support of the system's development environment impacts system integrator's ability to configure software in a timely manner.	Low	High	Schedule	• Involve DTS in the FSR, procurement, and implementation activities. • Inform DTS early in the project regarding the intent for the new development, environment, test, training, and production environments to reside at DTS.	• Contract with system integrator vendor to provide services.
11	New system's design or features are not compatible with HIPAA or other mandated requirements.	Low	High	Budget Scope	• Observe other system implementations at other client sites before selecting. • Stipulate compliance with these mandates within RFP requirements.	• Custom coding and/or workarounds to ensure compliance. CDPH will not compromise its compliance with any external mandates.
12	Existing IT support ends before new system is fully functional and acceptable (and has IT support in place).	Medium	High	Resources Budget	• Ensure current outside vendor contracts (e.g. Cooperative Personnel Services) are eligible for extension. • Ensure in-house legacy systems have an alternate support resource.	• Create addendum to outside vendor's contract for additional support. • If no in-house resource exists, either create a program workaround or contract with outside vendor for interim support.

#	Risk	Proba-bility	Impact	Affected Elements	Preventative Measures	Contingency Measures
13	Cost overruns during new system implementation.	Medium	High	Budget Scope	• Closely track and record project budget to actual costs at least monthly. • Escalate potential overruns to Project and Program Directors and Steering Committee early.	• Reduce scope to cut costs. • Identify alternative funding sources within CDPH. • Obtain approvals to request additional outside funding.

7.4 Risk Tracking and Control

The Risk Owner is responsible for planning appropriate risk response action and for tracking the status of the risk and the response activity. The Risk Owner reports any changes in risk status at the monthly project team meeting. The Risk Owner, with approval from the Risk Manager, determines the appropriate risk response strategy and actions plan.

7.4.1 Risk Response Strategy

The Risk Owner, with the approval of the Risk Manager, determines the appropriate risk response strategy from the options below:

- Research: Additional research will be taken prior to determining the appropriate strategy.
- Accept: If the project can continue and be successful with the anticipated impact of the risk, or if there is no practical way to avoid or mitigate the risk, the project may choose to accept the risk and expend no further resources managing it other than tracking the risk status.
- Avoid: Risk avoidance involves taking preventative steps to reduce the probability of the risk.
- Mitigate: Risk mitigation involves taking steps to reduce the impact of the risk. These steps can include actions to be taken immediately, and/or contingency plans to be implemented if a risk event occurs.

7.4.2 Action Planning

The Risk Owner, with the approval of the Risk Manager, determines the action plan to be taken to implement the selected strategy. Often a simple list of one or more action items, with responsibilities and due dates identified, will be an adequate plan. Some high severity risks may require more elaborate planning. For example a Microsoft

Project work plan and resource budget might be needed in response to a complex, high impact risk that seriously threatens the success of the project.

7.4.3 Risk Tracking

The Risk Owner records the risk title, ID, originator, origination date, owner, statement, context, probability, impact, severity, strategy, and action items of each risk in the project risk management database as well as a Risk Management Form. The Risk Manager summarizes the risks on the Risk Register.

The Risk Owner tracks the risk, including the status of each of the action items, and reports any changes at the monthly Risk Management meeting. The Risk Manager maintains the master copy of each Risk Management Form, records new events and actions, and documents the resulting changes to the risk's status.

All risks are tracked within a risk database. The database may be Microsoft Excel spreadsheet or a database included in a risk management tool, such as Risk Radar® [10]. The Risk Manager maintains the risk database and records new events, actions, and the resulting changes to risk status.

The EOL Project Manager will work with the Risk Owner to facilitate the resolution of project risks.

7.4.4 Risk Escalation

The Project Manager escalates risks to the Project Director, the Planning and Oversight Section (POS), and the EOL Steering Committee depending on risk severity, as indicated in the risk escalation matrix in Table 31.

Table 31: Risk Escalation Matrix

		Risk Severity		
		High	Medium	Low
Escalation	DOF	X		
	EOL Steering Committee	X	X	
	Project Director/POS	X	X	X

[10] Risk Radar® is a Microsoft Access® application that is used to document and manage risks in accordance with industry accepted Risk Management processes prescribed by the Software Engineering Institute (SEI).

The method of risk escalation is as follows:

- High, medium, and low severity risks are reported to the Project Director and the POS in regular project status reports.
- High and medium severity risks are reported to the EOL Steering Committee during Steering Committee Meetings.
- High severity risks are reported to the Department of Finance by the IPOC in monthly IPO Reports.

8.0 ECONOMIC ANALYSIS WORKSHEETS

This section contains Economic Analysis Worksheets (EAW) for those alternatives that satisfactorily meet the objectives and functional requirements. This section analyzes the costs associated with two alternatives for implementation of the Enterprise-wide On-line Licensing system. The two alternatives that would meet the minimum requirements are:

- Off-the-Shelf Software Product
- Custom-Developed Software Solution.

Economic analysis was not performed on the third alternative, Modify L&C's e-Licensing Management System (ELMS), for the following reasons:

- It is an existing custom-developed solution that lacks over 80% of the functionality required by the participating programs.
- It does not conform to CDPH's and DTS's three-tier architecture standard.
- It does not comply with the State's direction that production systems reside at a state Data Center.
- Total costs to enhance ELMS would not be less than the total cost to implement a new custom solution, for which an economic analysis has been developed.
- Implementing a proven, comprehensive, commercial solution rather than embarking on an enhancement project of ELMS would involve substantially less risk, as discussed in Section 5: Proposed Solution.

8.1 Existing System/Baseline Cost Worksheet

The following tables detail the line items in the Existing System/Baseline Costs Worksheet.

Table 32: Existing System/Baseline Cost – Continuing IT Costs

Line Item	Description
Staff	Currently there are 23.0 PYs supporting the various IT systems of the five participating programs. These 23.0 PYs account for $2,329,460 at current salary and benefits rates, and include the following 6.0 PYs who support RHB but report to Departmental or Divisional IT units (not the programs): • CDPH Information Technology Services Division (ITSD) currently provides 1.5 PYs to RHB in support of the HAL system. (This is in addition to staff that support HAL for other units not participating in this FSR). • CDPH ITSD currently provides 0.5 PYs to RHB for general infrastructure support of RHB's existing server and miscellaneous activities (e.g., mailing billing notices). • Division of Food, Drug, and Radiation Safety (DFDRS) Information Technology unit currently provides 4.0 PYs to RHB in support of existing MS Access databases, desktop support and LAN administration services.
Data Center Services	The state's Department of Technology Services (DTS) data center costs associated with the HAL system that are charged to RHB are currently estimated at $156,341 per year. The complete costs for HAL are shared across three organizations within CDPH.
Other	Operating Expenses and Equipment (OE&E) costs for the 23.0 PYs, at $9,900 per PY, currently cost the Department $227,700 per fiscal year.

Table 33: Existing System/Baseline Cost: Continuing Program Costs

		- Program Budget -		
Program Area	**PYs**	**Staff**	**Other**	**Total**
FDB	161.2	17,216,000	3,352,000	20,568,000
RHB	* 139.0	19,677,000	3,487,000	23,164,000
DWOCP	9.1	1,213,000	150,000	1,363,000
SDWS	90.9	10,350,000	2,057,000	12,407,000
MWMP	14.9	1,631,000	378,000	2,009,000
Total staff including IT	**415.1**	**50,087,000**	**9,424,000**	**59,511,000**
IT only	23	2,329,460	384,041	2,713,501
Total program (non-IT) staff	**392.1**	**47,757,540**	**9,039,959**	**56,797,499**

* These are the 133 RHB program staff plus the 6.0 PYs outside of RHB who are dedicated to RHB IT support, and paid for via allocated chargebacks to RHB.

8.2 Proposed Alternative: Off-the-Shelf Software Product

CDPH has analyzed the operational and financial benefits that this proposed EOL solution would offer.

Each participating program has conducted a thorough analysis of the workload effects that are expected to occur if a packaged software solution were to be in place that meets the Functional Requirements detailed in Section 3: Business Case.

In addition, project costs of implementing the EOL solution have been developed based on estimates provided by both internal sources (e.g. for state staffing costs) as well as commercial vendors (e.g. software license costs). DTS costs are based on the DTS Rate Schedule effective November 2007. Personnel costs are based on the published California State Civil Service Pay Scales - Online Manual 54th Edition (Pay Scales/PIE Updated 10/31/2007), and include the burden rate for employment benefits and taxes.

Vendor costs were averaged among the three cost estimates provided by commercial vendors of known candidate COTS/MOTS solutions, to arrive at estimates used in these EAWs. For this business-based procurement, it is understood that actual vendor costs are not fully known, and will not be known until receipt of vendor proposals during the competitive procurement phase. Vendor cost estimates were all within 50% of each other, providing a certain level of comfort regarding the estimates.

The effects on workload were estimated by each program's management, using the following methodology:

Steps followed by CDPH management of the respective programs

1. In view of today's current situation and processes, consider the processes that would be affected if the Functional Requirements detailed in Section 3: Business Case were being met by a new system.
2. Next, consider the specific effects that would occur within the overall workload of the program, as a result of the new system – steps eliminated, etc.
3. Quantify the resulting effect in terms of specific PY reductions, by position, where applicable.

The results obtained by the above methodology are as follows:

Food and Drug Program

The Food and Drug Branch estimates that the following activities will be directly affected by having such a solution in place:

Activities affected: Processing applications, data entry, preparing renewal, late & invalidation notices, trouble shooting incomplete applications, answering calls/questions, and cashiering.

The current staff effort for these activities is as follows:

Desk/Activity	Positions	Annual Cost
PFR Desk	1.0 Staff Services Analyst	$58,338
Water Desk	1.0 Staff Services Analyst	$58,338
Cannery/Organic Desk	0.5 Mgmt Services Technician	$47,557
Drug/Device Desk	1.0 Staff Services Analyst	$58,338
HMDR Desk	1.0 Staff Services Analyst	$58,338
Cashier	1.0 Staff Services Analyst	$58,338
Program Filing	1.0 Student Assistant (40 Hrs/Wk)	$17,760
Folding Notices/Stuffing Envelopes	1.0 Student Assistant (40 Hrs/Wk)	$17,760
Processing Incoming Mail	1.0 Student Assistant (40 Hrs/Wk)	$17,760
Total Staff	**8.5 FTE**	**$392,527**
OE&E		**$84,150**

Supply Material*	Number of Units Annually	Annual Cost
Window Envelopes	19,351	$872
Reams of Paper (for renewals, apps)	180 X $2.16	$388
Colored Return Envelopes	19,351	$3,672
Printer Ink Cartridges	1 Cartridge	$235
Postage (Renewal, Late, Invalid)	19,351 X $ 0.373	$7,217
		$12,384

* For Renewal, Late & Invalid Notices

Under the new system, the corresponding workload is estimated to be as follows:

Effect of changes: Internet application completion, e-mail of renewal and late notices, electronic payment on-line, mail hard copy invalid notices, answering calls/questions and minimal cashiering.

Desk/Activity	**Positions**	**Annual Cost**
Food Program Desks	1.0 Staff Services Analyst	$58,338
Drug/Device/HMDR Desks	1.0 Staff Services Analyst	$58,338
Cashier	0.5 Staff Services Analyst	$29,169
Program Filing	0.25 Student Assistant (10 Hrs/Wk)	$4,440
Folding Invalid Notices - Stuffing Envelopes	0.25 Student Assistant (10 Hrs/Wk)	$4,440
Processing Incoming Mail	0.25 Student Assistant (10 Hrs/Wk)	$4,440
Total Staff	**3.25 FTE**	**$159,165**
OE&E		**$32,175**

Supply Material*	**Number of Units Annually**	**Annual Cost**
Window Envelopes	1,453	$384
Reams of Paper (for renewals, apps)	10.3 X $2.16	$22
Colored Return Envelopes	1,453	$918
Printer Ink Cartridges	0.10 Cartridge	$24
Postage (Renewal, Late, Invalid)	1,453 X $0.373	$542
		$1,890

* For Invalid Notices Only. All others handled through Internet

		- Program Budget -		
	PYs	**Staff**	**Other**	**Total**
FDB summary of anticipated savings	5.25	233,362	62,469	295,831

Radiation Safety Program

The Radiologic Health Branch estimates that the following activities will be directly affected by having such a solution in place:

Activities affected: HAL system support, server/misc. support, MS Access database support, desktop support and LAN administration.

The current staff effort for these activities is as follows:

Desk/Activity	Positions	Annual Cost
IT support provided by DFDRS	2.0 Assistant ISA	$182,555
IT support provided by DFDRS	2.0 Staff ISA	$214,813
CDPH ITSD (HAL Support)	1.5 Staff ISA	$161,110
CDPH ITSD (Infrastructure Support)	0.1 Staff ISA	$10,741
CDPH ITSD (General Support)	0.4 Staff ISA	$42,963
Total Staff	**6.0 FTE**	**$612,182**
Total OE&E		**$59,400**

Chargeback costs paid to DTS for HAL support are currently estimated at $156,341 per year.

Under the new system, the corresponding workload is estimated to be as follows:

Effect of changes: Eliminated HAL system support, reduced IT support needs in the other affected areas.

Desk/Activity	Positions	Annual Cost
IT support provided by DFDRS	1.0 Assistant ISA	$91,277
IT support provided by DFDRS	1.0 Staff ISA	$107,407
CDPH ITSD (Infrastructure Support)	0.1 Staff ISA	$10,741
CDPH ITSD (General Support)	0.4 Staff ISA	$42,963
Total Staff	**2.5 FTE**	**$252,388**
Total OE&E		**$24,750**

Chargeback costs paid to DTS for HAL support would be eliminated.

		- Program Budget -		
	PYs	Staff	Other	Total
RHB summary of anticipated savings	3.50	359,794	190,991	550,785

Drinking Water Operator Certification Program

DWOCP estimates that the following activities will be directly affected by having such a solution in place:

Activities affected: Sending out renewal notices, exam notices, and pass/fail letters. Receiving and opening mail, processing fees, entering data, preparing and sending certificates, creating folders. Trouble shooting incomplete applications, answering calls/questions, and cashiering.

The current staff effort for these activities is as follows:

Desk/Activity	Positions	Annual Cost
Front Office	1.0 Word Processing Technician	$44,011
Renewals	0.33 Mgmt Services Technician	$16,228
Front Office & Tech Ops	1.6 Office Technician	$79,068
Total Staff	**2.93 FTE**	**$139,308**
Total OE&E		**$29,007**

Under the new system, the corresponding workload is estimated to be as follows:

Effect of changes: 10% of applicants use Internet to submit applications and use electronic payment on-line. Continue sending out renewal notices, exam notices, and pass/fail letters. Continue receiving and opening mail, processing fees, entering data, preparing and sending certificates, creating folders. Continue trouble shooting incomplete applications, answering calls/questions, and cashiering.

Desk/Activity	Positions	Annual Cost
Front Office	0.91 Word Processing Technician	$40,050
Renewals	0.33 Mgmt Services Technician	$16,228
Front Office & Tech Ops	1.54 Office Technician	$76,103
Total Staff	**2.78 FTE**	**$132,382**
Total OE&E		**$27,522**

Note: Assumption of 10% of applicants using Internet and on-line payments is based on type of applicants. In today's environment, Drinking Water Operators typically do not require use of computers in job assignments. Therefore, future savings could potentially increase if computer use among this profession increases.

		- Program Budget -		
	PYs	Staff	Other	Total
DWOCP summary of anticipated savings	0.15	6,926	1,485	8,411

Safe Drinking Water Systems Program

The SDWS Program estimates that the following activities will be directly affected by having such a solution in place:

Activities affected: Sending out invoices; receiving and opening mail, processing payments into the payment tracking system, cashiering, preparing and sending revised invoices, calculating cap charges and rebates, creating folders and filing. Answering inquiries on billings and preparing reports and responses.

The current staff effort for these activities is as follows:

Desk/Activity	Positions	Annual Cost
Billing Unit	1.0 Staff Service Analyst	$60,323
Billing Unit	1.0 Mgmt Svcs Technician	$49,177
Billing Unit	1.0 Office Technician	$49,418
TAS coordinator	1.0 AGPA	$80,962
Misc field staff (appl. Fee/Penalties)	1.0 Office Technician	$49,418
Misc field staff (permit issuance)	16.0 Sanitary Engineer	$1,412,599
Total Staff	**21 FTE**	**$1,701,897**
Total OE&E		**$207,900**

Under the new system, the corresponding workload is estimated to be as follows:

Effect of changes: 25% of invoices processed on the Internet and use on-line payment instead of the current paper system. Continue receiving and opening mail, processing payments, entering data, calculating cap charges and rebates, creating folders and filing. Continue answering inquiries on billings, and in preparing reports and responses.

Desk/Activity	Positions	Annual Cost
Billing Unit	1.0 Staff Service Analyst	$60,323
Billing Unit	.90 Mgmt Svcs Technician	$44,259
Billing Unit	.90 Office Technician	$44,476
TAS coordinator	1.0 AGPA	$80,962
Misc field staff (appl. Fee/Penalties)	.70 Office Technician	$34,592
Misc field staff (permit issuance)	16.0 Sanitary Engineer	$1,412,599
Total Staff	**20.50 FTE**	**$1,677,212**
Total OE&E		**$202,950**

Note: Assumption of 25% of applicants using Internet and on-line payments is based on types of systems on our inventory. Some smaller systems may not have Internet access to take advantage of this feature now, although this will change in the future. Also, various field staff handle initial intake of small water system permit application fees and invoicing of penalties. Various classifications are involved in these activities.

		- Program Budget -		
	PYs	Staff	Other	Total
SDWS summary of anticipated savings	0.5	24,685	4,950	29,635

Medical Waste Management Program

The MWMP Program estimates that the following activities will be directly affected by having such a solution in place:

Activities affected: Processing applications, data entry, preparing renewal, late & overdue notices, trouble-shooting incomplete applications, answering calls/questions, and cashiering.

The current staff effort for these activities is as follows:

Desk/Activity	Positions	Annual Cost
EMB Branch Reception	0.8 Office Assistant	$33,016
ERWM Section Reception	0.8 Office Technician	$39,534
ERWM Admin. Support	0.5 Staff Services Analyst	$30,161
Medical Waste Program	0.2 Environmental Scientist I	$14,598
Total Staff	**2.3 FTE**	**$117,309**
Total OE&E		**$22,770**

Under the new system, the corresponding workload is estimated to be as follows:

Effect of changes: Internet application completion, e-mail of renewal and late notices, electronic payment on-line, mail hard copy invalid notices, answering calls/questions and minimal cashiering.

Desk/Activity	Positions	Annual Cost
EMB Branch Reception	0.7 Office Assistant	$28,889
ERWM Section Reception	0.7 Office Technician	$34,592
ERWM Admin. Support	0.5 Staff Services Analyst	$30,161
Medical Waste Program	0.1 Environmental Scientist I	$7,299
Total Staff	**2.0 FTE**	**$100,942**
Total OE&E		**$19,800**

		- Program Budget -		
	PYs	Staff	Other	Total
MWMP summary of anticipated savings	0.3	16,368	2,970	19,338

The results of the workload analysis are summarized here:

Table 34: Proposed System: Saved PYs and Costs

		- Program Budget -		
Program Area	**PYs**	**Staff**	**Other**	**Total**
FDB	5.25	233,362	62,469	295,831
RHB	3.5	359,794	190,991	550,785
DWOCP	0.15	6,926	1,485	8,411
SDWS	0.5	24,685	4,950	29,635
MWMP	0.3	16,368	2,970	19,338
Total staff including IT	**9.7**	**641,135**	**262,865**	**904,000**
IT staff	3.5	359,794	190,991	550,785
Total program (non-IT) staff	**6.2**	**281,341**	**71,874**	**353,215**

In summary, CDPH projects a gross savings of $904,000 – nearly a million dollars per year – in annual operating costs, once the effects of implementing the EOL solution have been realized.

The resulting PYs and costs are as follows:

Table 35: Proposed System: Resulting PYs and Costs

		- Program Budget -		
Program Area	**PYs**	**Staff**	**Other**	**Total**
FDB	155.95	16,982,638	3,289,531	20,272,169
RHB	135.5	19,317,206	3,296,009	22,613,215
DWOCP	8.95	1,206,074	148,515	1,354,589
SDWS	90.4	10,325,315	2,052,050	12,377,365
MWMP	14.6	1,614,632	375,030	1,989,662
Total staff including IT	**405.4**	**49,445,865**	**9,161,135**	**58,607,000**
IT only	19.5	1,969,666	193,050	2,162,716
Total program (non-IT) staff	**385.9**	**47,476,199**	**8,968,085**	**56,444,284**

The following tables describe the resulting costs as shown in the line items in the Proposed Alternative: Off-the-Shelf Software Product worksheet, taking into account all of the above analysis.

As shown in Section 6.5.3 Project Approach and Schedule, the project activities are expected to last for **37 months**; implementation of the first set of programs (the DFDRS programs: FDB and RHB) is expected to last for **13 months**; implementation of all other programs (the DDWEM programs: DWOCP, SDWS, and MWMP) is expected to last for **8 months**; the two implementation phases together are expected to last for **21 months**.

Table 36: Proposed Alternative – One-Time IT Project Costs

Line Item	Description
Staff	• CDPH ITSD PMO will provide 0.2 PYs for 37 months to assist with procurement activities and as Program Director. • CDPH ITSD will provide 1.0 PYs for 13 months for project infrastructure support and general support. • DFDRS IT will provide 0.5 PY for 13 months (0.25 of each of two professionals) to assist in data mapping and conversion from existing MS Access and MS Excel tools to EOL; develop ad hoc reports; define and maintain security access; and participate in testing, training, and knowledge transfer activities. • CDPH ITSD will provide 0.5 PYs for 13 months to assist in data mapping and conversion from the HAL system. • FDB IT will provide 0.5 PYs for 13 months (0.25 of each of two professionals) to assist in data mapping and conversion from existing FDB systems. • The DDWEM programs will provide 0.7 PY for 8 months (0.1 to 0.2 of each of several professionals) to assist in data mapping and conversion from existing MS Access and MS Excel systems and tools to EOL; develop ad hoc reports; define and maintain security access; and participate in data mapping and conversion, testing, training, and knowledge transfer activities. • CDPH PMO will provide 0.5 PYs for 21 months to serve as Contract Oversight Manager.

Hardware Purchase	CDPH will procure the following servers. This size was deemed sufficient by the vendors in discussions, based on their experience. • 1 Development Server = $15,246 • 3 Test/Training Servers = $30,395 • 4 Production Servers = $44,527
Software Purchase/License	CDPH will procure the EOL off-the-shelf software product at a cost of $679,288 (the average of the vendor price estimates including a 15% cost contingency).
Telecommuni-cations	No project-specific one-time costs.
Contract Services	• CDPH will retain a Systems Integration vendor to configure the off-the-shelf software product; work with ITSD and DTS to establish the EOL technology environments; integrate external software products (as needed); perform data conversion; perform testing; coordinate and lead user acceptance testing; and perform training at an average hourly rate of $150 for the months specified for a total cost of $2,587,200 (includes a 10% cost contingency). • CDPH will retain a vendor to provide project management services to oversee the management and execution of the entire EOL project at an average hourly rate of $150 for the months specified at a total cost of $499,620 (includes a 10% cost contingency). • CDPH will retain a vendor to provide Independent Project Oversight Contractor (IPOC) services as required by state policy at an average hourly rate of $125 for the months specified for a total cost of $167,200 (includes a 10% cost contingency). • CDPH will retain a vendor to provide Independent Verification and Validation (IV&V) services as required by state policy at an average hourly rate of $150 for the months specified for a total cost of $200,640 (includes a 10% cost contingency).

Contract Services (cont'd)	• CDPH will retain a vendor to provide acquisition services to assist in the development of the Systems Integration vendor solicitation document and procurement at an average hourly rate of $130 for the months specified for a total cost of $326,040 (includes a 10% cost contingency).
Data Center Services	• DTS will provide services for the EOL development, test/training environment at a total cost of $35,820. Services will include building, deploying, maintaining, and performing backups of the servers. • DTS will provide services for the EOL production environment at a total cost of $20,165. Services will include building, deploying, maintaining, and performing backups of the production servers.
Agency Facilities	No additional costs are anticipated.
Other	No additional costs are anticipated.

Table 37: Proposed Alternative – Continuing IT Project Costs

Line Item	Description
Staff	Continuing support of the new system will be provided as follows: • The 0.5 PYs from CDPH ITSD that provide general infrastructure support of RHB's existing server and environment will be retained. • The 4.0 PYs that DFDRS IT that maintain current RHB MS Access and related systems will be reduced to 2.0 PYs to serve as first-level help desk for EOL; maintain EOL security; maintain standard and ad hoc reports; and provide user support. The other 2.0 PYs will no longer be needed. • The 1.5 PYs from CDPH ITSD that provide HAL support for RHB will no longer be needed. (Other HAL support will still be needed for other units not participating in this FSR.) • The 3.0 PYs within FDB IT will serve as IT support for FDB on the new system.
Hardware Lease / Maintenance	Maintenance for development, testing/training and production servers located at DTS are included in Data Center Services costs.
Software Maintenance/ Licenses	User and software licenses for the EOL off-the-shelf software product at an annual cost of $164,744, which includes a 10% contingency. This includes software licenses for all components necessary to meet the stated functional requirements (whether met by the base product or add-on module) including GIS capability, report writer, online bill pay, etc. This solution design element will become known during the competitive procurement.
Telecommuni-cations	CDPH will maintain a dedicated T-1 line to DTS for EOL at an annual cost of $13,800.
Contract Services	CDPH will retain the Systems Integration vendor for post-implementation maintenance at an annual cost of $158,400. This covers a base minimum of 12 months of support (Stage 6.1) after the first implementation go-live date (includes a 10% cost contingency).

Data Center Services	DTS will provide services (including administrative fees) for the EOL development, test/training environment at an annual cost of $105,547, production environment at an annual cost of $87,292, and database support at annual cost of $27,073.
Agency Facilities	No additional costs are anticipated.
Other	No additional costs are anticipated.

Table 38: Proposed Alternative – Continuing Existing Costs

Line Item	Description
Information Technology Staff	Current IT support not related to licensing functions (14.0 PYs) will continue.
Other IT Costs	• Current data center costs related to RHB's utilization of the HAL system will be eliminated upon implementation of EOL, for an annual cost savings of $156,341. • OE&E costs for IT staff will reduce proportionately to the staff reduction.
Program Staff	• No additional program staff will be added as a result of the project. • Upon full implementation, EOL will yield operational efficiencies that will save program staff costs for each program, in the amounts described above.
Other Program Costs	OE&E costs for program staff will reduce proportionately to the staff reduction.

The following table summarizes IT classifications currently supporting the licensing-related needs of the five programs, along with anticipated needs for the new EOL environment. The new system itself is anticipated to require less IT support than existing systems to be replaced; therefore, total IT support staffing will be reduced.

Table 39: IT Classifications Supporting Licensing-Related Activities

Classification	Existing	One-Time (Project)	Contin-uing	Justification
Senior Information Systems Analyst (Supervisor)	1	.25	1	One-time: participate in business process analysis and recommendation of process changes; participate in conversion analysis and "fit" confirmation; participate in review of planned configuration of EOL system; participate in data mapping and conversion from existing MS Access and MS Excel systems and tools to new system; participate in development of ad hoc reports; participate in security definition; participate in testing, training, and knowledge transfer activities. Continuing: Reduction from 9.0 PY to 5.5 PY is due to reduced IT support needs due to new EOL system, as detailed in Section 8.2 of the FSR, p. 154.
Staff Information Systems Analyst (Specialist)	6	2	3.5	
Assistant Information Systems Analyst (Specialist)	2	.25	1	
Various IT (temporary redirect from support of non-licensing functions)		.7		Temporary redirect – data mapping and conversion; develop ad hoc reports; security access; and general project support activities

The 0.7 PY loaned by the DDWEM programs will be from one-time redirections of resources not currently supporting licensing-related activities.

8.3 Alternative #1: Custom Development

The following table describes the line items in Alternative #1: Custom Solution worksheet.

In the estimated project schedule, the project activities are expected to last for **44 months**; implementation of the first set of programs (the DFDRS programs: FDB and RHB) is expected to last for **15 months**; implementation of all other programs (the DDWEM programs: DWOCP, SDWS, and MWMP) is expected to last for **11 months**; the two implementation phases together are expected to last for **26 months**.

Table 40: Alternative #1 - One-Time IT Project Costs

Line Item	Description
Staff	• CDPH ITSD PMO will provide 0.2 PYs for 44 months to assist with procurement activities and as Program Director. • CDPH ITSD will provide 1.0 PYs for 26 months for project infrastructure support and general support. • DFDRS IT will provide 0.5 PY for 15 months to assist in data mapping and conversion from existing MS Access and MS Excel systems and tools to EOL; develop ad hoc reports; define and maintain security access; and participate in testing, training, and knowledge transfer activities. • CDPH ITSD will provide 0.5 PYs for 15 months to assist in data mapping and conversion from the HAL system. • FDB IT will provide 0.5 PYs for 15 months to assist in data mapping and conversion from the existing FDB systems. • The DDWEM programs will provide 0.7 PY for 11 months to assist in data mapping and conversion from existing MS Access and MS Excel systems and tools to EOL; develop ad hoc reports; define and maintain security access; and participate in data mapping and conversion, testing, training, and knowledge transfer activities. • CDPH ITSD PMO will provide 0.5 PYs for 26 months to serve as Contract Oversight Manager.

Hardware Purchase	CDPH will procure the following servers (costs include software): • 1 Development Server = $15,246 • 3 Test/Training Servers = $30,395 • 4 Production Servers = $44,527
Software Purchase/License	• CDPH will procure five copies of a report writer tool at a total cost of $3,416 (includes a 15% cost contingency). • CDPH will procure GIS software (if not provided by the off-the-shelf product) at a total cost of $23,000 (includes a 15% cost contingency). • CDPH will procure barcode software (if not provided by the off-the-shelf product) at a total cost of $1,150 (includes a 15% cost contingency). • CDPH will procure ePay software (if not provided by the off-the-shelf product) at a total cost of $230 (includes a 15% cost contingency). • CDPH will procure Oracle Enterprise Edition software (if not provided by the off-the-shelf product) at a total cost of $37,584 (includes a 15% cost contingency).
Telecommuni-cations	No project-specific one-time costs.
Contract Services	• CDPH will retain a Systems Integration vendor to design, develop, and implement the custom solution; integrate external software products; work with ITSD and DTS to establish the EOL technology environments; perform data conversion; perform testing; coordinate and lead user acceptance testing; and perform training at an average hourly rate of $150 for the months specified for a total cost of $7,807,800 (includes a 10% cost contingency). • CDPH will retain a vendor to provide project management services to oversee the management and execution of the entire EOL project at an average hourly rate of $150 for the months specified at a total cost of $615,120 (includes a 10% cost contingency).

Contract Services (cont'd)	• CDPH will retain a vendor to provide Independent Project Oversight Contractor (IPOC) services as required by state policy at an average hourly rate of $125 for the months specified for a total cost of $202,400 (includes a 10% cost contingency). • CDPH will retain a vendor to provide Independent Verification and Validation (IV&V) services as required by state policy at an average hourly rate of $150 for the months specified for a total cost of $242,880 (includes a 10% cost contingency). • CDPH will retain a vendor to provide acquisition services to assist in the development of the Systems Integration vendor solicitation document and procurement at an average hourly rate of $130 for the months specified for a total cost of $417,560 (includes a 10% cost contingency).
Data Center Services	• DTS will provide services for the EOL development, test/training environment at a total cost of $35,820. Services will include building, deploying, maintaining, and performing backups of the servers. • DTS will provide services for the EOL production environment at a total cost of $20,165. Services will include building, deploying, maintaining, and performing backups of the production servers.
Agency Facilities	No additional costs are anticipated.
Other	No additional costs are anticipated.

Table 41: Alternative #1 - Continuing IT Project Costs

Line Item	Description
Staff	ITSD PMO will provide 0.1 PY to serve as Contract Manager during the Systems Integration vendor maintenance & operations period.
Hardware Lease / Maintenance	Maintenance for development, testing/training and production servers located at DTS are included in Data Center Services costs.
Software Maintenance/ Licenses	• Software maintenance on five copies of a report writer tool at an annual cost of $512. • Software maintenance on GIS software at an annual cost of $3,450. • Software maintenance on Barcode software at an annual cost of $173. • Software maintenance on ePay software at an annual cost of $414. • Software maintenance on Oracle software at an annual cost of $20,240.
Telecommunications	CDPH will maintain a dedicated T-1 line to DTS for EOL at an annual cost of $13,800.
Contract Services	RHB will retain the Systems Integration vendor for post-implementation maintenance at 5 percent of total implementation costs for an annual cost of $385,770. This covers a base minimum of 12 months of support after the first implementation go-live date.
Data Center Services	DTS will provide services (including administrative fees) for the EOL development, test/training environment at an annual cost of $77,603, production environment at an annual cost of $136,118, and database support at annual cost of $27,073.
Agency Facilities	No additional costs are anticipated.
Other	No additional costs are anticipated.

Table 42: Alternative #1 - Continuing Existing Costs

Line Item	Description
Information Technology Staff	• The 1.5 PYs from CDPH ITSD that provide HAL support for RHB will no longer be needed. (Other HAL support will still be needed for other units not participating in this FSR.) • The 0.5 PYs from CDPH ITSD that provide general infrastructure support of RHB's existing server and environment will be retained. • The 4.0 PYs that DFDRS IT that maintain current RHB MS Access and related systems will be reduced to 2.0 PYs in order to serve as first-level help desk for EOL; maintain EOL security; maintain standard and ad hoc reports; and provide user support. The other 2.0 PYs will no longer be needed.
Other IT Costs	• Current data center costs related to RHB's utilization of the HAL system will be eliminated upon implementation of EOL, for an annual cost savings of $156,341. • OE&E costs for IT staff will reduce proportionately to the staff reduction.
Program Staff	• No additional program staff will be added as a result of the project. • Upon full implementation, EOL will yield operational efficiencies that will save program staff costs for each program, in the amounts described above. The savings will be the same as in the proposed alternative, since both alternatives are assumed to meet the same functional requirements.
Other Program Costs	OE&E costs for program staff will reduce proportionately to the staff reduction.

Conclusion

Based on this analysis, Alternative #1 – Custom Solution would cost the state several million dollars more than the Proposed Alternative, with no additional benefit.

EXISTING SYSTEM/BASELINE COST WORKSHEET

All costs to be shown in whole (unrounded) dollars.

Department: California Department of Public Health

Date Prepared: 1/15/08

Project: Enterprise-wide On-line Licensing

	FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12		FY 2012/13		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
Continuing Information Technology Costs												
Staff (salaries & benefits)	23.0	2,382,881	23.0	2,382,881	23.0	2,382,881	23.0	2,382,881	23.0	2,382,881	**115.0**	**11,914,406**
Hardware Lease/Maintenance		0		0		0		0		0		**0**
Software Maintenance/Licenses		0		0		0		0		0		**0**
Contract Services		0		0		0		0		0		**0**
Data Center Services		156,341		156,341		156,341		156,341		156,341		**781,706**
Agency Facilities		0		0		0		0		0		**0**
Other		227,700		227,700		227,700		227,700		227,700		**1,138,500**
Total IT Costs	**23.0**	**2,766,922**	**23.0**	**2,766,922**	**23.0**	**2,766,922**	**23.0**	**2,766,922**	**23.0**	**2,766,922**	**115.0**	**13,834,612**
Continuing Program Costs:												
Staff	392.1	47,704,119	392.1	47,704,119	392.1	47,704,119	392.1	47,704,119	392.1	47,704,119	**1960.5**	**238,520,594**
Other		9,039,959		9,039,959		9,039,959		9,039,959		9,039,959		**45,199,794**
Total Program Costs	**392.1**	**56,744,078**	**392.1**	**56,744,078**	**392.1**	**56,744,078**	**392.1**	**56,744,078**	**392.1**	**56,744,078**	**1960.5**	**283,720,388**
TOTAL EXISTING SYSTEM COS	**415.1**	**59,511,000**	**415.1**	**59,511,000**	**415.1**	**59,511,000**	**415.1**	**59,511,000**	**415.1**	**59,511,000**	**2075.5**	**297,555,000**

PROPOSED ALTERNATIVE: Off-the-Shelf Software Product

All Costs Should be shown in whole (unrounded) dollars.

Date Prepared: 1/15/08

Department: California Department of Public Health

Project: Enterprise-wide On-line Licensing

	FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12		FY 2012/13		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
One-Time IT Project Costs												
Staff (Salaries & Benefits)	0.4	41,707	4.5	471,354	4.9	480,261	0.3	27,765	0.0	0	10.0	1,021,087
Hardware Purchase		0		90,168		0		0		0		90,168
Software Purchase/License		0		679,288		0		0		0		679,288
Telecommunications		0		0		0		0		0		0
Contract Services												
Software Customization		0		1,134,000		1,239,000		126,000		0		2,499,000
Project Management		72,000		172,800		230,400		19,200		0		494,400
Project Oversight		48,000		48,000		48,000		4,000		0		148,000
IV&V Services		57,600		57,600		57,600		4,800		0		177,600
Other Contract Services		261,000		0		0		0		0		261,000
TOTAL Contract Services		438,600		1,412,400		1,575,000		154,000		0		3,580,000
Data Center Services		0		32,564		18,332		0		0		50,896
Agency Facilities		0		0		0		0		0		0
Other		0		0		0		0		0		0
Total One-time IT Costs	**0.4**	**480,307**	**4.5**	**2,685,774**	**4.9**	**2,073,593**	**0.3**	**181,765**	**0.0**	**0**	**10.0**	**5,421,439**
Continuing IT Project Costs												
Staff (Salaries & Benefits)	0.0	0	0.0	0	3.2	348,763	5.5	597,880	5.5	597,880	14.2	1,544,523
Hardware Lease/Maintenance												630,411
Software Maintenance/Licenses		0		0		89,535		143,256		143,256		376,046
Telecommunications		0		9,000		12,000		12,000		12,000		45,000
Contract Services		0		0		90,000		54,000		0		144,000
Data Center Services		0		70,329		160,242		199,920		199,920		630,411
Agency Facilities		0		0		0		0		0		0
Other		0		0		0		0		0		0
Total Continuing IT Costs	**0.0**	**0**	**0.0**	**79,329**	**3.2**	**700,540**	**5.5**	**1,007,055**	**5.5**	**953,055**	**14.2**	**2,739,979**
Total Project Costs	**0.4**	**480,307**	**4.5**	**2,765,103**	**8.1**	**2,774,133**	**5.8**	**1,188,820**	**5.5**	**953,055**	**24.3**	**8,161,418**
Continuing Existing Costs												
Information Technology Staff	23.0	2,382,881	23.0	2,382,881	18.0	1,851,670	14.0	1,423,005	14.0	1,418,530	92.1	9,458,966
Other IT Costs		384,041		384,041		243,755		139,013		138,600		1,289,450
Total Continuing Existing IT Costs	**23.0**	**2,766,922**	**23.0**	**2,766,922**	**18.0**	**2,095,424**	**14.0**	**1,562,017**	**14.0**	**1,557,130**	**92.1**	**10,748,416**
Program Staff	392.1	47,704,119	392.1	47,704,119	389.0	47,358,111	386.0	47,066,982	385.9	47,062,984	1945.1	236,896,315
Other Program Costs		9,039,959		9,039,959		9,009,640		8,979,362		8,978,579		45,047,499
Total Continuing Existing Program Costs	**392.1**	**56,744,078**	**392.1**	**56,744,078**	**389.0**	**56,367,751**	**386.0**	**56,046,345**	**385.9**	**56,041,563**	**1945.1**	**281,943,814**
Total Continuing Existing Costs	**415.1**	**59,511,000**	**415.1**	**59,511,000**	**407.1**	**58,463,175**	**400.0**	**57,608,362**	**399.9**	**57,598,692**	**2037.2**	**292,692,230**
TOTAL ALTERNATIVE COSTS	**415.5**	**59,991,307**	**419.6**	**62,276,103**	**415.2**	**61,237,308**	**405.8**	**58,797,182**	**405.4**	**58,551,748**	**2061.5**	**300,853,648**
INCREASED REVENUES		0		0		0		0		0		**0**

ALTERNATIVE #1: **Custom Solution**

All Costs Should be shown in whole (unrounded) dollars.

Date Prepared: 1/15/08

Department: California Department of Public Health

Project: Enterprise-wide On-line Licensing

	FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12		FY 2012/13		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
One-Time IT Project Costs												
Staff (Salaries & Benefits)	0.4	41,707	3.5	358,656	7.4	744,418	4.0	340,937	0.0	0	15.3	1,485,719
Hardware Purchase				90,168		0		0		0		90,168
Software Purchase/License		0		56,852		0		0		0		56,852
Telecommunications		0		0		0		0		0		0
Contract Services												
Software Customization		0		1,260,000		3,192,000		2,730,000		0		7,182,000
Project Management		36,000		117,000		230,400		172,800		0		556,200
Project Oversight		48,000		48,000		48,000		36,000		0		180,000
IV&V Services		57,600		57,600		57,600		43,200		0		216,000
Other Contract Services		301,600		36,400		0		0		0		338,000
TOTAL Contract Services		443,200		1,519,000		3,528,000		2,982,000		0		8,472,200
Data Center Services		0		32,564		18,332		0		0		50,896
Agency Facilities		0		0		0		0		0		0
Other		0		0		0		0		0		0
Total One-time IT Costs	**0.4**	**484,907**	**3.5**	**2,057,240**	**7.4**	**4,290,750**	**4.0**	**3,322,937**	**0.0**	**0**	**15.3**	**10,155,835**
Continuing IT Project Costs												
Staff (Salaries & Benefits)	0.0	0	0.0	268,456	3.3	625,486	5.6	609,576	5.6	609,576	14.5	2,113,095
Hardware Lease/Maintenance		0		0		0		0		0		0
Software Maintenance/Licenses		0		21,556		21,556		21,556		21,556		86,222
Telecommunications		0		6,000		12,000		12,000		12,000		42,000
Contract Services		0		0		189,000		350,700		350,700		890,400
Data Center Services		0		23,988		103,299		194,292		194,292		515,871
Agency Facilities		0		0		0		0		0		0
Other		0		0		0		0		0		0
Total Continuing IT Costs	**0.0**	**0**	**0.0**	**320,000**	**3.3**	**951,341**	**5.6**	**1,188,124**	**5.6**	**1,188,124**	**14.5**	**3,647,588**
Total Project Costs	**0.4**	**484,907**	**3.5**	**2,377,240**	**10.7**	**5,242,091**	**9.6**	**4,511,061**	**5.6**	**1,188,124**	**29.8**	**13,803,423**
Continuing Existing Costs												
Information Technology Staff	23.0	2,342,815	23.0	2,342,815	21.6	2,192,521	23.7	2,337,717	14.0	1,378,464	105.3	10,594,333
Other IT Costs		390,971		390,971		348,728		136,727		128,106		1,395,503
Total Continuing Existing IT Costs	**23.0**	**2,733,786**	**23.0**	**2,733,786**	**21.6**	**2,541,249**	**23.7**	**2,474,444**	**14.0**	**1,506,570**	**105.3**	**11,989,836**
Program Staff	392.1	47,704,119	392.1	47,704,119	391.2	47,605,260	386.8	47,106,965	385.9	47,062,984	1948.1	237,183,446
Other Program Costs		9,039,959		9,039,959		9,031,297		8,987,200		8,978,579		45,076,994
Total Continuing Existing Program Costs	**392.1**	**56,744,078**	**392.1**	**56,744,078**	**391.2**	**56,636,556**	**386.8**	**56,094,165**	**385.9**	**56,041,563**	**1948.1**	**282,260,440**
Total Continuing Existing Costs	**415.1**	**59,477,864**	**415.1**	**59,477,864**	**412.8**	**59,177,805**	**410.5**	**58,568,609**	**399.9**	**57,548,133**	**2053.4**	**294,250,276**
TOTAL ALTERNATIVE COSTS	**415.5**	**59,962,771**	**418.6**	**61,855,104**	**423.5**	**64,419,896**	**420.1**	**63,079,671**	**405.5**	**58,736,257**	**2083.2**	**308,053,700**
INCREASED REVENUES		0		0		0		0		0		**0**

ECONOMIC ANALYSIS SUMMARY

Date Prepared: 1/15/08

All costs to be shown in whole (unrounded) dollars.

Department: California Department of Public Health

Project: Enterprise-wide On-line Licensing

	FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12		FY 2012/13		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
EXISTING SYSTEM												
Total IT Costs	23.0	2,766,922	23.0	2,766,922	23.0	2,766,922	23.0	2,766,922	23.0	2,766,922	115.0	13,834,612
Total Program Costs	392.1	56,744,078	392.1	56,744,078	392.1	56,744,078	392.1	56,744,078	392.1	56,744,078	1960.5	283,720,388
Total Existing System Costs	415.1	59,511,000	415.1	59,511,000	415.1	59,511,000	415.1	59,511,000	415.1	59,511,000	2075.5	297,555,000
PROPOSED ALTERNATIVE	**Off-the-Shelf Software Product**											
Total Project Costs	0.4	480,307	4.5	2,765,103	8.1	2,774,133	5.8	1,188,820	5.5	953,055	24.3	8,161,418
Total Cont. Exist. Costs	415.1	59,511,000	415.1	59,511,000	407.1	58,463,175	400.0	57,608,362	399.9	57,598,692	2037.2	292,692,230
Total Alternative Costs	415.5	59,991,307	419.6	62,276,103	415.2	61,237,308	405.8	58,797,182	405.4	58,551,748	2061.5	300,853,648
COST SAVINGS/AVOIDANCES	(0.4)	(480,307)	(4.5)	(2,765,103)	(0.1)	(1,726,308)	9.3	713,818	9.7	959,252	14.0	(3,298,648)
Increased Revenues		0		0		0		0		0		0
Net (Cost) or Benefit	(0.4)	(480,307)	(4.5)	(2,765,103)	(0.1)	(1,726,308)	9.3	713,818	9.7	959,252	14.0	(3,298,648)
Cum. Net (Cost) or Benefit	(0.4)	(480,307)	(4.9)	(3,245,410)	(4.9)	(4,971,718)	4.4	(4,257,900)	14.1	(3,298,648)		
ALTERNATIVE #1	**Custom Solution**											
Total Project Costs	0.4	484,907	3.5	2,377,240	10.7	5,242,091	9.6	4,511,061	5.6	1,188,124	29.8	13,803,423
Total Cont. Exist. Costs	415.1	59,477,864	415.1	59,477,864	412.8	59,177,805	410.5	58,568,609	399.9	57,548,133	2053.4	294,250,276
Total Alternative Costs	415.5	59,962,771	418.6	61,855,104	423.5	64,419,896	420.1	63,079,671	405.5	58,736,257	2083.2	308,053,700
COST SAVINGS/AVOIDANCES	(0.4)	(451,771)	(3.5)	(2,344,104)	(8.4)	(4,908,896)	(5.0)	(3,568,671)	9.6	774,743	(7.7)	(10,498,700)
Increased Revenues		0		0		0		0		0		0
Net (Cost) or Benefit	(0.4)	(451,771)	(3.5)	(2,344,104)	(8.4)	(4,908,896)	(5.0)	(3,568,671)	9.6	774,743	(7.7)	(10,498,700)
Cum. Net (Cost) or Benefit	(0.4)	(451,771)	(3.9)	(2,795,876)	(12.3)	(7,704,772)	(17.3)	(11,273,442)	(7.7)	(10,498,700)		
ALTERNATIVE #2												
Total Project Costs												
Total Cont. Exist. Costs												
Total Alternative Costs												
COST SAVINGS/AVOIDANCES												
Increased Revenues												
Net (Cost) or Benefit												
Cum. Net (Cost) or Benefit												

PROJECT FUNDING PLAN

Department: California Department of Public Health

All Costs to be in whole (unrounded) dollars

Date Prepared: 1/15/08

Project: Enterprise-wide On-line Licensing

	FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12		FY 2012/13		TOTALS	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
TOTAL PROJECT COSTS	**0.4**	**479,307**	**4.5**	**2,765,103**	**8.1**	**2,774,133**	**5.8**	**1,188,820**	**5.5**	**953,055**	**24.3**	**8,160,418**
RESOURCES TO BE REDIRECTED												
Staff	0.4	41,707	2.5	257,227	7.0	696,318	5.8	952,342	5.5	953,055	**21.1**	**2,900,649**
Funds:												
Existing System		0		0		283,980		236,478		0		**520,457**
Other Fund Sources	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	**0.0**	**0**
TOTAL REDIRECTED RESOURCES	**0.4**	**41,707**	**2.5**	**257,227**	**7.0**	**980,297**	**5.8**	**1,188,820**	**5.5**	**953,055**	**21.1**	**3,421,106**
ADDITIONAL PROJECT FUNDING NEEDED												
One-Time Project Costs	0.0	437,600	2.0	2,507,876	1.1	1,793,836	0.0	0	0.0	0	**3.1**	**4,739,312**
Continuing Project Costs	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	**0.0**	**0**
TOTAL ADDITIONAL PROJECT FUNDS NEEDED BY FISCAL YEAR	**0.0**	**437,600**	**2.0**	**2,507,876**	**1.1**	**1,793,836**	**0.0**	**0**	**0.0**	**0**	**3.1**	**4,739,312**
TOTAL PROJECT FUNDING	**0.4**	**479,307**	**4.5**	**2,765,103**	**8.1**	**2,774,133**	**5.8**	**1,188,820**	**5.5**	**953,055**	**24.3**	**8,160,418**
Difference: Funding - Costs	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	**0**	**0**

Total Estimated Cost Savings	**0.0**	**0**	**0.0**	**0**	**5.1**	**493,859**	**9.6**	**899,218**	**9.7**	**904,000**	**24.4**	**2,297,077**

ADJUSTMENTS, SAVINGS AND REVENUES WORKSHEET
(DOF Use Only)

Department: California Department of Publi

Date Prepared: 1/15/08

Project: Enterprise-wide On-line Licensing

Annual Project Adjustments	FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12		FY 2012/13		Net Adjustments	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
One-time Costs												
Previous Year's Baseline	0.0	0	0.0	437,600	2.0	2,507,876	1.1	1,793,836	0.0	0		
(A) Annual Augmentation /(Reduction)	**0.0**	**437,600**	**2.0**	**2,070,276**	**(0.9)**	**(714,040)**	**(1.1)**	**(1,793,836)**	**0.0**	**0**		
(B) Total One-Time Budget Actions	0.0	437,600	2.0	2,507,876	1.1	1,793,836	0.0	0	0.0	0	**3.1**	**4,739,311**
Continuing Costs												
Previous Year's Baseline	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0		
(C) Annual Augmentation /(Reduction)	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**		
(D) Total Continuing Budget Actions	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	**0.0**	**0**
Total Annual Project Budget Augmentation /(Reduction) [A + C]	**0.0**	**437,600**	**2.0**	**2,070,276**	**(0.9)**	**(714,040)**	**(1.1)**	**(1,793,836)**	**0.0**	**0**		

[A, C] Excludes Redirected Resources

3.1	**4,739,312**

Annual Savings/Revenue Adjustments

Cost Savings	0.0	0	0.0	0	5.1	493,859	4.5	405,358	0.1	4,782		
Increased Program Revenues		0		0		0		0		0		

Appendix A: Acronyms

Acronym	Term
ACH	Automated Clearing House
ACO	Aspen Central Office
ACTS	Aspen Complaint Tracking System
AIMS	Agency Information Management Strategy
ASE	Aspen Survey Explorer
ASPEN	Automated Survey Processing Environment
CAMIS	California Mammography Information System
CCR	California Code of Regulations
CDHCS	California Department of Health Care Services (newly formed)
CDHS	California Department of Health Services (now split into two departments)
CDPH	California Department of Public Health (newly formed)
CEU	Continuing Education Unit(s)
CHT	Certified Hemodialysis Technician
CIO	Chief Information Officer
CMAS	California Multiple Award Schedules
CM&AS	Client Management & Administration System
CMS	Centers for Medicare and Medicaid Services (formerly HCFA, Healthcare Finance Administration)
COTS	Commercial Off The Shelf
CTU	Client Technology Unit
DB	Database
DBMS	Database Management System
DCA	Department of Consumer Affairs
DDWEM	Division of Drinking Water & Environmental Management
DED	Deliverable Expectations Document
DFDRS	Division of Food, Drug, and Radiation Safety
DGS	Department of General Services
DHCP	Dynamic Host Configuration Protocol
DHCS	Department of Health Care Services (newly formed)
DNS	Domain Name System
DOF	Department of Finance
DOJ	Department of Justice

Acronym	Term
DSSU	Data Systems Support Unit
DTS	Department of Technology Services
DWOCP or OCP	Drinking Water Operator Certification Program
EFT	Electronic Funds Transfer
ELAP	Environmental Laboratory Accreditation Program
EOL	Enterprise-wide On-Line Licensing
EPA	(United States) Environmental Protection Agency
FDA	(United States) Food and Drug Administration
FDB	Food & Drug Branch
FOA	Fields of Accreditation
FOT	Fields of Testing
FSR	Feasibility Study Report
FTP	File Transfer Protocol
GIS	Geographic Information Systems
GLD	Generally Licensed Devices
HAL	Health Application Licensing
HIV	Human Immunodeficiency Virus
HMDR	Home Medical Device Retailer
HSC	Health and Safety Code
HTTPS	Hypertext Transfer Protocol over an encrypted Secure Sockets Layer (SSL)
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPOC	Independent Project Oversight Consultant
IT	Information Technology
ITPP	Information Technology Procurement Plan
ITSD	Information Technology Services Division
IV&V	Independent Verification and Validation
IVR	Integrated Voice Response
LAN	Local Area Network
LLRW	Low-Level Radioactive Waste
LLRWTS	Low-Level Radioactive Waste Tracking System
MQSA	Mammography Quality Standards Act
MOTS	Modified Off The Shelf
MQAA	(California) Mammography Quality Assurance Act

Acronym	Term
MRU	Monitoring Review Unit
MS	Microsoft
MWMA	Medical Waste Management Act
MWMP	Medical Waste Management Program
NELAP	National Environmental Laboratory Accreditation Program
NOS	Network Operating System
NOV	Notice of Violation
NSF	Non-Sufficient Funds
OCP or DWOCP	Drinking Water Operator Certification Program
PC	Personal Computer
PE/PT	Performance Evaluation and Proficiency Testing
PICME	Permits, Inspections, Compliance Monitoring & Enforcement
PDMA	Prescription Drug Marketing Act
PIER	Post-Implementation Evaluation Report
PMBOK	PMI's Project Management Body of Knowledge
PMI	Project Management Institute
PMO	Project Management Office – or – Project Management Officer
PMP	Project Management Plan
PPMB	Planning and Project Management Branch
PT	Proficiency Testing
PY	Personnel Year(s)
RAM	Radioactive Materials
RFP	Request for Proposal
RHB	Radiologic Health Branch
RPS	Rapid Processing System
SAM	State Administrative Manual
SDLC	System Development Life Cycle
SDWA	Safe Drinking Water Act
SDWIS	Safe Drinking Water Information System
SDWS	Safe Drinking Water Systems Program
SIMM	State Information Management Manual
SPR	Special Project Report
SQL	Structured Query Language
SSL	Secure Sockets Layer

Acronym	Term
TAS	Time Accounting System
USEPA	United States Environmental Protection Agency
VPN	Virtual Private Network
WAN	Wide Area Network
WINS	Windows Internet Naming Service
WQI	Water Quality Inquiry
WQM	Water Quality Monitoring

Appendix B:

CDPH Information Security Standards SR-1

INFORMATION SECURITY OFFICE

Information Systems Security Requirements for Projects (ISO/SR1)

Version 3.5

October 2007

Revision History

Doc No. / Rev No.	Revision Date	Revised By	Description of Revision / Change
S19 / R1.5	1/10/2007	A. Lancashire CDHS	Reformatting changes
SR1 / R1.0	9/12/2007	M. Serapio DHCS, B. Kelsey CDPH	Updated to address new best practices (previous version had dependencies to best practices from pre-SOA), fill existing regulatory gaps, remove vendor dependencies, reword language to make applicable to COTS/MOTS applications, and re-designated document number and name.
SR1/v1.5	9/14/2007	I. Sanford DHCS	Various grammatical and definition changes. Clarification of terms and responsibilities.
SR1/v2.0	9/21/2007	I. Sanford DHCS	Post team review updates
SR1/v2.1	10/17/2007	J. Cleveland CDPH	2nd team review comments/changes
SR1/V2.2	10/21/2007	J. Cleveland CDPH	Added Admin User ID and password section from Ian Sanford and Data Query section from Brett Kelsey.
SR1/V2.3	10/22/2007	J. Cleveland CDPH	Modifications to Admin User ID and password section and Data Query section.
SR1/V3.0	10/25/2007	J. Cleveland CDPH	Minor grammatical changes, removal of dynamic web links, and added COTS language in C.8.
SR1/V3.5	10/26/2007	J. Cleveland CDPH	Addition of Sections A.13, A.14, B.12, B.13, B.14, B.15, and B.16 for the purpose of covering Privacy, when used in conjunction with BAAs.

Type: **ISO Requirements**	
Issued: **October 26, 2007**	*Doc Number:* **SR 1/v3.5**
Revised:	
Title: **Information Systems Security Requirements for Projects**	

I. Purpose

This document provides the minimum security requirements, mandated by the Information Security Office (ISO) from projects governed and/or subject to the policies and standards of the California Department of Public Health (CDPH). Projects that intend to deploy systems/applications into the Department's system infrastructure or will consume Department information system services are also subject to these minimum security requirements.

This document is intended to assist the Department and its service consumers in understanding the criteria the Department will use when evaluating and certifying the system design and security features and protocols used by project solutions consuming Department services. The security requirements herewith will also be used in conjunction with the Department ISO's compliance review program of its information system services consumers.

This document will serve as a universal set of requirements which must be met regardless of physical hosting location or entities providing operations and maintenance responsibility. These requirements do not serve any specific project nor do they prescribe any specific implementation technology.

II. Scope of Requirements

The information security requirements herein are organized in five categories (sections) and address at a minimum:

- Administrative/Management Safeguards
- Technical and Operational Safeguards
- Solution Architecture
- Documentation of Solution
- ISO Notifications

III. Contact

Chief Information Security Officer
California Department of Public Health
Information Security Office
1615 Capital Avenue
Sacramento, Ca 95814

IV. Information Systems Security Requirements

A. Administrative / Management Safeguards

1. Workforce Confidentiality Statement

All persons working with Department information must sign a confidentiality statement. The statement must include at a minimum; General Use, Security and Privacy safeguards, Unacceptable Use, Audit, and Enforcement policies. (Contact the ISO for the current version of the Security & Confidentiality form in use.)

The statement must be signed by the project member prior to being granted access to the Department's information. The statement must be renewed annually.

2. Access Authorization

Project/Program must implement and document clear rules and processes for vetting and granting authorizations; and procedures for the supervision of workforce members who work with Department information or in locations where it might be accessed.

3. Access Authorization Maintenance

On at least a semi-annual basis, Project/Program will review and remove all authorizations for individuals who have left the department, transferred to another unit, or assumed new job duties within the department.

4. Information System Activity Review

Project/Program must implement and document procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

5. Periodic System Security Review

All systems shall allow for periodic system security reviews that provide assurance that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection.

The reviews may include technical tools and security procedures such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest hardware/software “patches”), and penetration testing.

6. Periodic System Log Review

All systems processing and/or storing Department information shall have a method or procedure in place to create and review system logs for unauthorized access. Logs may be stored within the system or on a centralized logging server or service, and shall be maintained for a minimum of three years.

7. Business Impact Analysis

Project/Program will conduct annually a Business Impact Analysis of the application to determine the Maximum Acceptable Outage (MAO), cost of lost functionality, system component dependencies, business function dependencies, and business partner dependencies.

8. Change Control

All systems processing and/or storing Department information must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity, and availability of information.

For those systems running within the Department’s environment and/or are consuming Department services, those systems shall comply with DTS and Department standards for change control process and procedures.

9. Incident Response

Establish procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

The emergency response procedures shall be added to the existing Operational Recovery Plan (ORP). The ORP shall address what to do if a computer system and/or the information files are violated, lost, damaged, or inaccessible.

10. Disaster Recovery

Establish procedures that allow facility access in support of restoration of lost information under the ORP and emergency mode operations plan in the event of an emergency.

The restoration/recovery support procedures shall be added to the existing Operational Recovery Plan (ORP) to restore any loss of information and assure continuity of computing operations for support of the application and information.

Recovery procedures shall be developed using Appendix "J" Template from the Department's ORP.

11. Emergency Mode Operation Plan

Establish an Emergency Mode Operation Plan to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. This plan shall be added to the existing ORP.

12. Periodic System Recovery Testing

All systems, as part of a new or existing project, shall allow for periodic system recovery testing. The period between tests should be defined as part of the project and be consistent with relevant department disaster recovery standards. Such testing should provide assurances that plans (Incident Response, Disaster Recovery, Emergency Mode Operation, and Data Backup) and controls (management, operations, personnel, and technical) are functioning effectively and providing adequate levels of protection during an incident, disaster, or breach.

13. Supervision of Data

Public Health Information (PHI) in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk, or office. Unattended means that information is not being observed by an employee authorized to access the information. Department PHI in paper form shall not be left unattended at any time in vehicles or planes and shall not be contained in checked-in baggage on commercial airplanes.

14. Escorting Visitors

Visitors to areas where Department PHI is contained shall be escorted and Department PHI shall be kept out of sight while visitors are in the area.

B. Technical and Operational Safeguards

1. System Security Compliance

All project systems shall comply with applicable department security policies and requirements, as specified in the State Administrative Manual, Health Administrative Manual, HIPAA, Privacy Act, and any other applicable state or federal regulation. All security safeguards and precautions shall be subject to the approval of the Department ISO.

2. Virus Protection

All systems shall install and actively use comprehensive third-party anti-virus and virus protection software, and routinely update such software when updates are released. All security safeguards and precautions shall be subject to the approval of the Department ISO.

3. Patch Management

All systems shall install and actively use comprehensive third-party patch management program and routinely update system and application software when updates are released. All security safeguards and precautions shall be subject to the approval of the Department ISO.

4. Encrypted Electronic Transmissions

All information transmissions that contain confidential information must be encrypted end-to-end using an industry-recognized encryption standard. The electronic transport must utilize Secure Socket Layer (SSL) and Department information and confidential information shall be encrypted at the minimum of 128 bit AES or 3DES (Triple DES) if AES is unavailable. Equivalent or stronger algorithms may be used upon approval of the Department ISO.

5. Encrypted Data Storage

All confidential information must be encrypted when stored using a department approved encryption standard. Confidential information shall be encrypted at the minimum of 128 bit AES or 3DES (Triple DES) if AES is unavailable. Equivalent or stronger algorithms may be used upon approval of the Department ISO.

6. Workstation / Laptop Encryption

All workstations and laptops that process and/or store Department information must be encrypted with a Department approved solution or a solution using a vendor product specified on the California Strategic Sourced Initiative (CSSI) located at the following link:
www.pd.dgs.ca.gov/masters/EncryptionSoftware.html

7. Removable Media Encryption

All electronic files that contain Department information must be encrypted when stored on any removable media type device (i.e. USB thumb drives, floppies, CD/DVD, tape backup, etc.) with a Department approved solution or a solution using a vendor product specified on the California Strategic Sourced Initiative (CSSI) located at the following link:
www.pd.dgs.ca.gov/masters/EncryptionSoftware.html

8. Secure Connectivity

All transmission and data-links between the information and application/system and DBMS and the DTS WAN shall be secure between transmission systems as required by regulation, policy or standard and as prescribed for the given application/system.

9. Intrusion Detection and Prevention

All systems that are accessible via the Internet, are critical, or contain ePHI shall install and actively use a Department approved comprehensive third-party real-time host based intrusion detection and prevention program that reports security events directly to the Department ISO. All security safeguards and precautions shall be subject to the approval of Department ISO.

10. Minimum Data Downloads

In accordance with the principle of need-to-know, only the minimum amount of information required to perform necessary business functions should be copied or downloaded.

11. Data Destruction

All Department information must be wiped from systems when the information is no longer necessary. The wipe method must conform to Department of Defense and Department standards for information destruction. Once information has been destroyed, the Department contract manager must be notified. If an agency or other entity is unable to destroy media in accordance with Department standards and provide notification, the media must be returned to the Department after usage for destruction in an approved manner.

12. Confidential Destruction

Department PHI in paper form must be disposed of through confidential means, such as cross cut shredding and pulverizing.

13. Removal of Data

Department PHI in either electronic or paper form shall not be removed from Department premises or from the premises of an authorized vendor or contractor without the written permission of the Department ISO.

14. Faxing of Confidential Information

Facsimile transmissions containing PHI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers must be verified before sending.

15. Mailing of Confidential Information

Department PHI shall only be mailed using secure methods. Large volume mailings of Department PHI must be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted with a Department approved solution or a solution using a vendor product specified on the CSSI.

C. Solution Architecture

1. System Security Compliance

The system shall comply with all applicable Department security policies and requirements, as well as those specified in the State Administrative Manual, Health Administrative Manual, HIPAA, Privacy Act, and any other applicable state or federal regulation. All security safeguards and precautions shall be subject to the approval of the Department ISO.

2. Access Point Warning Banner

All systems containing Department information shall display a warning banner stating that information is confidential, activity is logged, and system use is for business purposes only. User shall be directed to log off the system if they do not agree with these requirements.

The following warning banner shall be used for all access points (e.g., desktops, laptops, web applications, mainframe applications, servers and network devices):

> ***WARNING: This is a State of California computer system that is for official use by authorized users and is subject to being monitored and/or restricted at any time. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.***
>
> ***LOG OFF IMMEDIATELY, if you do not agree to the conditions stated in this warning.***

3. Layered Application Design

Application must be able to be segmented into a layered application design separating at a minimum the Presentation, Application/Business Logic, and Data Access Logic, and Data Persistence/Database layers.

4. Separation of Layers

The Presentation, Application/Business Logic, and Data Access Logic layer must be separated physically by a firewall regardless of physical implementation.

Vendor-provided commercial off-the-shelf (COTS) packages or components where physical separation of layers is not possible requires ISO approval.

5. Business Logic Layer Communication

Any system request made to the Business logic layer must be authenticated.

6. Data Access Logic Layer Design

The Data Access Logic Layer may take the form of stored procedures, database API, Data Access Objects/Components, Data Access Middleware, Shared Data Services, or Secure Web Service.

7. Data Access Logic Layer Communication

Any system request made to the Data Access logic layer must be authenticated and authorized.

8. Data Persistence/Database Layer Isolation

No direct access to the Data Persistence/Database layer will be permitted, except through the Data Access logic layer.

All calls to the Data Persistence/Database layer will be made through the Data Access logic layer as a trusted sub-system that utilizes a single database access account to all transactions.

Vendor-provided commercial off-the-shelf (COTS) packages or components where physical separation of Data Access Logic layer from Data Persistence/Database layer is not possible require ISO approval.

9. User Input Validation

All user input must be validated. The system must manage client input controls from server side to the extent possible. All third-party client side input controls must be documented and approved by the Department ISO.

10. Data Input Validation

All user information input must be validated before being committed to the database or other application information repository.

11. Data Queries

All Data queries (including In-line SQL calls) will not be allowed from the Presentation or the Business Logic layers unless validated for appropriate use of query language and validated for appropriate quantity/quality of data input. All data queries solution must be approved by department CISO.

Database table names and column names must not be exposed. Applications must use an alias for every table and column.

Dynamic SQL will not be permitted from the Presentation Layer without prior approval from the department ISO.

12. Username/Password Based Authentication

When usernames and passwords are going to be used as the method for system authentication the following for each must be met:

- Username requirements:
  - Usernames are unique and are traceable to an individual worker.
  - Usernames are NOT to be shared and never hard-coded into system logic.
- Password requirements:
  - Are not to be shared.
  - Must be 8 characters or more in length.
  - Must NOT be a word found in the dictionary, regardless of language.
  - Password must NOT be stored in clear text.
  - Must be changed at least every 60 days.
  - Must be changed immediately if revealed or compromised.
  - Passwords must be encrypted using irreversible industry-accepted strong encryption.
  - Accounts must be locked after 3 failed logon attempts.
  - Account lock-out reset timers must be set for a minimum of 15 minutes.
  - Must be composed of characters from at least three of the following four groups from the standard keyboard:
    - Upper case letters (A-Z);
    - Lower case letters (a-z);
    - Arabic numerals (0 through 9); and
    - Non-alphanumeric characters (punctuation symbols).

13. Administrator Username/Password Based Authentication

- Username requirements:
  - Must be unique and are traceable to an individual person.
  - Must NOT be shared.
  - Must never be hard-coded into system logic.
  - Must NOT be the same across different zones (e.g. Web Zone, Internal network, and Test Labs / Environments).
  - The default built-in Administrator account must be renamed and disabled.
  - The naming convention for administrator usernames must not make it obvious that usernames belong to administrator accounts.
  - If a generic Administrator account is created:
    - It must only be used in an Emergency.
    - It is NOT to be used for routine maintenance.
    - The password storage and management process for generic administrator accounts must be approved by the Department ISO.
- Password requirements:
  - Must not be the same as any of the previous 10 passwords.
  - Must not to be shared.

- Must NOT be the same across different zones (e.g. Web Zone, Internal network, and Test Labs / Environments).
- Must be 12 characters or more in length.
- Must NOT be a word found in the dictionary, regardless of language.
- Password must NOT be stored in clear text.
- Must be changed at least every 60 days.
- Must be changed immediately if revealed, or compromised.
- Must be changed immediately upon the termination or transfer of an employee with knowledge of the password.
- Passwords must be encrypted using industry accepted, irreversible strong encryption.
- Accounts must be locked after 3 failed logon attempts.
- Account lock-out timers must be set for at least 60 minutes.
- Must be comprised of characters from at least three of the following four groups from the standard keyboard:
  - Upper case letters (A-Z);
  - Lower case letters (a-z);
  - Arabic numerals (0 through 9);
  - Non-alphanumeric characters (punctuation symbols).

14. Role - Based Access

Any system deployed during, or as a result of a project, shall provide secure role-based access for authorization utilizing the principle of least privilege at all layers/tiers.

15. User / Entity Authentication Logging

System must log success and failures of user authentication at all layers as well as log all user transactions at the database layer as required by regulation, policy or standard and as prescribed for the given application/system. This logging shall be included for all user privilege levels including but not limited to systems administrators. This requirement applies to systems that process, store, and/or interface with PII and/or confidential information.

16. Automatic System Session Expiration

The system must provide an automatic timeout of user sessions after 20 minutes of inactivity.

17. Automatic System Lock-out and Reporting

The system must provide an automatic lock-out of users and a means to audit a minimum of 3 failed log-in attempts. The means of providing audit information must be approved by the departmental ISO.

18. Role-based Access to Audit Functions and Data

All systems/applications will implement role-based access to auditing functions and audit trail information utilizing the principle of least privilege

19. Secure Online Access to Audit Functions

All systems / applications will implement a secure online interface to Audit Capabilities and Reporting by way of application programming interface (API) or network service (or Web Service); to allow Department ISO to view logs, auditing procedures, and audit reporting.

20. Audit Trails

This requirement delineates the (minimum) log information that audit trails should record for any system that contains or is involved in the transmission of confidential information. The information listed below should be available on every system running a production environment. Not only will this information assist with problem resolution efforts and system restore operations, it will also be invaluable to system penetration attack investigations, fraud investigations, and the like.

The system must record (at minimum) the following events and any other events deemed appropriate by the Department ISO:

Transaction Types

- Any and all administrative changes to the system (ie: administrative password changes (forgotten password resets), system variables, network configuration changes, disk subsystem modifications, etc).
- Logon failures.
- Logons during non-business hours.
- Program or file access denial.
- Addition, deletion, or modification of users or program access privileges.
- Changes in file access restrictions.
- Database addition, deletion, or modification.
- Copy of files before and after read and write changes.
- Transaction issued.

Individual audit trail records shall contain the information needed to associate each query transaction to its initiator and relevant business purpose. Individual audit trail records should capture at a minimum the following:

Minimum Audit Trail Record Content

- Date and Time Stamp.

- Unique Username of Transaction Initiator.
- Transaction Recorded.
- Success or Failure of Transaction Recorded.
- Relevant business process or application component involved.
- Data captured (if any).

Audit Trail logs shall be maintained at minimum for three years after the occurrence or a set period of time determined by the Program's ISO that would not hinder a detailed forensic investigation of the occurrence. The Department ISO has final approval authority.

D. Documentation of Solution

1. System Configuration

As part of each project, assigned staff will document and maintain a full inventory of the major hardware, software, and communications platforms in use; system configurations; all applications/components with descriptions encompassing the solution; and a description of the solution's security design features and user access control mechanisms. Project will ensure a custodian(s) is assigned to each application/component.

2. Data In Use Classifications

Project will document and maintain information classification matrix of all information elements accessed and/or processed by solution.

The matrix should identify at a minimum:

- information element.
- information classification/sensitivity.
- relevant function/process or where is it used.
- system and database or where is it stored.

3. System Roles and Relationships

Project will document the organizational structure and relationships between systems managers, systems security personnel, and users, including an estimate of the number of users that will have access to Department information within the system solution and an explanation of their job descriptions.

4. Audit Method Documentation

Project will document the solution's auditing features and provide samples of audit reporting.

5. Retention of Documentation

The system/application maintainers will retain documentation, including audit and activity logs, for a minimum of three years (up to seven years) from the date of its creation or the date it was last in effect, whichever is later.

E. ISO Notifications

1. Security Compliance Notification

As part of each project, assigned staff will document how proposed solution meets or addresses the requirements specified in this document and must be submitted to the Department ISO prior to taking custody of Department owned information.

2. Notification of Changes to Solution

Once a project is approved as final by the ISO, no changes will be made to the project scope, documentation, systems or components without a change approval by the ISO.

3. Notification of Breach or Compromise

The system/application maintainers shall immediately and in writing report to the ISO on any and all breaches or compromises of system and/or information security, and shall take such remedial steps as may be necessary to restore security and repair damage, if any.

In the event of a breach or compromise of system and/or information security, the ISO may require a system/application security audit. The ISO shall review the recommendations from the security audit, and make final decisions on the steps necessary to restore security and repair damage.

The system/application maintainers shall properly implement any and all recommendations of the security audit, as approved by the ISO.

Appendix C:

Hardware and Software Standards

California Department of Health Services

Information Technology Hardware and Software Standards

Volume 1

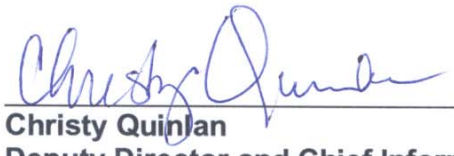
Revised May 31, 2007

Information Technology Standards

I am pleased to present the latest Information Technology Standards to the California Department of Health Services (CDHS). These Information Technology (IT) standards are intended to provide consistency across the CDHS, to facilitate the cost effective implementation of IT systems, ensure high-quality service levels, and to maximize the Department's return on IT investments.

The standards presented in this document provide direction to divisions, offices and all other operating units in the acquisition of new IT systems and in the migration of existing systems and components to a standardized environment. The standards address the hardware, software and IT operating practices to be used by the Department and attempt to ensure compatibility, connectivity and interoperability. The standards apply to the Department's entire IT environment and are applicable in all operating units of the Department.

I believe that you will find this document a strategic asset in helping CDHS realize the many benefits to be derived from a unified technology environment.



5/31/07

Christy Quinlan
Deputy Director and Chief Information Officer
Information Technology Services Division

Date

Department of Health Services
Information Technology Standards

TABLE OF CONTENTS

1 Introduction

1.1 Objectives and Benefits

This document defines effective and usable standards in support of the CDHS' business processes and environment. The objectives and benefits of the CDHS IT standards include:

- Improve service level to internal and external customers.

  The CDHS IT standards are based on mature technology proven to interoperate effectively. The standards contribute to higher levels of customer service and facilitate the establishment of Service Level Agreements (SLA).

- Improve cost effectiveness and reduce life cycle costs.

  The CDHS IT standards leverage our existing infrastructure and expertise while providing cost effective migration paths to newer technologies. Common hardware and software configurations reduce the complexity of the environment resulting in fewer failure opportunities. Staffing, training and development costs are reduced because there are fewer technologies to support. Common configurations also facilitate the consolidation of spare inventories, allow for centralized testing and validation and create a broader base of knowledgeable support staff. The opportunity to establish department-wide software licensing agreements also results in overall cost reductions.

- Increase system availability, maturity and stability.

  Standardized information technology environments lower the risk of technology investment failures and are integral to the delivery of effective solutions. Fewer products from fewer vendors reduce the complexity that frequently leads to interoperability and compatibility related service disruptions.

- Ensure intradepartmental interoperability and efficiency.

  The CDHS IT standards support information interchange, shared services (e.g., e-mail, print services, and database services) and backup and recovery services. The standards also support workflow applications involving all CDHS operating units. A common set of technologies for the creation, transfer and storage of information will enhance the overall efficiency and effectiveness of the Department.

- Improve portability, flexibility and scalability.

  The CDHS IT standards define an information technology environment that supports existing applications and positions the CDHS for continued implementation of new IT solutions. Through these standards, applications developed in one business unit are more easily migrated to other units, and applications designed for small workgroups can be implemented for larger groups with little difficulty.

- Improve security.

  The Department's IT Security Policy and Plan specifies requirements for security. The standards for physical, Internet, Intranet, and personal computer security enable consistent and manageable security over the Department's IT assets. The application of these standards enables CDHS to continue providing a secure IT environment.

- Improve network manageability.

  Standards-based infrastructure design and implementation are essential for a network that is predictable, provides high availability and is managed effectively. The CDHS IT standards define this infrastructure as well as the tools for effective management.

1.2 Implementation Requirements and Exceptions

The CDHS IT standards are requirements for all CDHS operating units. Within the CDHS, the Chief Information Officer (CIO) is responsible for establishing information technology policy and enforcing the standards.

No exceptions to compliance with these standards are allowed unless appropriate approval is obtained in advance by the CDHS' CIO.

Exceptions to these standards must be approved by the CIO prior to procurement, and are granted on a case-by-case basis. Exceptions can be requested by using the Request for Exception Form and process posted at http://dhsintranet/sites/i2e.

1.3 Changes to the Standards

The CDHS IT standards will be reviewed and updated semi-annually to address changes in technology and business requirements. More frequent updates may occur as necessary. Ongoing review of this document will ensure accuracy and compatibility with business objectives.

The following items may drive changes to the standards:

- Changes in technology
- Security requirements
- New business needs
- Exception request trends
- Specific request

It is the responsibility of each division to suggest changes to the CDHS IT standards which address identified or anticipated business needs. Changes can be submitted by business units, LAN Administrators, and ITSD staff. Such feedback should be directed to the I2E Committee. The I2E Committee is a team of ITSD and business unit staff who evaluate IT standard changes, for recommendation to the CIO. After approval by I2E and the CIO, changes will be incorporated into the next document release, and published on the CDHS Intranet. A high level summary of the changes will be added to the revision history log at the end of this document.

1.4 Definitions

The following words and phrases are used throughout this document and are defined here for ease of review.

Term:	Definition:
Desktop:	A personal computer commonly found on a user's desk, also referred to as a microcomputer.
Desktop Printer:	A printing resource (printer) attached directly to the user's desktop computer with a local connection.
Laptop:	A portable computer running the traditional Windows Operating system (i.e. Win 2K, or Win XP)
Minimum:	In those instances where the standard is indicated as a minimum, the standard may be exceeded without an exception requirement.
Multi-Workgroup:	Applications or devices used by more than one workgroup of CDHS employees.
Personal Computer (PC):	A desktop or laptop computer.
Standard	Is an acceptable choice for procurement and installation within CDHS, provided a business case exists and is not in conflict with other CDHS policies, procedures or guidelines. Listing as a standard does not imply support by ITSD or the program LAN Administrator, they should be consulted regarding the appropriateness of each use case.
Tier 1 Build:	A suite of applications and their configurations, approved for use on every CDHS personal computer.
Workgroup:	An application or device used by a Workgroup within a CDHS Division or Office. The Workgroup could be a business unit within a Branch or Office, or within a small business unit.
Workgroup Printer:	A printing resource available on the Local Area Network that is shared by two or more users.

2 Desktop, Laptop, Printer, and Mobile Computing Standards

2.1 Desktop and Laptop Hardware Standards

Below are the hardware standards for all newly acquired desktop and laptop computers.

Desktop Unit – HP		
Category	**Standard**	**Remarks**
Manufacturer & Model:	HP/Compaq DC7700 CMT	P/N: RK870US#ABA
Processor:	Intel® Pentium® D	
Processor Speed:	3.0 GHz	
Network Interface:	10/100/1000 Ethernet	
Storage (Disk):	80 GB Hard Drive and 1.44 FDD	
Memory:	1 GB RAM	
DVD Reader:	CD-RW/DVD-ROM Drive	

Desktop Unit – Gateway		
Category	**Standard**	**Remarks**
Manufacturer & Model:	Gateway E4500D	DGS P/N: 1008486 Item # 5 on CSSI contract
Processor:	Intel Pentium IV	
Processor Speed:	3.0 GHz	
Network Interface:	10/100/1000 Ethernet	
Storage (Disk):	80 GB Hard Drive and 1.44 FDD	
Memory:	1 GB RAM	
DVD Reader:	CD-RW/DVD-ROM Drive	

Laptop Unit – IBM (Tier 1)		
Category	**Standard**	**Remarks**
Manufacturer & Model:	IBM/Lenovo ThinkPad R60	P/N: 9459W1M
Processor:	Intel Core Duo Processor T2400	
Processor Speed:	1.83 GHz	
Network Interface:	10/100/1000 Ethernet	
Storage (Disk):	60 GB Hard Drive	
Memory:	1 GB RAM	
DVD Reader:	CD-RW/DVD Combination Drive	
Accessory Requirements	Floppy, ThinkPad Mini-Dock, Carrying Case	Mini-Dock P/N: "ThinkPad Essential Port Replicator" whose model name is "250510W"
Display Size:	15 in.	
Screen Type:	TFT	
Display Resolution:	1024 x 768 @ 16.7 Million Colors (24-bit) Internal Support 2048 x 1536 @ 16.7 Million Colors (24-bit) External Support	

Laptop Unit – Gateway (Tier 1)		
Category	**Standard**	**Remarks**
Manufacturer & Model:	Gateway M465E	P/N: 1008637-PWR
Processor:	Intel Core Duo Processor T2400	
Processor Speed:	1.83. GHz	
Network Interface:	10/100/1000 Ethernet	
Storage (Disk):	40 GB Hard Drive	
Memory:	1 GB RAM	
DVD Reader:	CD-RW/DVD Combination Drive	
Accessory Requirements	Floppy, Port Replicator, Carrying Case	
Display Size:	15.4 in.	
Screen Type:	TFT	
Display Resolution:	1280X800 Max, (t1 build sets it to 1024 x 768 @ 16.7 Million Colors (24-bit) Internal Support)	

Tablet PC Unit – Gateway (Tier 1)		
Category	**Standard**	**Remarks**
Manufacturer & Model:	Gateway M285-E	Recommended model for general tablet needs: 108804
Processor:	T2300	
Processor Speed:	1.660 GHz	
Network Interface:	10/100/1000 Ethernet	
Storage (Disk):	40 GB Hard Drive	
Memory:	512 MB	
DVD Reader:	CD-RW/DVD Combination Drive	
Display Size:	14.1 in.	
Screen Type:	TFT	

Tablet PC Unit – Lenova (Tier 1)		
Category	**Standard**	**Remarks**
Manufacturer & Model:	Lenovo X60	Recommended only where weight of the is a factor as this tablet cannot accommodate an internal DVD/CD drive
Processor:	T2400	
Processor Speed:	1.830 GHz	
Network Interface:	10/100/1000 Ethernet	
Storage (Disk):	40 GB Hard Drive	
Memory:	512 MB	
DVD Reader:	No DVD drive	Omitted due to weight.
Display Size:	12.1 in.	
Screen Type:	TFT	

2.2 Monitor Standards

Below are the hardware standards for all newly acquired monitors.

LCD Monitor		
Category	**Standard**	**Remarks**
Manufacturer:	Gateway	HP Monitors can only be purchased as part of a PC bundle
Model:	FPD 1775	DGS P/N: 1533998
Size:	17” color TFT	
Dot Pitch:	0.264mm dot pitch	
Resolution:	1280 X 1024	
Compliant Standards:	FCC Class B certified, CE, UL, TUV GS, VCCI, cUL, EPA Energy Star, NOM	
Response Time:	8 ms	

.

2.3 Printer Standards

2.3.1 Workgroup Printer Standards

Below are the standards for all departmental printers to be operated within the CDHS environment. These standards must be met for a printer to be supported in any activity including connection to the CDHS network.

Black and White Networked Printer, HP		
Category	**Standard**	**Remarks**
Manufacturer:	HP	High Volume Printing
Model:	LaserJet 4250n	DGS P/N: Q5401A
Resolution:	1200 DPI	
Network Interface:	Hi-speed USB 2.0 port, IEEE 1284-B compliant parallel port	
Print Languages:	PCL 6, PCL 5e, PostScript® 3™ emulation	
Memory:	64 MB RAM	
Printing:	Letter, Legal, Duplexing	

Black and White Networked (Workgroup) Printer, HP		
Category	**Standard**	**Remarks**
Manufacturer:	HP	Low Volume Printing
Model:	LaserJet P3005dn	DGS P/N: Q7815A#ABA
Resolution:	1200 DPI	
Network Interface:	Hi-speed USB 2.0 port, IEEE 1284-B compliant parallel port	
Print Languages:	PCL 6, PCL 5e, PostScript® 3™ emulation	
Memory:	80 / 320 MB RAM	
Printing:	Letter, Legal, Automatic Duplexing	

Color Networked Printer, HP		
Category	**Standard**	**Remarks**
Manufacturer:	HP	
Model:	LaserJet 3600dn	DGS P/N: Q5988A#ABA
Resolution:	600 DPI	
Connectivity:	1 USB, 1 parallel, 1 Ethernet	
Print Languages:	PCL 6, PCL 5e, PostScript® 3™ emulation	
Memory:	64 MB RAM	
Printing:	Letter, Legal, Duplexing	

Plotter Printer, HP		
Category	**Standard**	**Remarks**
Manufacturer:	HP	
Model:	DesignJet 1055cm Plus	DGS P/N: C6075B#ABA
Resolution:	Black: 1200 x 600 DPI ; Color: 600 x 600 DPI	
Connectivity:	Centronics parallel, IEEE 1284-compliant (including ECP), HP EIO internal print server for Fast Ethernet 10/100 Base-TX	
Print Languages:	HP=G/L/2, HP-GL, HP RTL, Adobe PostScript® 3™ emulation	
Memory:	64 MB RAM min 256 MB max	
Printing:	8.3 to 36 in wide sheets; 24” and 36 “ rolls	Max print length 300 ft; 900 Ft with optional multi-roll feeder

2.3.2 Desktop Printer Standards

Below are the standards for all desktop (personal) printers to be operated with the CDHS departmental infrastructure. These standards must be met for a printer to be supported in any activity.

Standalone Printer, HP		
Category	**Standard**	**Remarks**
Manufacturer:	HP	
Model:	LaserJet 1020	DGS P/N: Q5911A
Resolution:	1200 DPI	
Printing:	Letter, Legal	
Print Languages:	Host-based Printing	
Memory:	2 MB RAM	
Connectivity:	USB	

Standalone Mobile Printer, HP		
Category	**Standard**	**Remarks**
Manufacturer:	HP	
Model:	Inkjet Mobile Printer 460C	DGS P/N: C8150A
Resolution:	Black: 1200 DPI; Color: 4800 DPI	
Printing:	Letter, Executive, Legal	
Print Languages:	HPPCL 3 Enhanced	
Memory:	32 MB RAM	
Connectivity:	USB	

2.3.3 Networked Multifunction Laser Printer Standards

Below are the standards for all networked multifunction laser printers to be operated within the CDHS environment.

Multifunction Networked Printer, Sharp		
Category	**Standard**	**Remarks**
Manufacturer:	Sharp	
Model:	AR-M550N	
Resolution:	600 DPI	
Network Interface:	Bidirectional IEEE 1284-B compliant parallel port, USB 2.0 port	
Print Languages:	PCL 6, PCL 5e, PostScript® 3™ emulation	
Memory:	128 MB RAM	
Printing:	Letter, Legal, Duplexing	

Multifunction Networked Printer, HP		
Category	**Standard**	**Remarks**
Manufacturer:	HP	
Model:	LaserJet 9050mfp (9050DN is acceptable)	HP P/N Q3728A This item is not on the CSSI contract. No MFP is covered under CSSI
Resolution:	600 DPI	
Network Interface:	Bidirectional IEEE 1284-B compliant parallel port, available EIO slots	
Print Languages:	PCL 6, PCL 5e, PostScript® 3™ emulation	
Memory:	128 MB RAM	
Printing:	Letter, Legal, Duplexing	

2.4 Software Standards – Tier 1

All newly acquired personal computers must be configured with the authorized CDHS Tier I Build which consists of the following software. The Client Technology Unit (CTU) is responsible for creating the authorized CDHS Tier I Build.

Category	Standard	Remarks
Operating System:	Microsoft (MS) Windows XP Professional SP2	Support for Windows 2000 Pro ends June 2009
Hard Disk Encryption	GuardianEdge Encryption Plus Hard Disk 7.1.5	
Office Application Suite:	MS Office 2003 Professional SP2 - MS Word - Word Processing - MS Excel - Electronic Spreadsheet - MS PowerPoint - Presentation Graphics - MS Access – Database	Support for Office XP (2002) ends June 2008 Support for Office 2000 ends June 2007
Anti-Virus:	Symantec Antivirus 10.0.2.2021	Check with ITSD for the latest recommended version
System Management:	MS Systems Management Server (SMS) 2003 SP1	
E- Mail and Calendaring:	MS Outlook 2003	Support for Outlook XP (2002) ends June 2008 Support for Outlook 2000 ends June 2007
Web Browser:	MS Internet Explorer v6 SP1	IE v7 under testing
Compression Software:	WinZip 11.0	
Document Reader:	Adobe Acrobat Reader 8.x	

2.5 Software Standards – Tier 2 & Tier 3

The following software packages are to be used for specific individual and workgroup applications when needed:

Category	Standard	Remarks
Project Management	MS Project 2003	Support for Project 2002 ends June 2011 Support for Project 2000 ends June 2009
Document Publishing	Adobe Acrobat 8	
Web content development	MS FrontPage 2003	Support to be retired February 2008
Application Development	MS Visual Studio 2005	
Diagramming	Visio 2003	Support for Visio 2002 ends June 2010 Support for Visio 2000 ends June 2007
3270 Terminal Emulation:	IBM Personal Communications	
Secure FTP	Ipswitch WS-FTP Pro 2007	
Data Analysis	SAS	
Geographic and Spatial Analysis	ArcGIS, ArcView, ArcInfo 9.x	
Graphics Editor	Adobe PhotoShop CS2	
Graphics Design	Adobe Creative Suite Standard	
Desktop Reporting	Crystal Reports XI	
Screen Capture	SnagIt 8.x	
Screen Recording	Camtasia Studio Presentation 4.x	
Speech Recognition	Dragon NaturallySpeaking 9	
Browser animation plug-in	Adobe Flash Player 9	
Web Conferencing plug-in	Microsoft Live Meeting WebEx	Note: Streaming video should only be done after consultation with ITSD
DVD Authoring	Pinnacle Avid Liquid Pro	
Reference management	EndNote, Reference Manager	
Self Extracting Compression	WinZip Self-Extractor 3.0	

Computer Aided Design	Autodesk AutoCAD, Autodesk Raster Design	
Website Testing - Firefox	Firefox 2.0	For authorized website testing only, not to be used for general Internet browsing or set as the default browser.
Website Testing – Internet Explorer	Internet Explorer 7.0	For authorized website testing only, not to be used for general Internet browsing or set as the default browser. IE 7.0 will later be approved for general purpose use.
Peripheral Support	Label printing software, DVD/CD burner software, DVD Player software, Scanning software, Photo loading software, Mouse driver	Software use is limited to the minimal necessary software to operate the peripheral, and which was included free. This does not include suites and other evaluation software bundled with the hardware.

2.6 Software Standards – Administration Utilities

The following software packages will generally only be used by authorized PC or Server administrators:

Category	Standard	Remarks
Desktop Imaging	Symantec Ghost Solution Suite (Ghost 10)	
Remote Control	PC: Microsoft SMS Server: Microsoft Terminal Server	
Server Administration Utilities	Dameware 6.x Lieberman User Manager Pro 7.0x Lieberman Service Account Manager 5.0x SecureCopy Vcom Partition Commander 10 HP Web JetAdmin 8.x SysInternals	
Active Directory Utilities	Netpro Diagnostics for Active Directory Suite Scriptlogic Active Administrator 4.0x ADJanitor Quest Recovery Manager	

2.7 Mobile Computing Standards

2.7.1 Wireless Messaging Standards

Below are the standards for Wireless Messaging devices to be operated with the CDHS departmental infrastructure.

Category	Standard	Remarks
Manufacturer:	Research in Motion	
Model:	Sprint Blackberry 8703e Nextel Blackberry 7520, 7100i Verizon Blackberry 8703e	
Synchronization:	Must not require local administrative or elevated user or network rights for normal use.	Desktop Manager v 4.1 needed to manually synchronize device

3 Network Server Technology Standards

The server standards covered in this document have been prepared by the Information Technology Services Division (ITSD) of the California Department of Health Services (CDHS) and must be adhered to when purchasing CDHS servers. The following server standards were developed to maximize server availability, supportability, security, data integrity and to lower the total cost of ownership in CDHS. These server standards apply to all CDHS servers or servers containing CDHS information whether they are acquired or maintained through normal CDHS procurement channels or outside contractors.

3.1 Server Hardware Standards

Server hardware shall be purchased that conforms to the following standards. For specific models, part numbers and prices, contact the ITSD Server Support Unit. Since models change frequently, the list is maintained and updated regularly. Contact the ITSD Server Support Unit to size special or non-standard server configurations. Note that application and database servers may require an approved feasibility study report (FSR) prior to purchase.

3.1.1 Standard Server Configuration

The following hardware configuration is the standard configuration for most of the servers within CDHS. These systems are the basic platform for file, print, web, monitoring, backup, domain controllers, WINS, DNS, DHCP, ISA, application and small to medium database servers.

Category	Standard	Remarks
Server Type:	Dell PowerEdge 29xx series with rack mount conversion kit	
Processor :	Two Intel Xeon Dual Core processors at 2.8 GHz or higher	Included in CSSI-Basic 2 PC Server
RAM Memory:	2 GB RAM or higher	Included in CSSI-Basic 2 PC Server
Controller:	Embedded RAID – PERC5. Minimum of 256 MB Battery Backup Write and Read Cache (BBWC)	Included in CSSI-Basic 2 PC Server
Disk Drives:	A minimum of four SCSI 72GB or bigger drives. Standard configuration is Raid 5 plus one hot spare	CSSI Off Spec Only 36 GB hard disk drives are on CSSI for this model.
Network Interface Card:	Dual NIC 10/100/1000	Included in CSSI-Basic 2 PC Server
Power Supplies:	Dual redundant hot plug power supplies	Included in CSSI-Basic 2 PC Server
Fans:	Dual redundant hot plug fans	Included in Basic 2 PC Server
Warranty:	Four years of DELL service maintenance should be purchased with the server. This is a 24x7x4 hours.	Upgrade to CSSI –Basic 2 PC Server
DRAC Dell Remote Access Card:	These boards are not required but may be purchased to provide access to servers installed at remote locations	CSSI Off Specs

3.1.2 High End Server Configuration

The following high end server specifications are typically used for large database servers and Exchange e-mail servers. Anyone purchasing such servers should consult with the ITSD Server Unit to determine appropriate size and capacity needed.

Category	Standard	Remarks
Server Type:	Dell PowerEdge 2900 series with rack mount conversion kit.	CSSI- Basic 2 PC Server-
Processor:	Two Intel Xeon Dual Core processors at 2.8GHz or higher	The dual core processors are an allowed option under CSSI.
RAM Memory:	2 GB Ram or higher	
Disk Drives:	A minimum of four SCSI 72GB or bigger drives. Standard configuration is Raid 5 plus one hot spare	CSSI Off Spec Only 36 GB hard disk drives are on CSSI for this model.
RAID Controller:	Embedded RAID - PERC5. Minimum of 256 MB Battery Backup Write and Read Cache (BBWC)	
Network Interface Card:	Dual NIC 10/100/1000	Multiple NICs may be used for special circumstances only.
Power Supplies:	Dual redundant hot plug power supplies.	
Fans:	Dual Redundant Hot Plug Fans.	
Warranty:	Four years of DELL service maintenance should be purchased with the server. This is a 24x7x4 hours.	Upgrade to CSSI –Basic 2 PC Server
DRAC Dell Remote Access Card:	These boards are not required but may be purchased to provide access to servers installed at remote locations	CSSI Off Spec

3.1.3 Custom Server Configuration

Custom servers shall comply with the above standards as closely as possible. The purchase of a non-standard server shall be based on specific business needs that can not be met with either a standard server or an approved high end server. These needs must be justified in writing and receive CIO approval prior to its purchase. Any request for a non-standard server shall be reviewed by the ITSD Server Management Unit and their input will be given to the CIO before a final purchasing decision is made.

3.1.4 Racks and Accessories

Servers shall be properly mounted in a rack designed to house servers and have rack-mounting rails designed specifically for the server type. All servers being purchased shall be rack mountable style. Freestanding models are not acceptable. The following types of racks, Uninterruptible Power Supplies (UPS) and accessories need to be purchased for the number of servers and types being installed.

Category	Standard	Remarks
Racks:	Hewlett Packard (HP) 36U server racks. A maximum of 3 UPSs per rack and no more than 6 servers per rack will be located in each rack if only one 20 amp circuit is provided to that rack.	
UPS:	HP Smart UPS standard, 1500 watt - 110 volt plug versions only. One 1500 watt UPS may only serve a maximum of two servers. All power supplies in a given server should be plugged into a common UPS.	Due to their weight, UPSs must be mounted at the bottom of the rack.
Rails:	Each server shall have rails that allow it to be mounted in a standard 19” server rack.	
Other:	One Monitor, Keyboard, Mouse and 8-port IP Enabled KVM switch will be purchases for every two racks installed. (Exception: In small sites where only one rack is installed, one Monitor, Keyboard, Mouse and a 4-port KVM switch can be purchased per rack.)	
Tape Media Format:	LTO960	
Tape Library:	HP MSL6030, MSL6060, ELS322E	

3.2 Server Software Standards – Tier 1

Software purchased for CDHS servers shall adhere to the following standards. Application level software written or developed for CDHS servers shall be compatible with the above hardware and the following software standards. For specifications on the current versions of the listed Tier 1 software, please contact the ITSD Server Support Unit.

Tier 1 server software encompasses the operating system and software that is common to all servers on the CDHS network.

Category	Standard	Remarks
Operating System:	Microsoft Windows Server 2003 SP1. Enterprise Edition, x64, and R2 versions are permitted when required by an application/	Support for MS Windows Server 2000 SP4 ends Dec 2007
Anti-Virus:	Symantec Antivirus 10.0.2.2021	Check with ITSD for the latest recommended version
Installation:	HP SmartStart 7.x and Dell Openmanage Server Assistant 5.x	
Backup:	Veritas Backup Exec 11.D	Support for Veritas Backup Exec 10D with SP3
Asset Management:	Microsoft Systems Management Server 2003 SP1	
Server Monitoring:	HP System Insight Manager 5.0 HP OpenView 7.5 Dell Open Manage 8.x	
Patch Deployment:	Update Expert 6.3 or SMS	
Web Browser:	Internet Explorer 6.0	
Remote Administration:	Terminal Services	Built into Microsoft OS
Power Management:	HP Power Management 4.0	

3.3 Server Software Standards – Tier 2

Software purchased for CDHS servers shall adhere to the following standards. Application level software written or developed for CDHS servers shall be compatible with the above hardware and the following software standards. For specifications on the current versions of the listed Tier 2 software, please contact the CDHS Service Desk.

Tier 2 software includes commonly used applications that are used on a large number of servers, such as File, Print, Web, Database and E-mail servers that are the foundation for other specific applications that may run on top of these servers. Tier II software assumes that all standard software in Tier 1 is used unless otherwise specified below.

3.3.1 Messaging

Category	Standard	Notes
Messaging Software	Exchange 2003 Enterprise Edition SP2	
Email Encryption	Voltage Appliance 3.0	
Content Filtering & Anti-Spam	Proofpoint Appliance 4.0	
Fax Servers	Right Fax 9.3 FP1	
List Servers	LSoft ListServ 14.4	
Storage Area Network:	HP SAN Platform Kit 3.0F Microsoft MPIO Driver	
Email Anti-Virus	Trend Micro Scan Mail for Exchange 7.0	

3.3.2 Web

Category	Standard	Remarks
Web Server	MS Internet Information Server (IIS) 6.0	Support for IIS 5.0 ending Dec 2008
Content Management	MS Office SharePoint Portal 2007	Site Server 3.0, SharePoint 2003 and Content Management Server 2003 support ending Dec 2008
SharePoint Template Development	MS SharePoint Designer	
Performance Diagnostics		Support for Spotlight 3.0 (IIS 5.0) ending Dec 2007
Web Analytics Reporting	Webtrends 8	
Usability & Accessibility	WatchFire Web XM 4.5	
PKI Certificates	Verisign Managed PKI	
Secure FTP	IP Switch WS-FTP	
Application Monitoring	Applications Manager 7.0	

3.3.3 Database Management

Category	Standard	Remarks
SQL Servers	Microsoft SQL 2005 SP1	Also support for SQL 2000, SP4. Support for SQL 7 with SP4, Security fix 1004 ends June 2007
DB Administration	Idera SQLSuite, Ent. Ed.	
Database Tuning:	SQL Server Resource Kit Idera SQL Suite – Ent. Ed.	Resource Kit includes: SQL Load Simulator, Data Simulator, Database Generator, Data Sizer, SQL Execution Timer, SQL Hard Disk Test Utility
Database Diagnostic:	SQL Profiler Idera SQL Suite – Ent. Ed.	
Database Auditing:	Idera SQL Suite – Ent. Ed.	
Database Change Management:	Redgate SQL Bundle	
Database Reporting and Business Intelligence	Business Objects 6.5 MS SQL Reporting Services 2005	

3.3.4 Service Desk

Category	Standard	Remarks
Core Component:	Remedy Action Request System (ARS) Software, Version 6.3	
Help Desk Component:	ITSM Help Desk Module, Version 6.0	
Asset Management Component:	ITSM Asset Management Module, Version 6.0	
Change Management Component:	ITSM Change Management Module, Version 6.0	
Report Component:	Crystal Reports, Version 8.5/9	Developing reporting capabilities with Business Objects
Service Level Agreement Component	Remedy Service Level Agreement Module, Version 6.0	
Remedy Web Component	Remedy Mid-Tier 6.3	

3.3.5 Remote Access and Communication

Category	Standard	Remarks
Remote Access	Citrix Presentation Server 4.0	
Blackberry to Exchange Synchronization	RIM Blackberry BES 4.1	
Mainframe Gateway	Microsoft Host Integration Server 2000 Version 5.00.0798	
Web Conferencing	Avaya Meeting Exchange	

3.3.6 Infrastructure Support and Utilities

Category	Standard	Remarks
IP Address allocation	Microsoft DHCP, Windows Server 2003	
Name Resolution	Microsoft DNS and WINS, Windows Server 2003	
Directory Services and Authentication	Active Directory 2003	
Anti-Virus	Symantec Enterprise Security Architecture (SESA) 2.1 Symantec System Center 6.0	

Asset Management	MS Systems Management Server 2003, Version 2.50.3174.1018 SMS Advanced Client Version 2.50.3174.1015	
Application Security Gateway	MS Internet and Acceleration Server 2006	
Message Broker	MS BizTalk 2006	
Server Monitoring	HP Insight Manager 7.3	
Disk Defragmenter	Diskeeper 2007 Server	

3.3.7 Security

Note: Several of these security tools have network and client components however all are consolidated here for convenience.

Category	Standard	Remarks
Server auditing and reporting	Ecora Auditor Professional	
Server Intrusion Detection	Cisco Security Agent	
Network Intrusion Detection	Cisco IDS/CiscoWorks VMS	
Windows Event Log Collection	GFI EventsManager 7	
Computer Forensics	Guidance EnCase	
Network Scanning and Auditing	nCircle IP360, nCircle Security Intelligence Hub, Nessus	
Event Data Consolidation	Symantec Security Information Manager 4.5, WinSSHD	
Internet Content Filter	Websense Enterprise	

3.4 Server Environmental Standards

In order to maximize uptime and avoid costly repairs, servers must be maintained in a suitable environment. The following standards outline optimal conditions for servers and should be adhered to as closely as possible. Major deviations from these requirements must be approved in advance by the CIO.

Servers are to be maintained in a secure, cool, dry, and relatively dust free environment with adequate electrical and air conditioning service to meet the loads required by the servers. CDHS programs shall address the environmental requirements listed below for the total number of servers being installed before purchasing server equipment.

Category	Standard	Remarks
Air Conditioning:	Adequate tonnage of air conditioning shall be provided to accommodate the BTU output of all servers in order to maintain the temperature and humidity standards. Redundant air conditioning should be provided in large facilities housing many servers.	
Electrical:	One or two dedicated 110-volt 20-amp circuits with a minimum of four outlets shall be provided for each server rack.	
Humidity:	Maintain relative humidity between 40% and 60%, 24 hours and 7 days a week.	
Miscellaneous:	No food, drinks or liquids should be allowed in the immediate vicinity of any server or server rack.	
Space: Required:	Each rack requires 2’ wide x 9’ long clear floor space to permit access to the front and back of each rack.	
Storage/Access:	Each server shall be rack mounted in a secure locked room and/or locked rack in such a manner that physical access to the server is limited to server administrators only.	
Temperature:	Maintain ambient air temperature between 66 and 72 degrees Fahrenheit, 24 hours a day, 7 days a week.	

4 Network and Data Communication Standards

The Telecommunications, Network, and Remote Access standards described here were compiled by the Network Infrastructure Unit (NIU) of the Information Technology Services Division (ITSD) of the California Department of Health Services (CDHS). These standards were developed to ease connectivity into, maintain compatibility with, and reduce the total cost of ownership of the CDHS Enterprise Network. Abiding by these standards will allow CDHS to keep the CDHS Enterprise Network current with regards to patches, fixes, and updates. Exceptions to these standards must be processed through the CDHS exception process.

4.1 Telecommunication Standards

In general, CDHS standards usually provide for two (2) CAT5e data jack and two (2) analog telephone jacks per workstation. All telephone services, including DSL, Digital, ISDN, Multi-channel, ISDN, BRI's and PRI's, are handled by the Telecommunications Unit of Programs Support Branch through a Telephone/Data Service Request Form or through DTS depending on the termination point.

4.1.1 High-speed Data Circuits

The following High-speed Data circuits, acquired through DTS via the Service Request Process, are currently approved methods for the CDHS Enterprise WAN.

Category	Standard	Remarks
OC3		Provided by DTS
T3	ATM & Point-to-Point	Provided by DTS
T1	Frame Relay	Provided by DTS
Fractional T1	Frame Relay	Provided by DTS
DSL:	Private or Internet	Provided by DTS
ISDN		Provided by DTS

4.1.2 Voice Circuits

The following circuits, acquired through DTS or CDHS's Program Support Branch, are currently approved methods for voice circuits and phone bridges.

Category	Standard	Remarks
Channelized T3		Provided by DTS or PSB
Channelized T1		Provided by DTS or PSB
PRI		Provided by DTS or PSB
BRI		Provided by DTS or PSB

4.1.3 Telecom Closet Standards

The following items must be met to meet the minimum qualifications for a CDHS Main Data Facility (MDF) or an Intermediate Data Facility (IDF).

Category	Standard	Remarks
Temperature	A/C capacity to maintain 72 degrees during summer.	
Electrical	Dedicated Circuit availability up to 30 amps.	
Physical	Key lock or key card restricted/limited access	
MPOE access	MDF direct access to MPOE or in same room.	
Other:	SBC requirements	

4.1.4 Racks and Accessories

The following items are used to populate the Main Data Facility (MDF) or an Intermediate Data Facility (IDF).

Category	Standard	Remarks
Racks:	Chatsworth Universal 19" or equivalent enclosure	pending application
UPS:	APC Rack-mount Smart-UPS 20 amp versions, usually 1500XL or 2200XL	15 min. min.; 1/pwr supply/device
Cable Runways:	Chatsworth Universal or better	
Seismic:	As necessary to meet or exceed State Earthquake Zone Requirements	
Electrical:	Minimum 2 – Dedicated 20 amp electrical circuits	
Other:		

4.2 Network Topology Standards

Current network topology standards are based on a hub and spoke design with DTS as the hub point for all CDHS sites. CDHS remote sites are connected to the CDHS Enterprise network via a Dynamic Multipoint Virtual Private Network (DMVPN). This provides an end-to-end encrypted tunnel that drops off behind the EEC firewall, providing a secure data transport path within the DTS network. Firewalls are used at the transition points between the Edge of the CDHS Enterprise network and the DTS network, and into the CDHS Extranet.

4.3 Network Topology and Equipment Standards

CDHS has standardized on Cisco Systems Inc. for our network equipment. The primary reason for this is the ability to push out patches and updates to this equipment from a central management tool.

4.3.1 Router, CSU/DSU Hardware

Category	Standard	Remarks
DSL (1-10 users)	Cisco 1700 Series with K9 Security Bundles w/ internal CSU/DSU	provided through DTS
Low capacity (1-300 Users)	Cisco 2800 Series with K9 Security Bundles w/ internal CSU/DSU	provided through DTS
Mid capacity (300-1000 Users)	Cisco 3800 Series with K9 Security Bundles w/ internal CSU/DSU	provided through DTS
High capacity (1000+ Users):	Cisco 7200 Series with K9 Security Bundles w/ internal CSU/DSU	provided through DTS

4.3.2 Switching Hardware

Category	Standard	Remarks
Access <40 staff	Cisco 2960 Series	
Access >100 staff	Cisco 3750 / 3750G or 4500 Series	
Distribution	Cisco 4506 Series or Cisco 6500 Series	
Core	Cisco 6500 Series for a large campus'	
Other:		

4.3.3 Battery Backup / UPS Standards

Category	Standard	Remarks
UPS:	APC Rack-mount Smart-UPS 20 amp versions, usually 1500XL or 2200XL	15 min. min.; 1/pwr supply/device
Other:	APC UPS Network Management Card	

4.4 Data Cabling & Connector Standards

4.4.1 Data Cabling Standards

Category	Standard	Remarks
Copper 300' max	CAT5e or higher	
Fiber 0-2000'	62.5/125 micron Multi-mode fiber	
Fiber 2000' +	8 micron Single-mode fiber	
Copper Patch Cord	CAT5e or higher stranded patch cord, wired straight through.	Length based on application.
MMF Patch Cord	62.5/125 terminated with SC connectors on each end.	Length based on application.
SMF Patch Cord	62.5/125 terminated with SC connectors on each end.	Length based on application.
Other		

4.4.2 Data Jack/Connector/Wiring Standards

Category	Standard	Remarks
Copper Jacks	RJ-45 wired to AT&T 568B specs	
Fiber Jacks	SC form factor	
Copper Patch Panels	Panduit Data-Patch CAT5e Patch Panel T568B Wired or equivalent	
Fiber Patch Panels	Leviton RDP Series Fiber Rack-mount enclosures or equivalent.	
Other:		

4.5 Communications Protocols and Addressing Standards

4.5.1 Protocols Standards

Category	Standard	Remarks
Routing	RIP, EIGRP	
Routed	IP, SNA, DLSW	

4.5.2 IP Addressing Standards

CDHS is deploying a Private IP (PIP) Addressing throughout the CDHS Enterprise. Below is a summary of how PIP will be deployed and broken out at our remote sites.

Management Networks

The first choice at each site is to have a separate network for the infrastructure management from the user subnets. This would allow the users network to be disabled when needed for troubleshooting, and still be able to manage the infrastructure devices. The limitation on this design would be dependent upon the site's router model and IOS. If the hardware limitation does not allow this implementation, then the user and management networks will be from the same class C.

From the class B network, the first eight class C's will be designated as the management subnets. We will not use (initially) the first class C – 10.1.0.0. Further, each class C will be subnetted with a mask of 255.255.255.224 (27 bit). This will give eight subnets per class C, with 32 available hosts (devices) in each subnet. The DTS router will use the first IP address in the subnet. Infrastructure devices will begin with the fourth IP address. See sample table below.

Network	Router	Infrastructure IP Range
10.1.1.0	10.1.1.1	10.1.1.4 – 10.1.1.31
10.1.1.32	10.1.1.33	10.1.1.36 – 10.1.1.63
10.1.1.64	10.1.1.65	10.1.1.68 – 10.1.1.95
10.11.96	10.1.1.97	10.1.1.100 – 10.1.1.127
10.1.1.128	10.1.1.129	10.1.1.132 – 10.1.1.159
10.1.1.160	10.1.1.161	10.1.1.164 – 10.1.1.191
10.1.1.192	10.1.1.193	10.1.1.196 – 10.1.1.223
10.1.1.224	10.1.1.225	10.1.1.228 – 10.1.1.255

User Subnets (networks)

Category	Standard	Remarks
Subnet Class	Users will have full class C's for their IP addresses	
Network Assignment	Networks will be assigned in order as rollout proceeds (as with the management networks).	
Network Start	The first network used will be 10.1.8.0	
Subnet Expansion	Each remote site will have either 1 or 2 additional class C, not initially configured, but allocated for future use	
Initial Network	Each remote site's initial user network will be an even numbered network (10.1.8.0, 10.1.10.0, etc.).	

Usage of 4th Octet

Sites With Separate Management Networks		
Address Range	**Purpose**	**Quantity**
10.1.x.0	Network	
.1	Default gateway (actual or HSRP)	1
.2-.3	Default gateway (switches if HSRP)	2
.4-.15	Reserved for future use	12
.16-.191	Computers	176
.192-.223	Special use (NAT, switches, etc)	32
.224-.254	Printers	31
.255	Broadcast	1
		255 Total

Sites With Combined User and Management Networks		
Address Range	**Purpose**	**Quantity**
10.1.x.0	Network	
.1	Default gateway (actual or HSRP)	1
.2-.3	Default gateway (switches if HSRP)	2
.4-.31	Infrastructure Management	28
. .32-.191	Computers	160
.192-.223	Special use (NAT, switches, etc)	32
.224-.254	Printers	31
.255	Broadcast	1
		255 Total

Items to be addressed with site contact:

- Redefine print queues
- Readdress servers and network devices.
- Note any applications that require specific access to foreign entities
- Note any (internet) sources that require access to devices within the site
- Note any (extranet) sources that require access to devices within the site
- Reboot all workstations

4.6 Network Management Standards

Category	Standard	Remarks
Up/Down Alerting	HP OpenView Network Node Manager 7.5 or higher	
Device Configuration	CiscoWorks 2000 LAN Management System 2.5 and Virtual Management System 2.3 or higher	
Performance Monitoring	nGenius Performance Manager 3.01 or higher	
Authentication	Cisco TACACS Windows v3.3	

4.7 VPN Standards

Category	Standard	Remarks
VPN Client	Cisco VPN Client, for use with DTS VPN	VPN is for special use cases only, Citrix is the CDHS remote access standard.

4.8 Enterprise Video Conferencing Standards

The general design of the CDHS Enterprise Video Conferencing network incorporates ISDN PRI's to our larger office locations and multiple ISDN BRI's at our smaller office locations. In a large campus environment, where there are multiple video conferencing rooms, CDHS incorporates a gateway to convert the ISDN based H.320 protocol to the H.323 protocol so that IPVC can be distributed throughout the campus.

Category	Standard	Remarks
End Stations	Tandberg stations	Sized according to need / room size.
MCU	Tandberg MCU 16	Centralized
Gateway	Tandberg Gatekeeper	Primarily for campus environment use.
Management.	Tandberg Management Suite (TMS) & Scheduler	Centralized

5 Naming Standards

5.1 E-mail Address Standards

Prior to July 1, 2007

The CDHS Internet E-mail address standard will consist of the individual's first name initial followed by up to 7 characters of their last name, followed by @dhs.ca.gov. Example: jdoe@dhs.ca.gov. Duplicate names will be differentiated by the addition of a number added to the end of the individual's name. Example: jdoe2@dhs.ca.gov.

Effective July 1, 2007

The following new E-mail address standards will go into place July 1, 2007, due to the Department split. This E-mail address format will be used on all new E-Mail. Individual staff will be assigned the correct domain name depending on which department they work for after the split.

Firstname.Lastname@dhcs.ca.gov (Department of Health Care Services)
Firstname.Lastname@cdph.ca.gov (Department of Public Health)

Duplicate names will be differentiated by the addition of a number added to the end of the individual's last name. Example: **John.Smith2@dhcs.ca.gov**

For a period of time yet to be determined, pre-existing email addresses will continue to function. Additionally, to ease transition, email sent to the old E-mail alias combined with the new domain name will be supported, e.g. someone with E-mail address **jdoe@dhs.ca.gov** can receive E-mail under **jdoe@dhcs.ca.gov** or **jdoe@cdph.ca.gov** depending on which Department they work for.

5.2 Userid Naming Standards

Userids must be unique across all of CDHS, and use only alphabetic and numeric characters. The following naming conventions are to be used within CDHS:

- Userid is constructed with the person's first initial and last name, up to 8 characters
- Conflicts will be resolved by adding a number to the end of the Userid, keeping it within 8 characters
- The first two letters will be capitalized
- The full name field will be "Last Name, First Name"

Administrative Userids will be the same as the regular Userid, but with an "a" suffix.

5.3 PC Naming Standards

The following naming conventions must be used on all CDHS workstations:

All workstations will be named **XXXYYYYZZZZZZZZ** where:

XXX is the acronym assigned to the program, branch or division (3 chars)
YYYY represents the facility location number (4 digits)
ZZZZZZZZ represents the CDHS asset tag number (8 chars max)

If assistance is needed on naming, contact ITSD through the Remedy help desk system.

5.4 Network Printer Naming Standards

The following naming conventions must be used on all CDHS networked printers:

Printer Name (or Description):
9999-999-XXX-Q99 Make-Model-UserVariable

The first 4-digit field is the building location code, the next 3-digit field is the Floor #, the next 3 letters are the program ID and the last 2-digit is the print queue sequential #. The printer Make and Model, and specific user(s) if any, are appended to be more informational.

Example: 1541-1st-ITS-Q01 HP LaserJet 4050 Snoopy, which means: “location code 1541 (Bldg 173, 1615 Capitol Ave.), 1st Floor, ITSD, Print Queue 01, which is a HP LaserJet 4050 and may have a common name of Snoopy if desired by the program.”

If assistance is needed on naming, contact ITSD through the Remedy help desk system.

5.5 Server Naming Standards

The following naming conventions must be used on all CDHS servers. Additionally, the description field within Active Directory should be filled in with the location of the server.

Windows Servers are named **DHSXXXXYYYNN** where:

DHS DHS is always the first 3 characters.
XXXX Physical location, Domain name, Zone type or Program name, and may use 3 or 4 characters
YYY Server function or application type, and is 2 or 3 characters.
NN Is a two digit sequential number (01-99) to make the server unique when multiple servers of one type exist and also indicate the type of server

The following page gives examples of the most common uses of the XXXX and YYY fields

DHSXXXXYYYNN Breakdown

Use of XXXX Field:

EXC	Exchange Server
EXT	Server in the Extranet Domain and zone
INT	Server in the Internet Domain and zone
RLC	Server at Richmond Labs Campus
SAC	Server in the Sacramento Area
XXXX	In some cases this might be a program acronym

Use of YYY Field:

APP	Custom Applications
BKP	System Backup
CDR	CD ROM Storage
DHC	Dynamic Host Configuration Protocol (DHCP)
DNS	Domain Name System (DNS)
FTP	IIS with Internet File Transfer Protocol
IDC	Active Directory Intranet Domain Controller
INT	Internet Support Services within the Intranet Zone
MSG	Exchange Mailbox Server
OWA	Exchange Outlook Web Access Server
PRX	Proxy Server
PRT	Print Server
RAS	Remote Access Server
RDC	Active Directory Intranet/Root Domain Controller
RDM	Remedy Server

SAA	SAA Gateway
SMS	System Management Server
SNA	System Network Architecture Communication Server
SPR	Spare Server
SQL	SQL Database Server
SRV	File and Print Server
SS	Site Server/Windows Commerce Server
UTL	Utility/Multiple Function
WNS	Windows Internet Naming Service
ZZZ	Specific Application, i.e. DhsSacTrak01, DhsSacVisg01, DhsSacDB201, DhsSacInv01, and DhsSacAcc01

Use of NN field:

01 – 19	Production Server
20 – 29	Test Server (Production Environment)
30 – 39	Development Server
40 – 49	Lab Server

5.6 Group Naming Standards

The following naming conventions must be used when creating groups in Active Directory or on servers.

- Group names should only use A-Z, a-z, 0-9, and dashes. Spaces should not be used unless necessary.
- Group names should include an acronym which identifies the program area or application which the group is associated with.
- Global Groups should only have a DHS prefix if they were previously migrated from an NT4 domain.
- Domain Local Group must begin with the DLG- prefix.
- Server based local groups should be avoided, however if required should have a LOC- prefix.
- Global Groups should be used for organizing people by role, function, organization, or project. Domain Local and Server Local groups should be matched up with specific rights to be granted, and then linked to one or more global groups.
- The Description field should be used to provide additional information about the purpose of the group.

5.7 Group Policy Object Naming Standards

Group Policy Objects within Active Directory must contain the acronym associated with the program or application. Where applicable, the acronym should match the OU the Group Policy is associated with. Misnamed or unidentifiable Group Policy objects are subject to removal.

5.8 DNS Naming Standards

All URL's or DNS names needing visibility only to internal CDHS staff will be placed on the CDHS Internal DNS system. These will be placed within the DNS suffix **intra.dhs.ca.gov**. These names will only be visible to computers on the CDHS network.

URL's or DNS names also needing visibility outside of CDHS (i.e. other state agencies and Internet) will be placed on the CDHS External DNS system. These will be placed within the DNS suffix **dhs.ca.gov**. Names should not be placed in the External DNS unless necessary, due to security considerations.

DNS name creation requests pointed to servers which do not meet the following criteria may require approval by the CDHS CIO:

- Meet all CDHS IT standards
- Are approved by the CDHS Information Security Office
- Meet CDHS and State project guidelines, e.g., FSR requirements
- Are hosted on the CDHS network

Effective July 1, 2007, the following new domain names will be active for use due to the Department split:

dhcs.ca.gov – California Department of Health Care Services
cdph.ca.gov – California Department of Public Health

6 Programming Standards

6.1 Development Languages

The following are standard languages currently in use within CDHS. Note: No new development should be done using the MS Windows - Legacy languages.

MS Windows – New Development
Visual Basic .Net
C#

MS Windows – Scripting
VBScript
JavaScript

MS Windows – Legacy Development
Visual Basic 5.0, 6.0
Clipper 5.2, 5.3, 97
Power Builder 5, 8

Mainframe
COBOL
IBM VisGen (IBM Visual Age Generator)
EGL, Java (IBM Rational Application Developer)
Easytrieve
Natural (Adabase)
REXX
JCL

Database
SQL

7 Revision History

The following revisions have made since the previous version dated June 30, 2006

Section	Changes
1.2	Reference to forms and process in appendix changed to I2E website address.
1.4	Definition of standard added.
2.1	HP Desktop model changed from DC7600 to 7700, IBM Laptop changed from R52 to R60. Tablet PC's added.
2.2	CRT monitors removed.
2.3	Printer section updated to current models.
2.4	Version Updates: WinZip, GuardianEdge, Acrobat Reader.
2.5	Version Updates: Adobe Acrobat, Dragon Naturally Speaking, Visual Studio, WS-FTP Pro, Camtasia, ArcGIS, and SnagIt. Remedy Client removed, new system is web-based.
2.5	Added: Adobe Flash Player, Web Conferencing plug-ins, Adobe Creative Design Suite Standard, Pinnacle Avid Liquid Pro, EndNote, Reference Manager, AutoCAD, Raster Design. Firefox/IE7 (Website Testing).
2.5	Added multiple types of common peripheral software.
2.5	Added: FrontPage 2003 support to end February 2008.
2.6	Version changes for User Manager Pro, Ghost, Service Account Manager Added ADJanitor, Partition Commander, Recovery Manager, HP WebJetAdmin, SecureCopy, SysInternals.
2.7.1	Updated models of supported Blackberry devices. Section 2.7.1/2.7.2 swapped.
2.7.2	Removed PDA section, these should be handled through I2E exception.
3.1.1	Server models changed from 2800/2900 to 29xx updated processors, RAID controller, RAM, removed old references.
3.1.4	KVM changed to IP Enabled KVM, Added tape media and tape library.
3.2	Windows 2003 x64 and R2 versions added.
3.2	Version changes to HP Insight Manager, Dell Openmanage, HP Power, and Backup Exec.
3.3.1	Version upgrades for messaging software.
3.3.2	Applications Manager added as application monitoring tool for Web servers.
3.3.2	Version Updates: Webtrends, Watchfire.
3.3.2	MS Office SharePoint Portal 2007 replaces SharePoint 2003 & Content Management Server 2002.

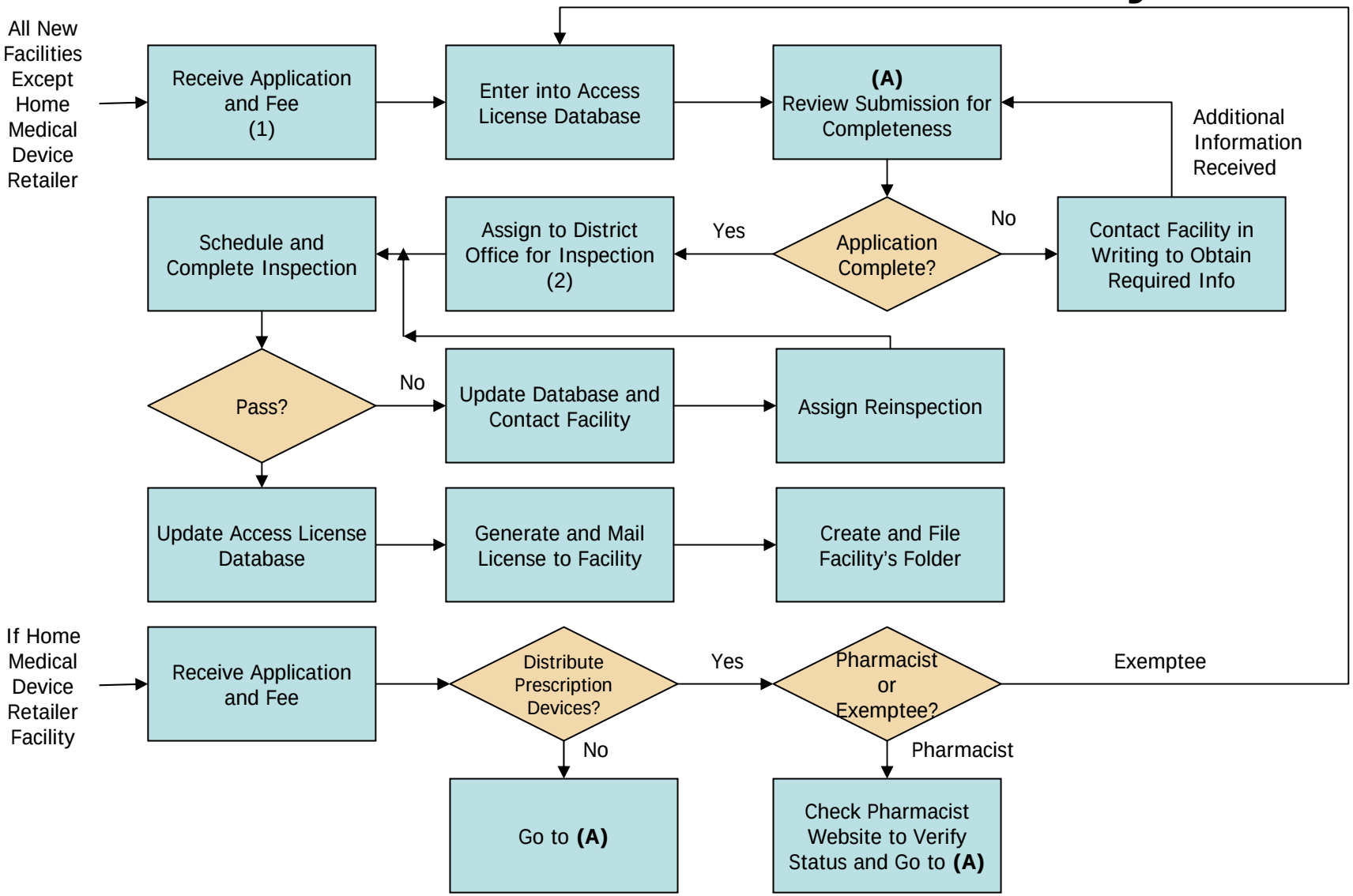
3.3.2	MS SharePoint Designer added.
3.3.3	MS SQL updated to SQL 2005 SP1, Business Objects to 6.5.
3.3.4	Descriptions and versions changed for all sections of Service Desk software.
3.3.5	Blackberry BES version updated.
3.3.6	Version Updates: MS BizTalk, MS ISA.
3.3.6	Diskeeper 2007 Server added.
3.3.7	Added new Security section, and relocated Ecora and Cisco CSA.
3.3.7	Added existing security tools: Cisco IDS, GFI EventsManager, Guidance EnCase, nCircle, Symantec Security Information Manager, Websense Added, WinSSHD. Updated Ecora version.
4.2	Description enhanced.
4.3.2	Switch model updated to 2960.
4.7	Renamed title to VPN Standards, added clarification regarding VPN usage.
5.1	Updated E-Mail standards section to include new naming conventions for Department split.
5.8	Added new domain names for Department Split.
7	Form and process for exceptions was removed, section 1.2 will reference I2E site instead, so the form and process can be updated independently.

Appendix D:

Current Process Flowcharts

Food & Drug Program

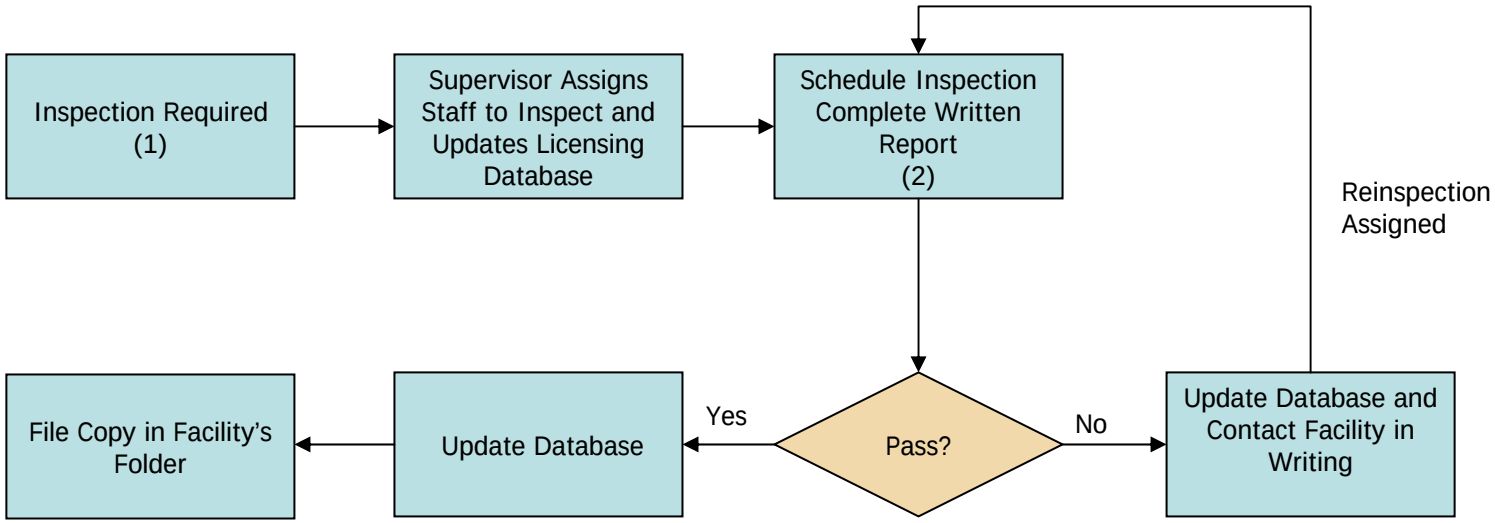
F&D - License New Facility



Note: (1) If a drug manufacturer will make prescription drugs, they must submit a Prescription Drug Manufacturing ACT (PDMA) application for key management with their drug manufacturing application.

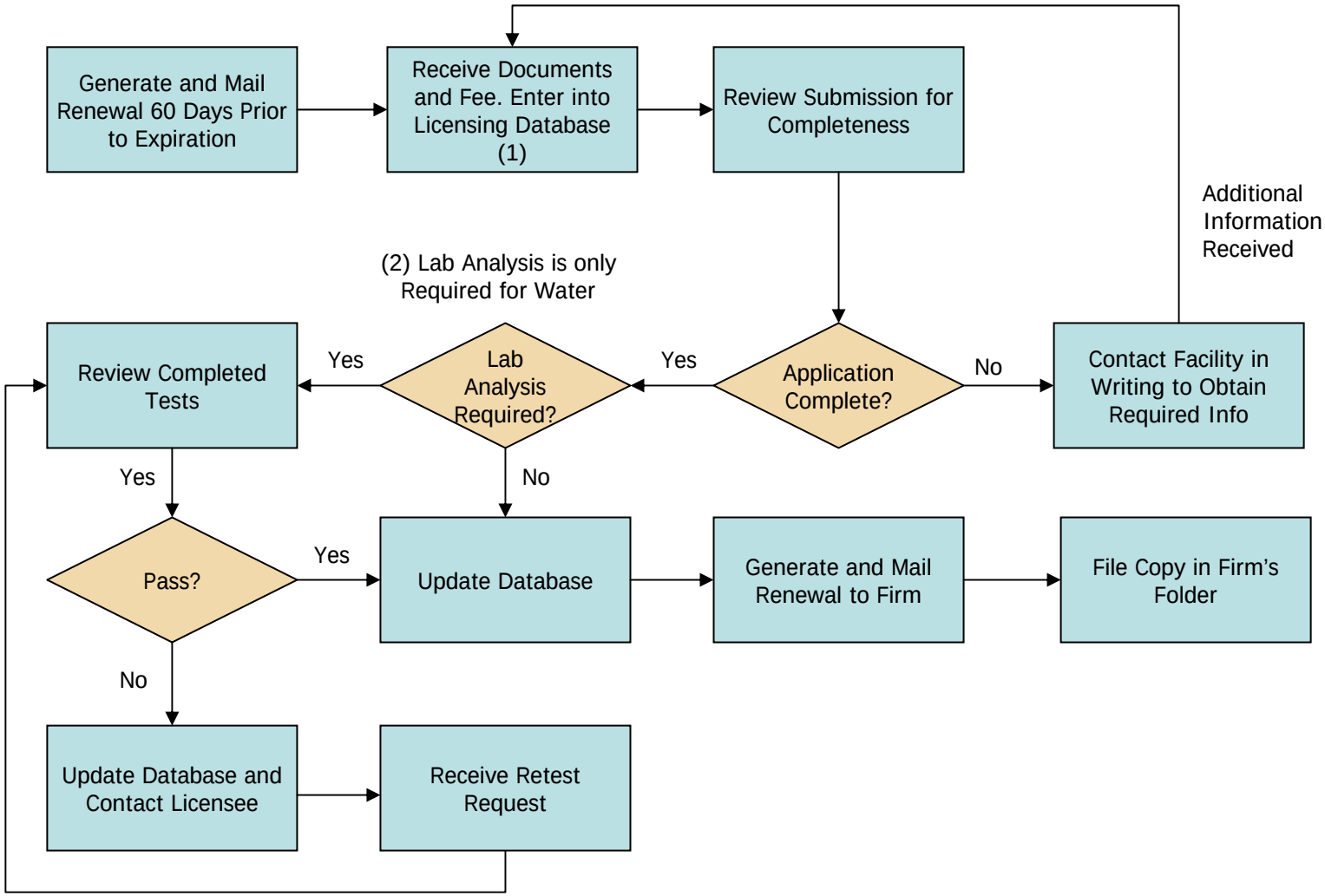
(2) Devise and HMDR assign to supervisor who then assigns to an investigator.

F&D - Inspect Food Processors, Drugs and Devices



Note: (1) Inspection triggers include a complaint, the relative risk factor, or a volatile history.
(2) A second inspection fee is collected if it is for a reinspection for the food program. This is not applicable to Drug, Device and HMDR firms.

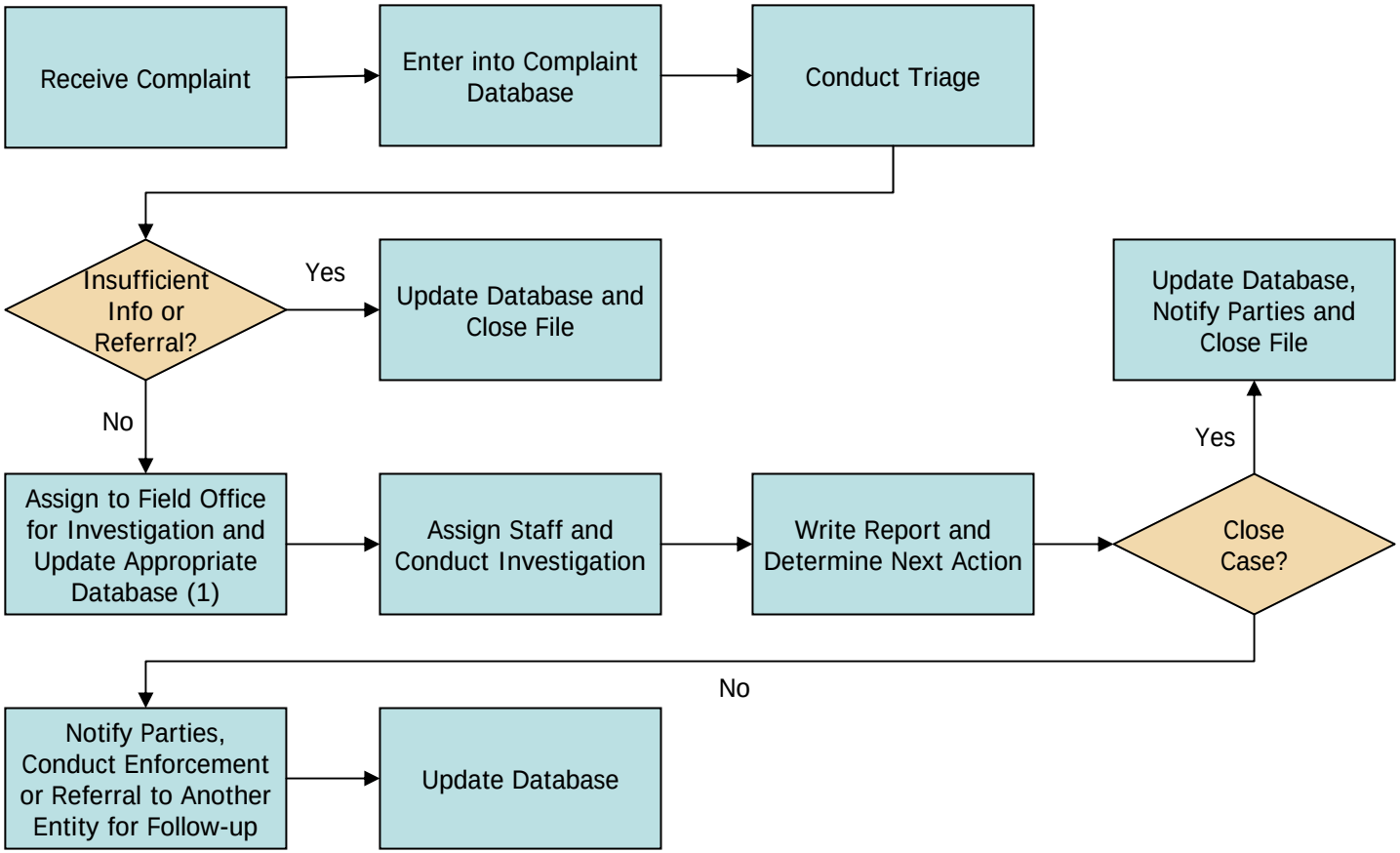
F&D - Renew Food Processors, Drugs, Devices



Note: (1) If renewal application is not received, a late notice is generated. If there is still no response, and invalidation late notice is generated and mailed and referred to enforcement for action.

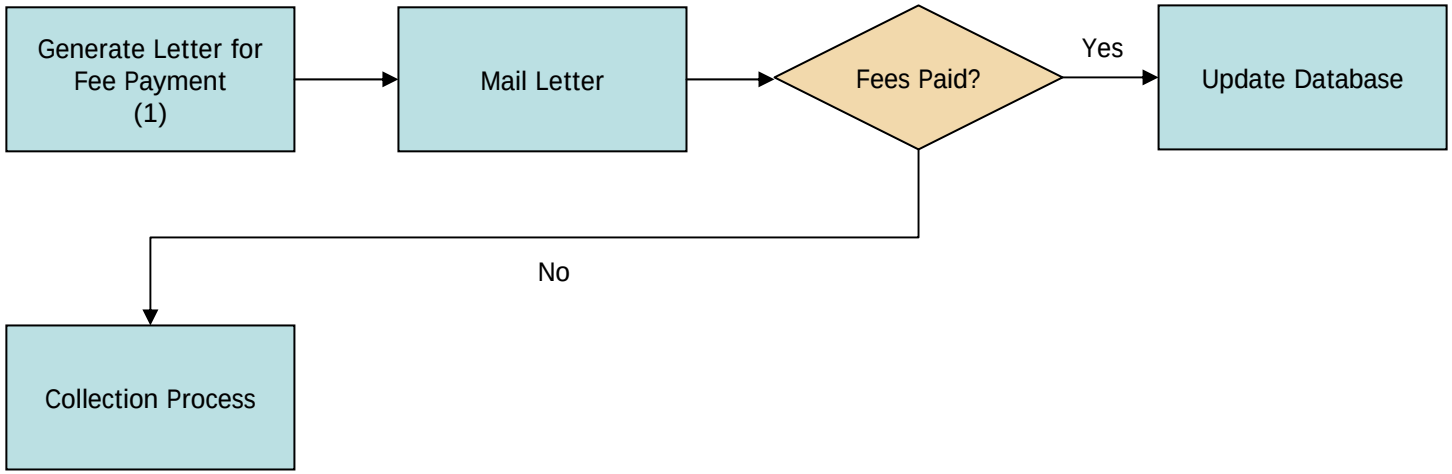
(2) Not required for Drug, Device and HMDR facilities.

F&D - Process Food, Drug, Device Complaint



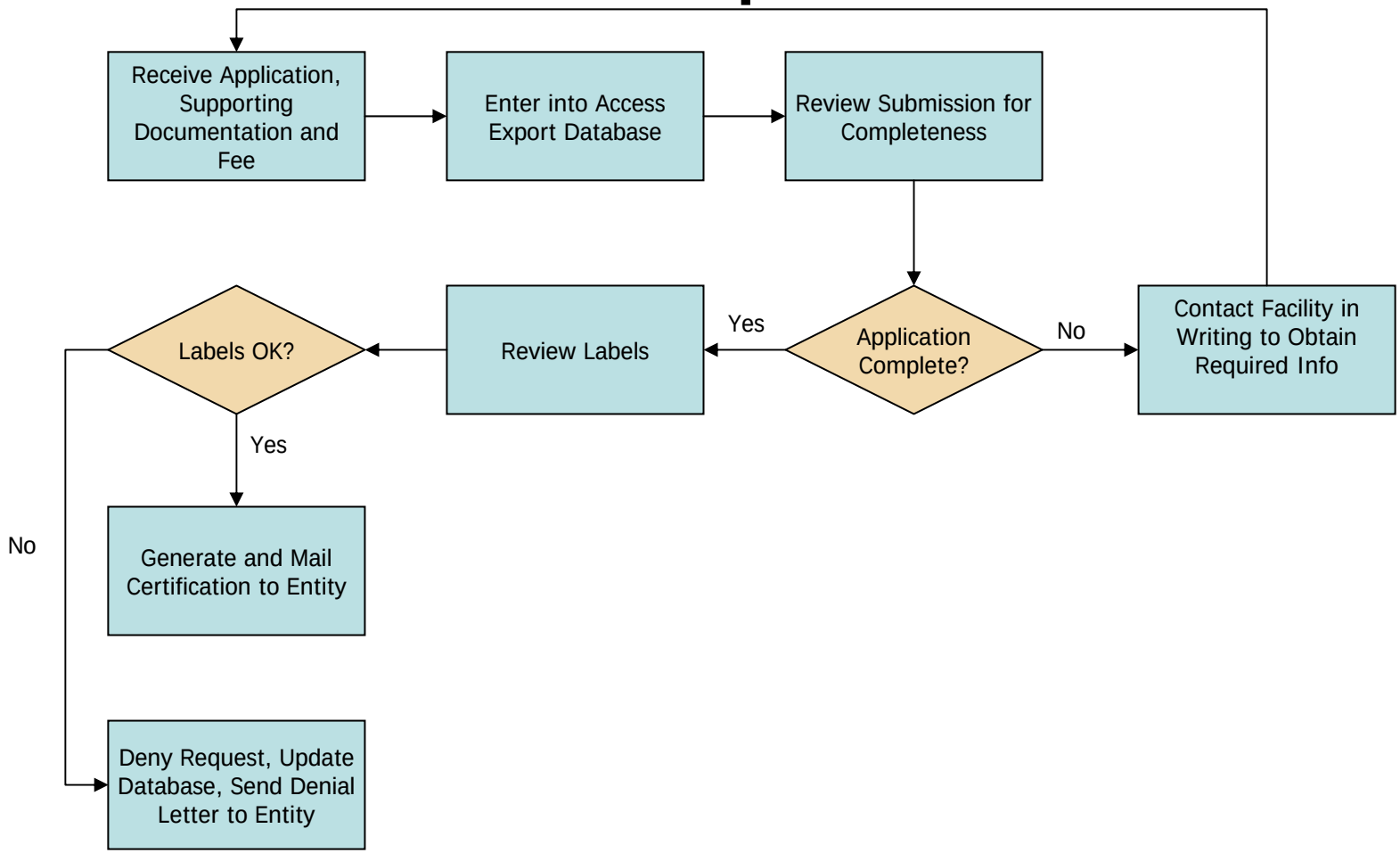
Note: (1) For Drug, Device and HMDR complaint is tasked out by the licensing desk to the Supervising Investigator who assigns it to an investigator for follow-up.

F&D – Process Food Reinspection Fees



NOTES: (1) Billing Fees come from reinspection and civil penalties. New system must interface with Financial System.

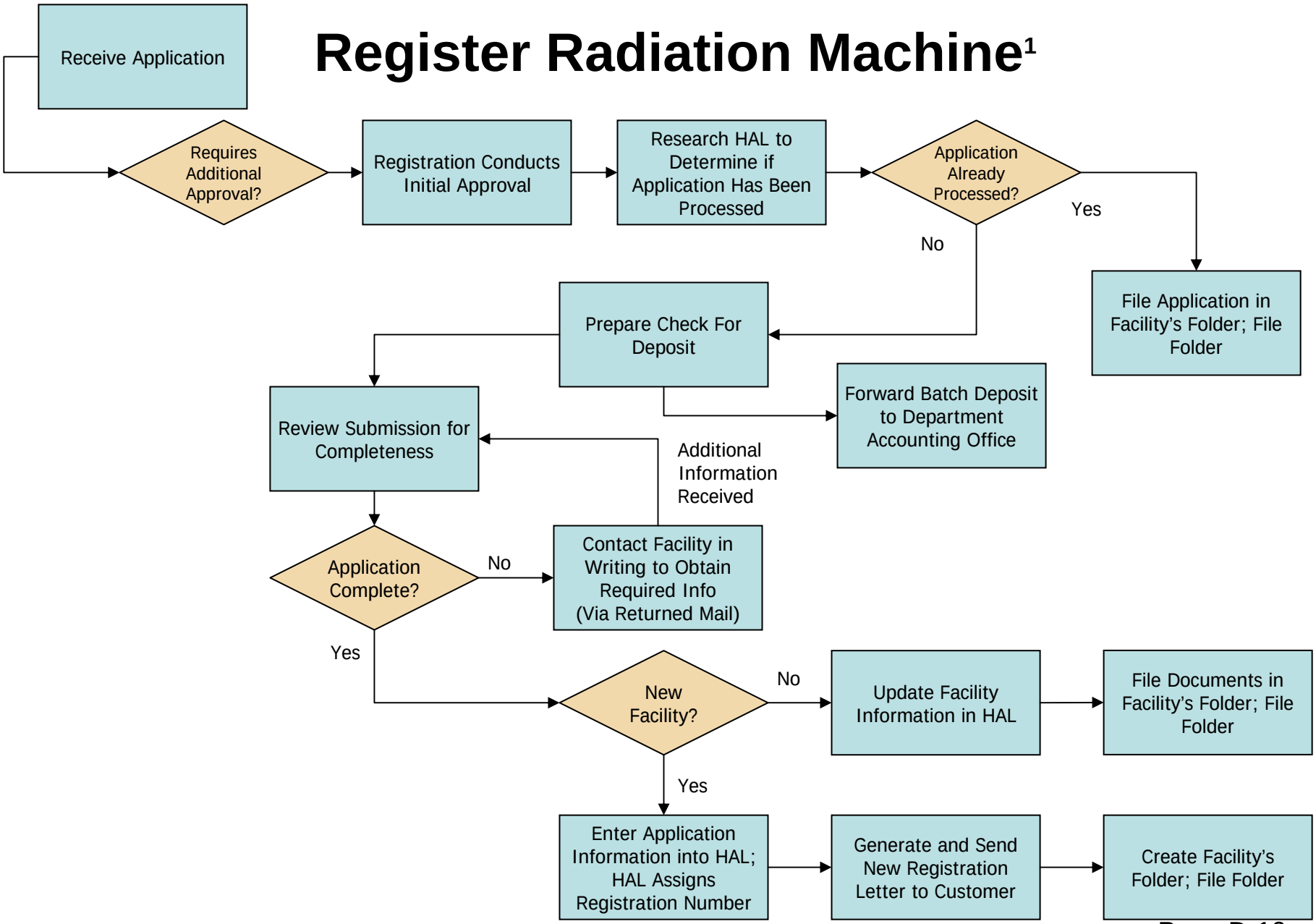
F&D - Certify Food, Drug, Device, Cosmetic for Export



NOTES:

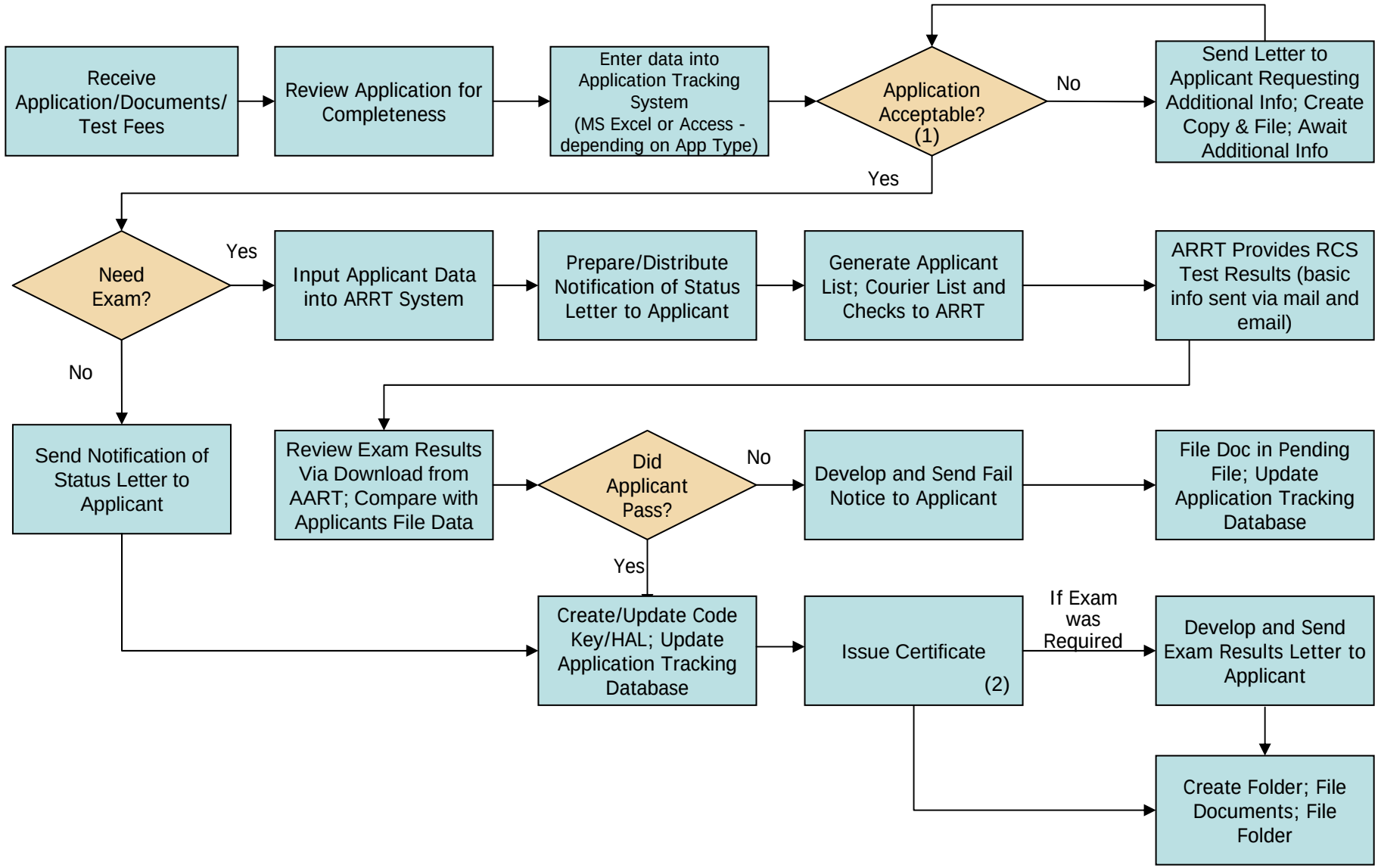
Radiation Safety Program

Register Radiation Machine[1]



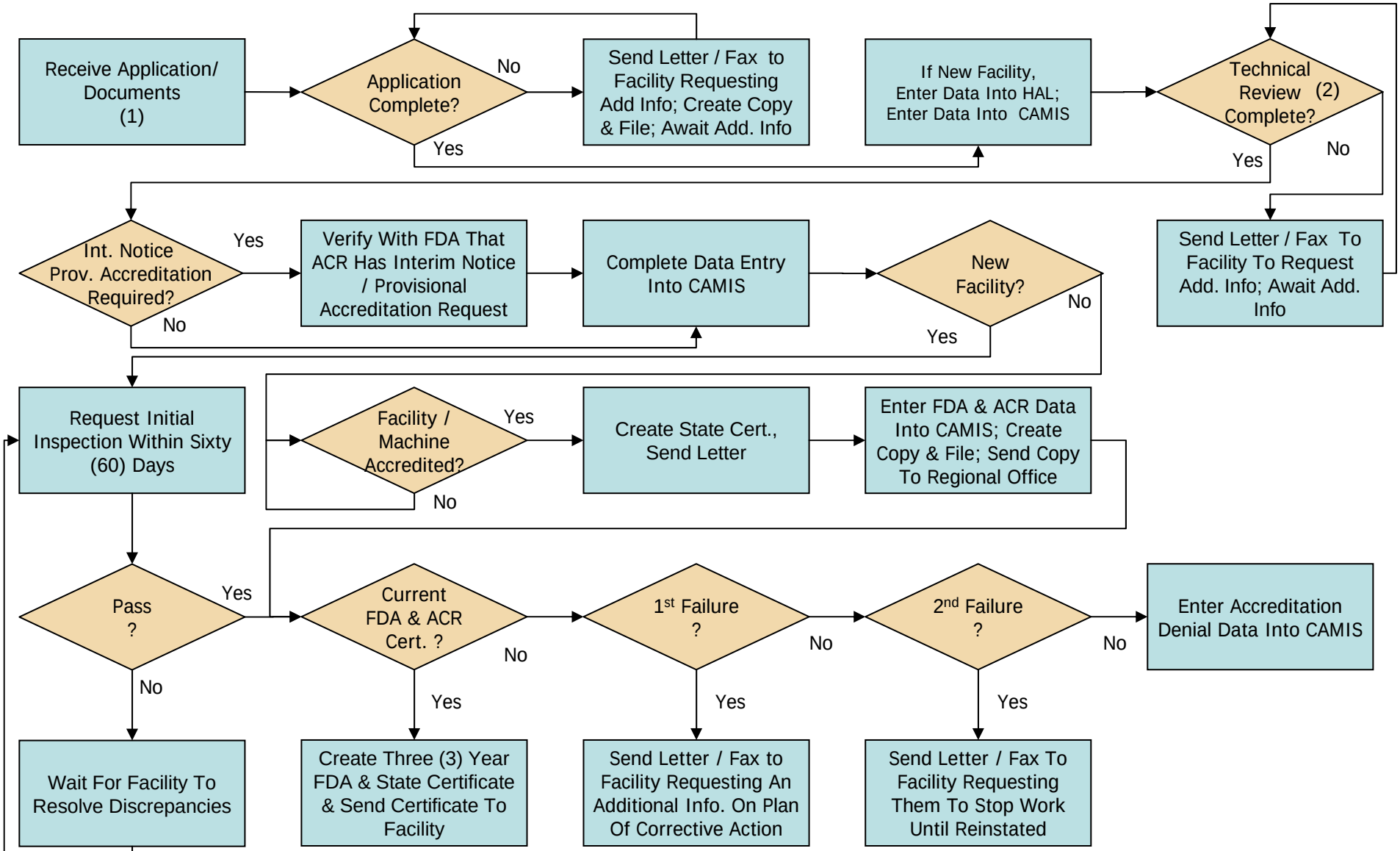
NOTES: (1) Today, applications are received and processed without receipt of application fees (customers are billed separately); in 2007, application fees will be submitted with the application- slightly modifying this process

Certify Radiation Machine Operators



NOTES: (1) Includes reviewing application package and determining if all forms/attachments are submitted, completed correctly.
(2) Using the Code Key data, HAL generates certificates
(3) Certification for Bone Densitometry Registration follows the same process steps but certificates are manually generated.

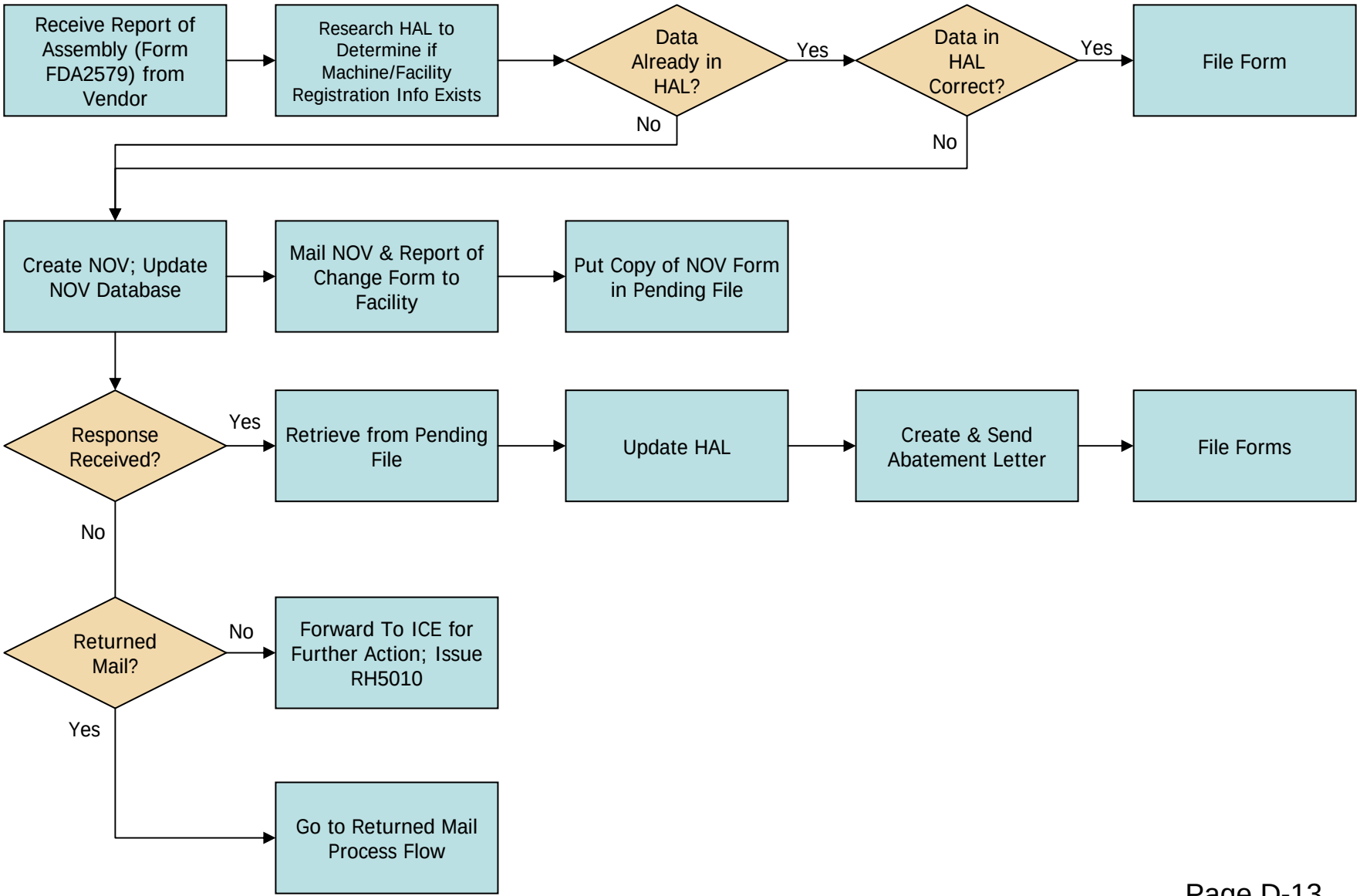
Accredit Mammography Facilities



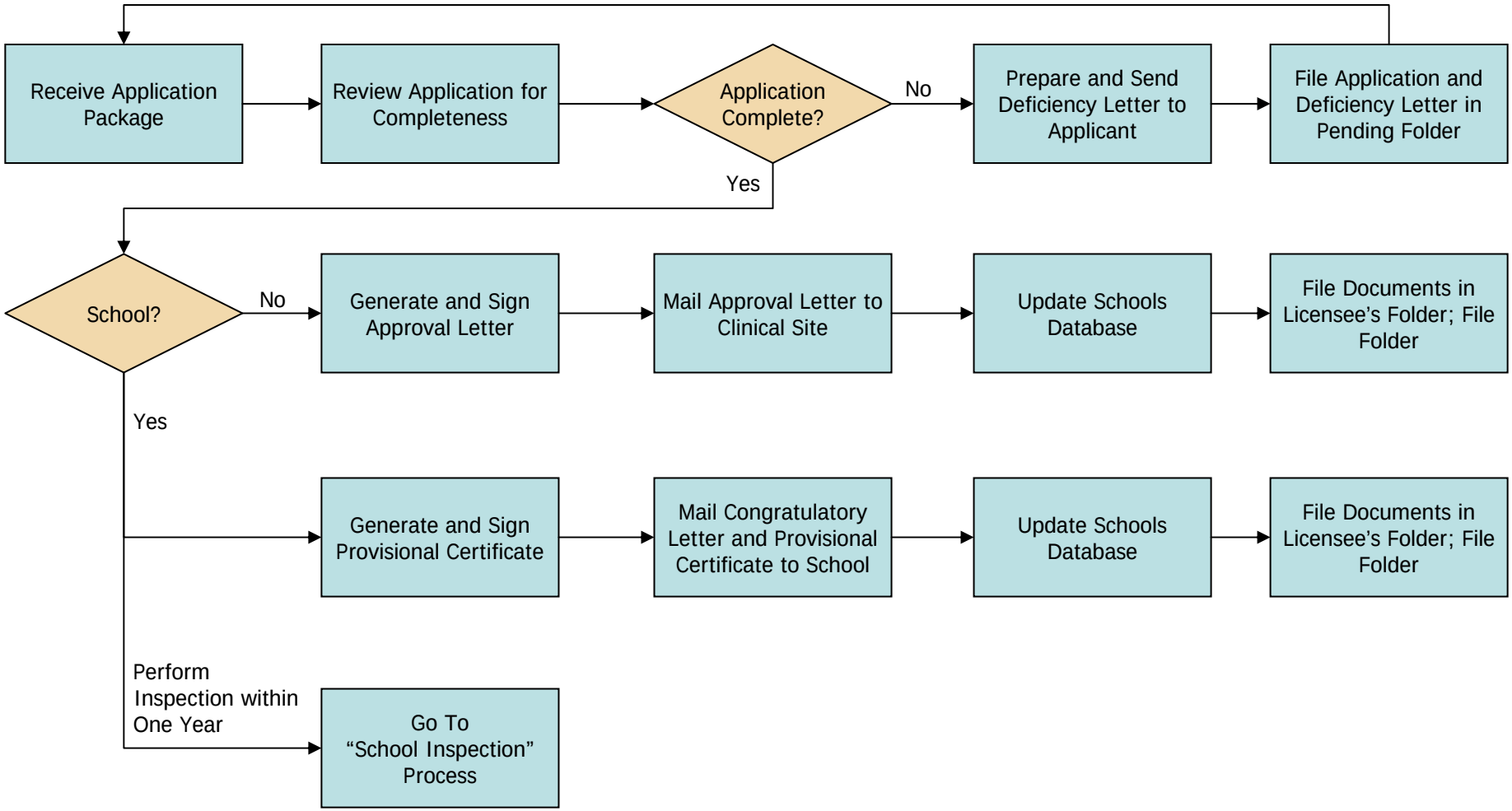
NOTES: (1) Applications can be new or renewal certificate requests for a facility or machine or request for personnel changes; this step includes determining if the fees are current in HAL

(2) Includes validation and verification of personnel qualifications; validation of the physics survey and Title 17 requirements

Reconcile Report of Assembly

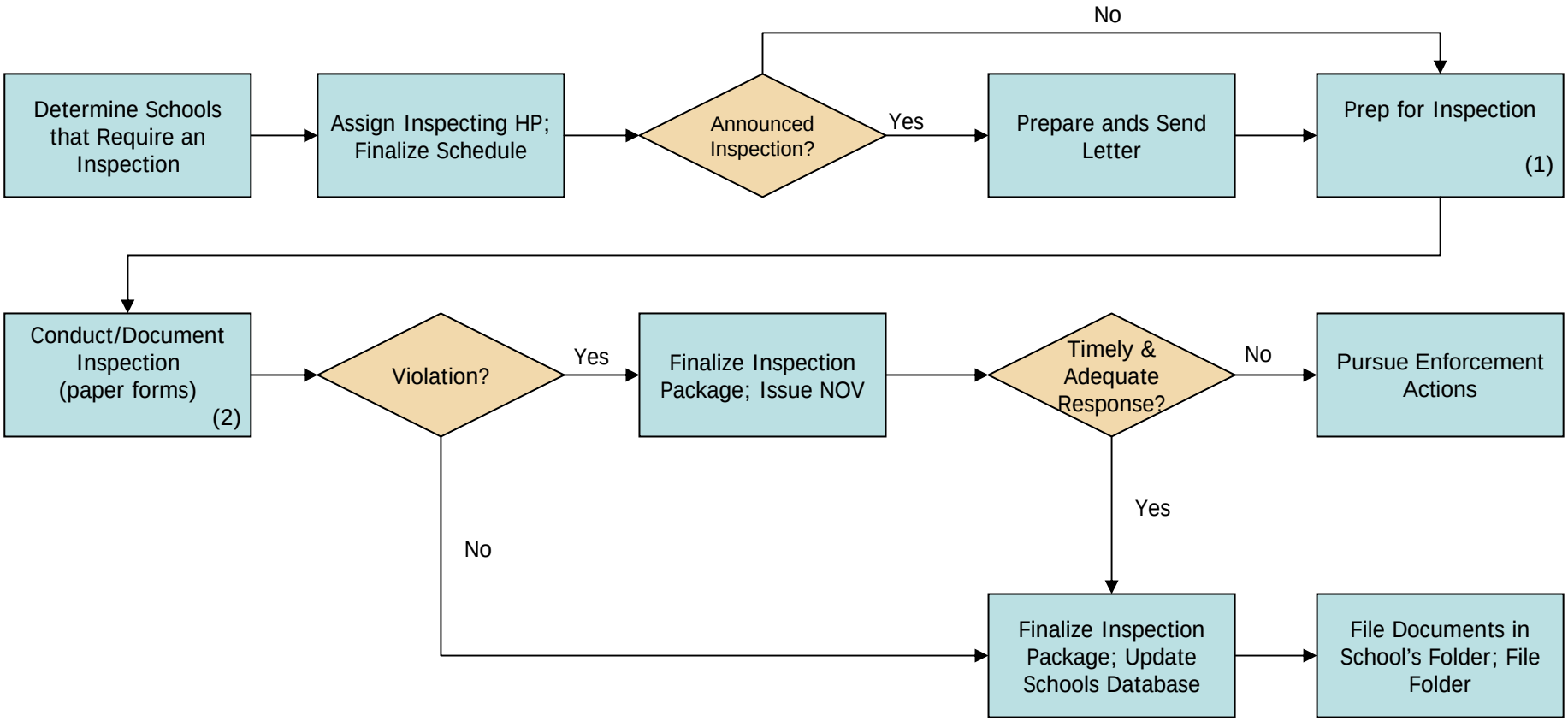


Certify School/Clinical Site



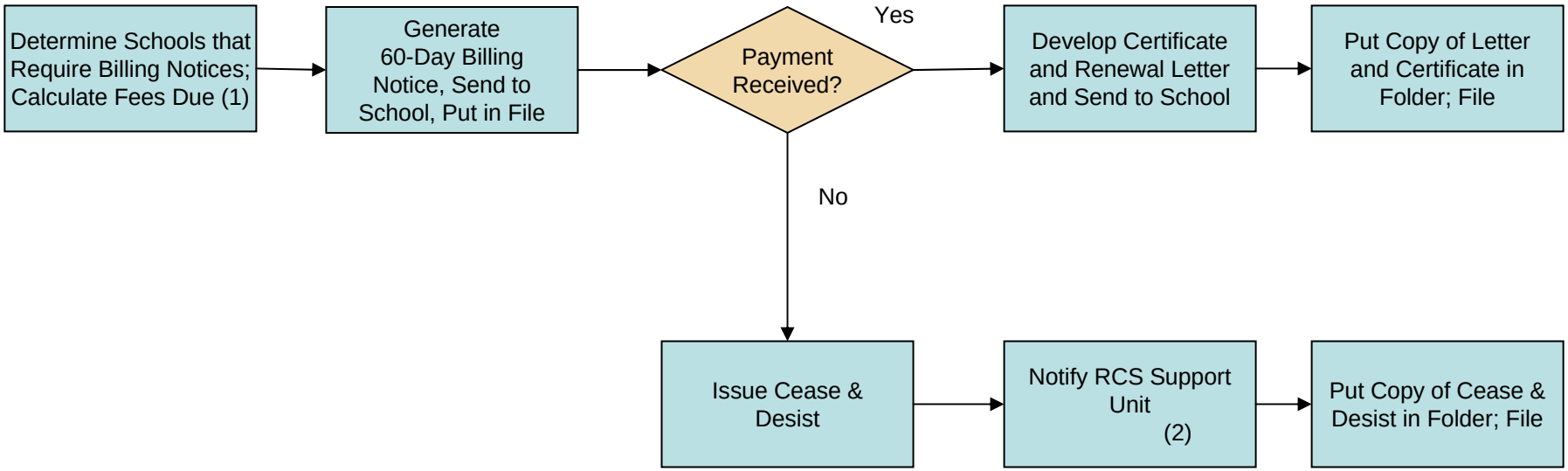
NOTES: (1) Today, applications are received and processed without receipt of application fees (customers are billed separately); in 2007, application fees will be submitted with the application- slightly modifying this process

Perform Radiologic Technology School Inspection



NOTES: (1) Includes scheduling appt, obtaining/reviewing file, making travel arrangements, obtaining info from Schools database, contacting ICE, etc.
(2) Includes touring school, inspecting teaching materials, inspecting lab, evaluating classes, etc.

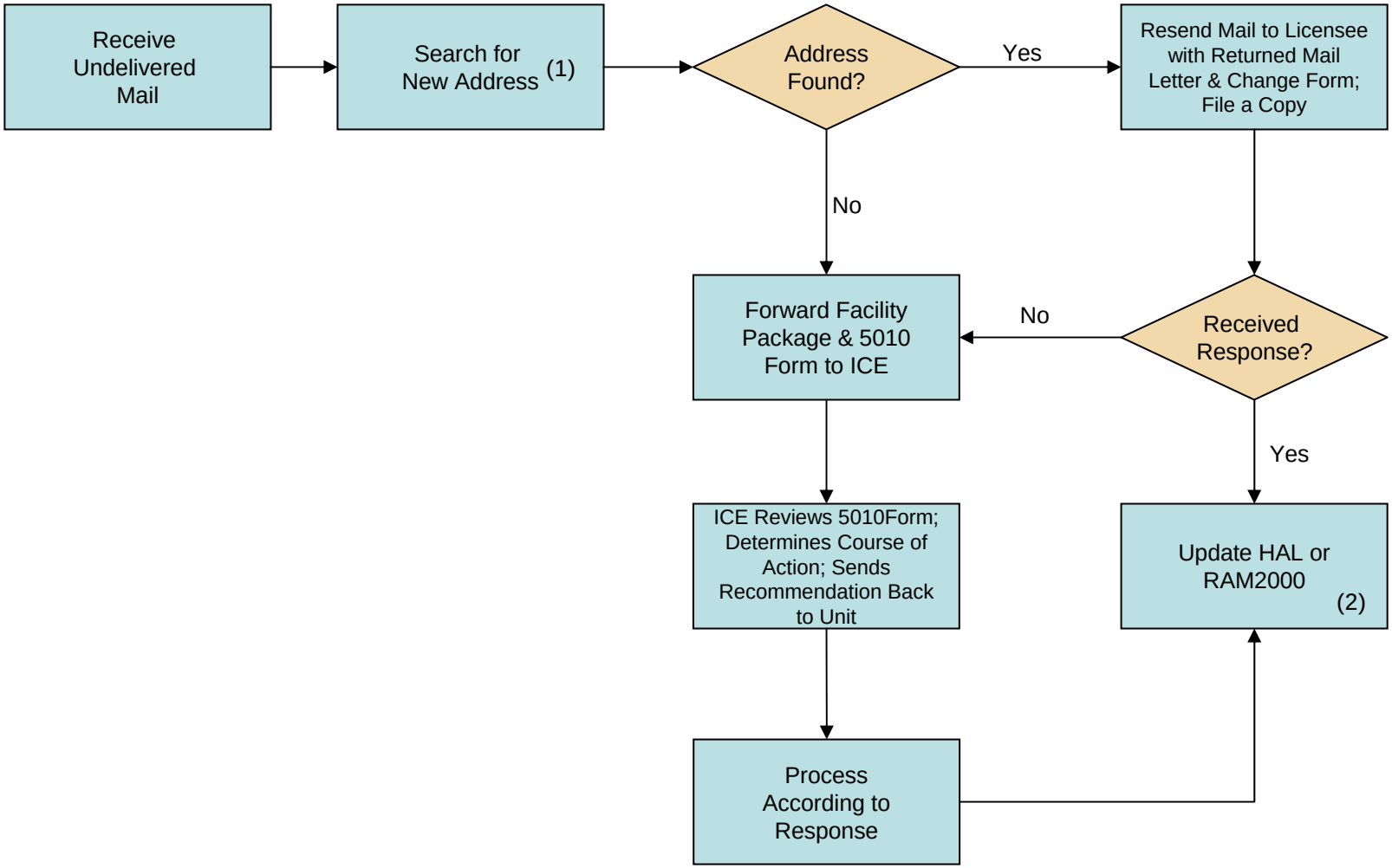
Issue School Billing Notices



NOTES: (1) Activities include identifying clinical sites associated with a school, applying standard fees per school/per clinical site, and determining total fees due

(2) Performed so that RCS Support Unit does not accept applicants who have been licensed by the school since the school is not in good standing

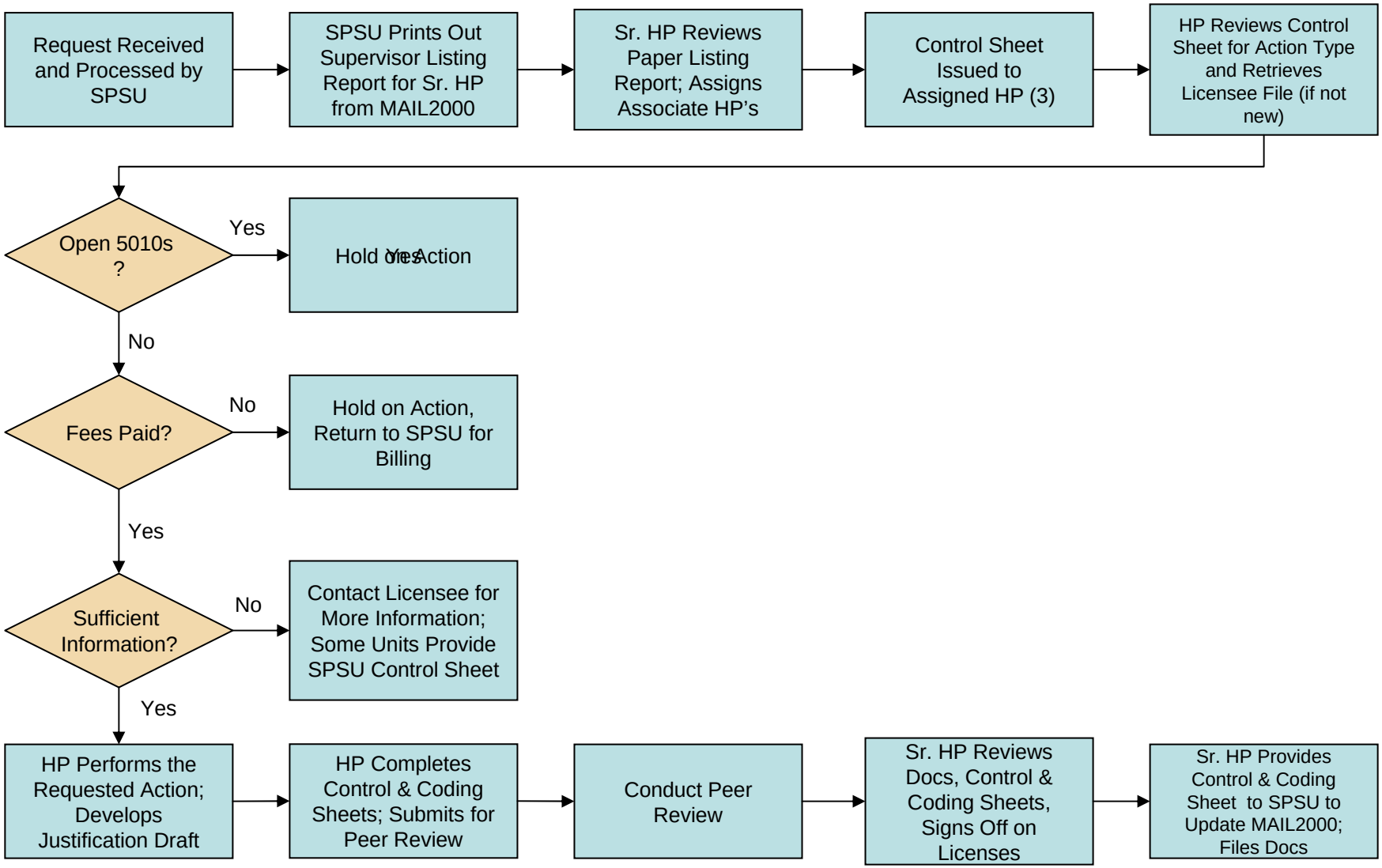
Process Returned Mail



NOTES: (1) May include: reviewing data in HAL to contact facility and request new address; contact directory assistance; etc.

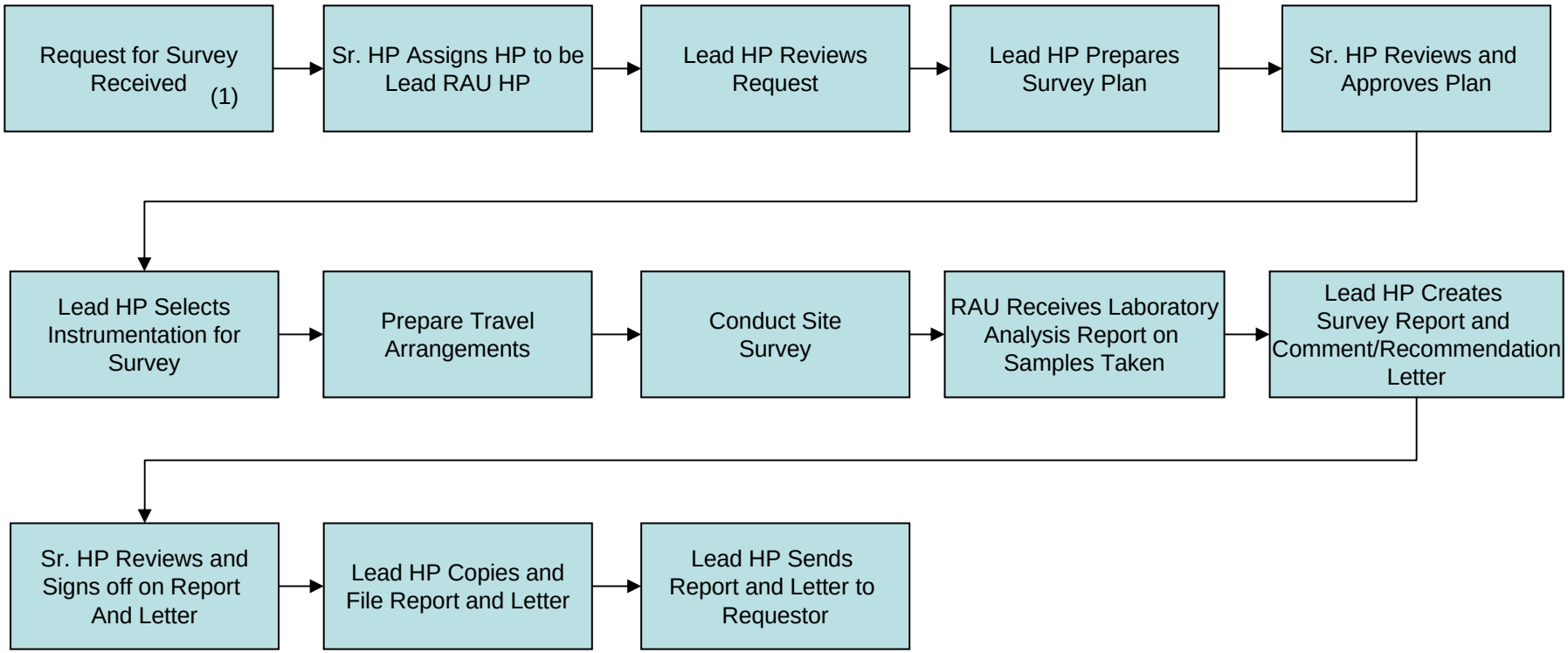
(2) Recommended course of actions may include inactivating a facility, updating HAL or RAM2000 with information obtained by ICE, etc.

Perform Radioactive Materials Licensing Action (1) (2)



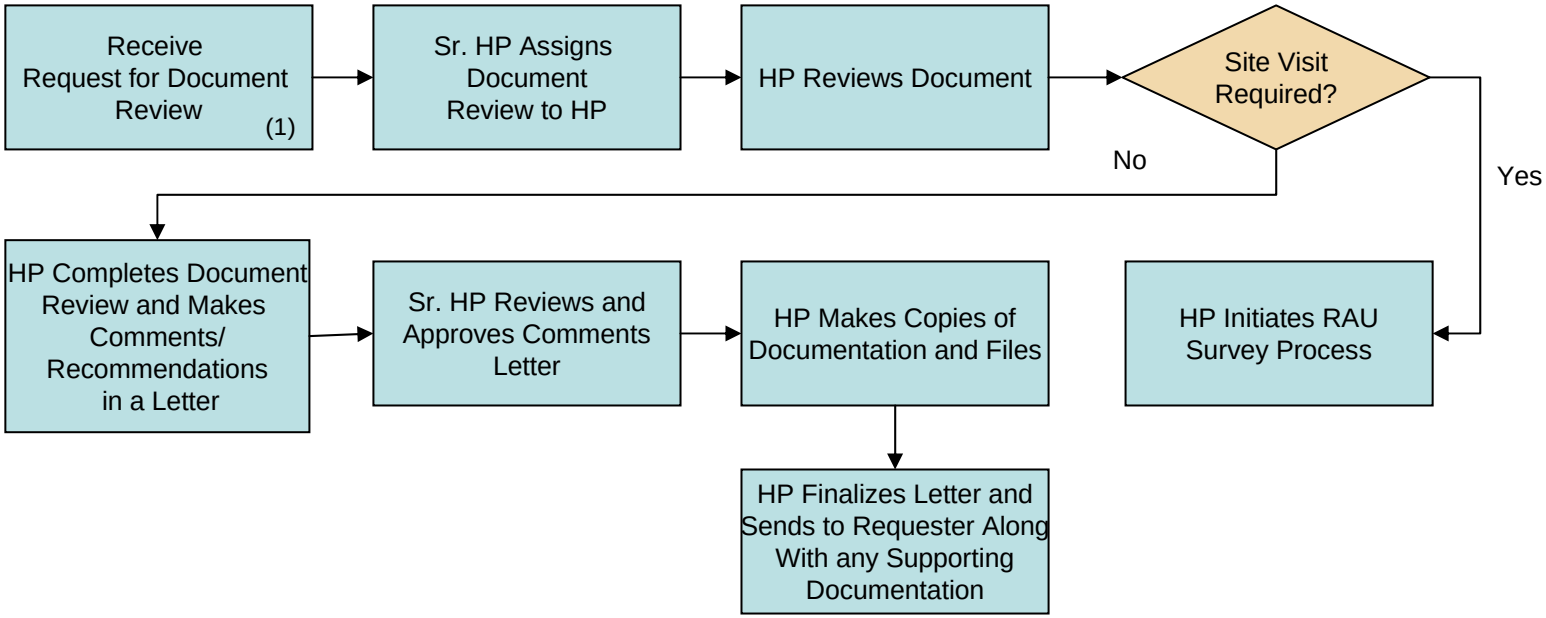
NOTES: (1) Action types may include: Termination, decommission, amendment, follow-up for an existing action, new application
(2) Process varies among RML Units; flow represents the most common worksteps
(3) Some Sr. HPs assign their staff via MAIL2000 and skip this step; some Sr. HPs provide the Control Sheets to SPSU for assignment in MAIL 2000

Perform Radiological Survey



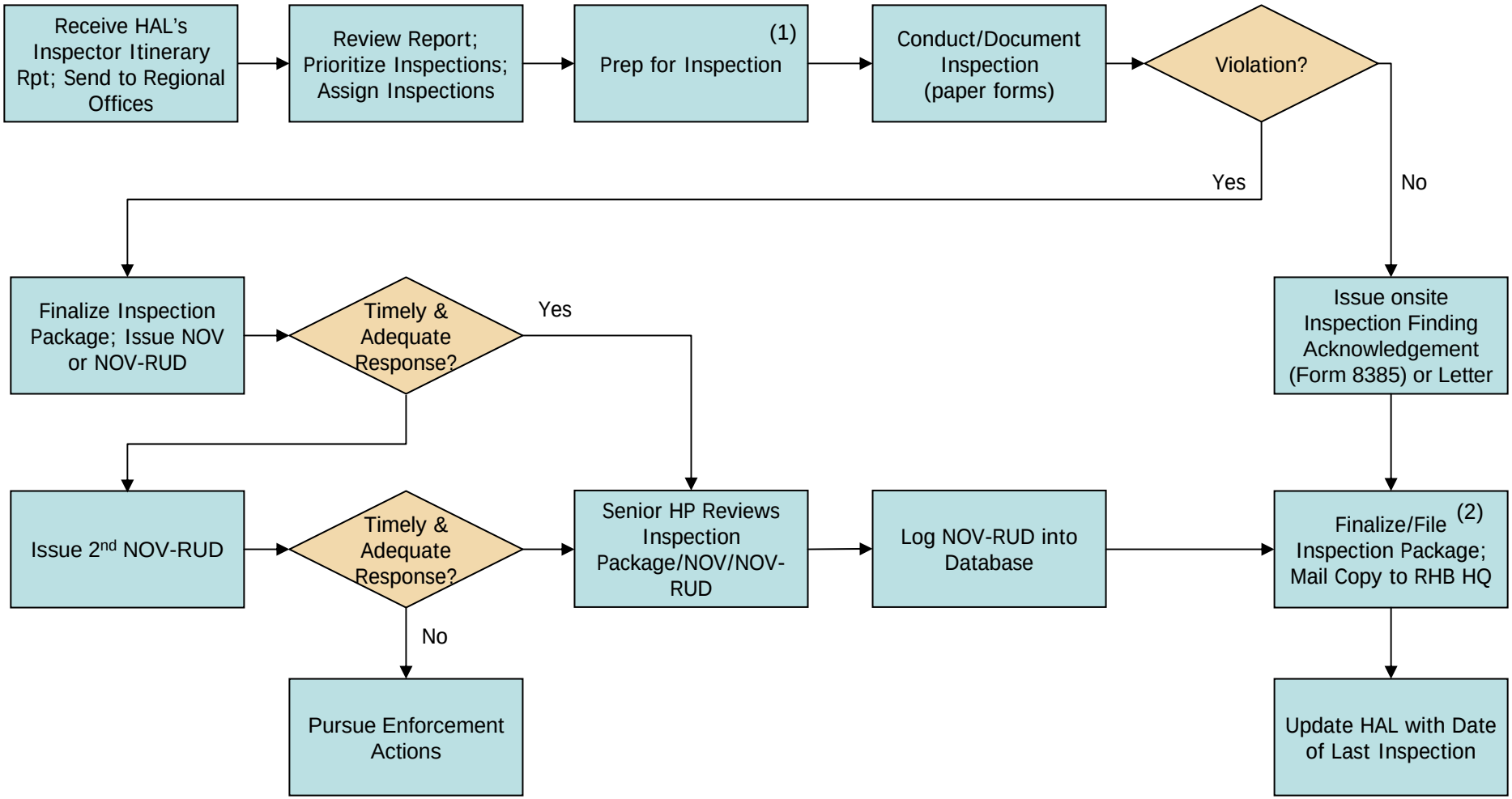
NOTES: (1) Request for Survey may come from any of the following: RML, ICE, State RML licensed facilities, Federally licensed facilities within the state Public Inquiry including individuals, DHS branch other than RHB, local and state governments

Perform Radiological Document Review



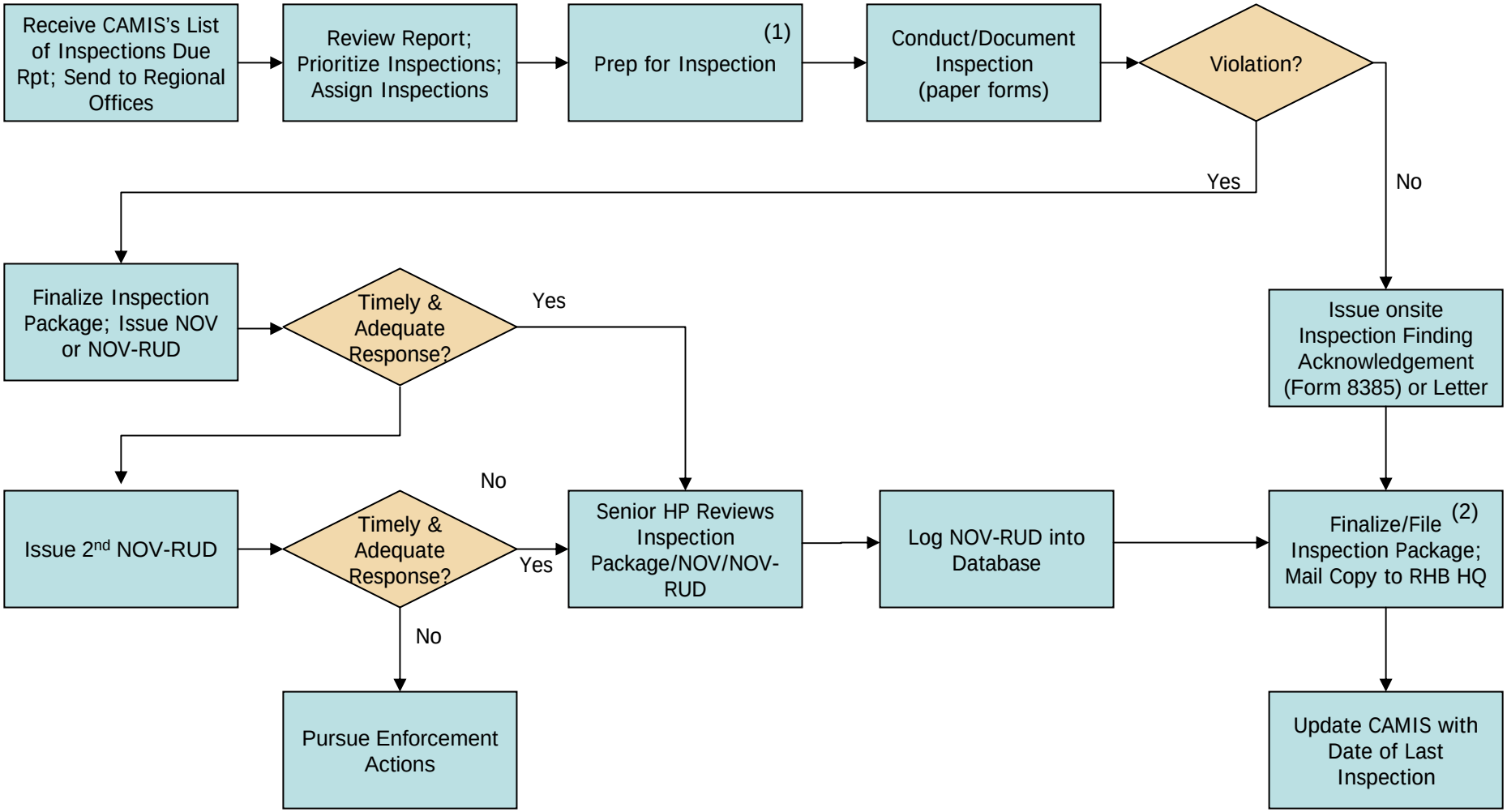
NOTES: (1) Request for Review may come from any of the following: RML, ICE, State RML licensed facilities, Federally licensed facilities within the state Public Inquiry, DHS branch other than RHB

Perform Radiation Machine Inspection



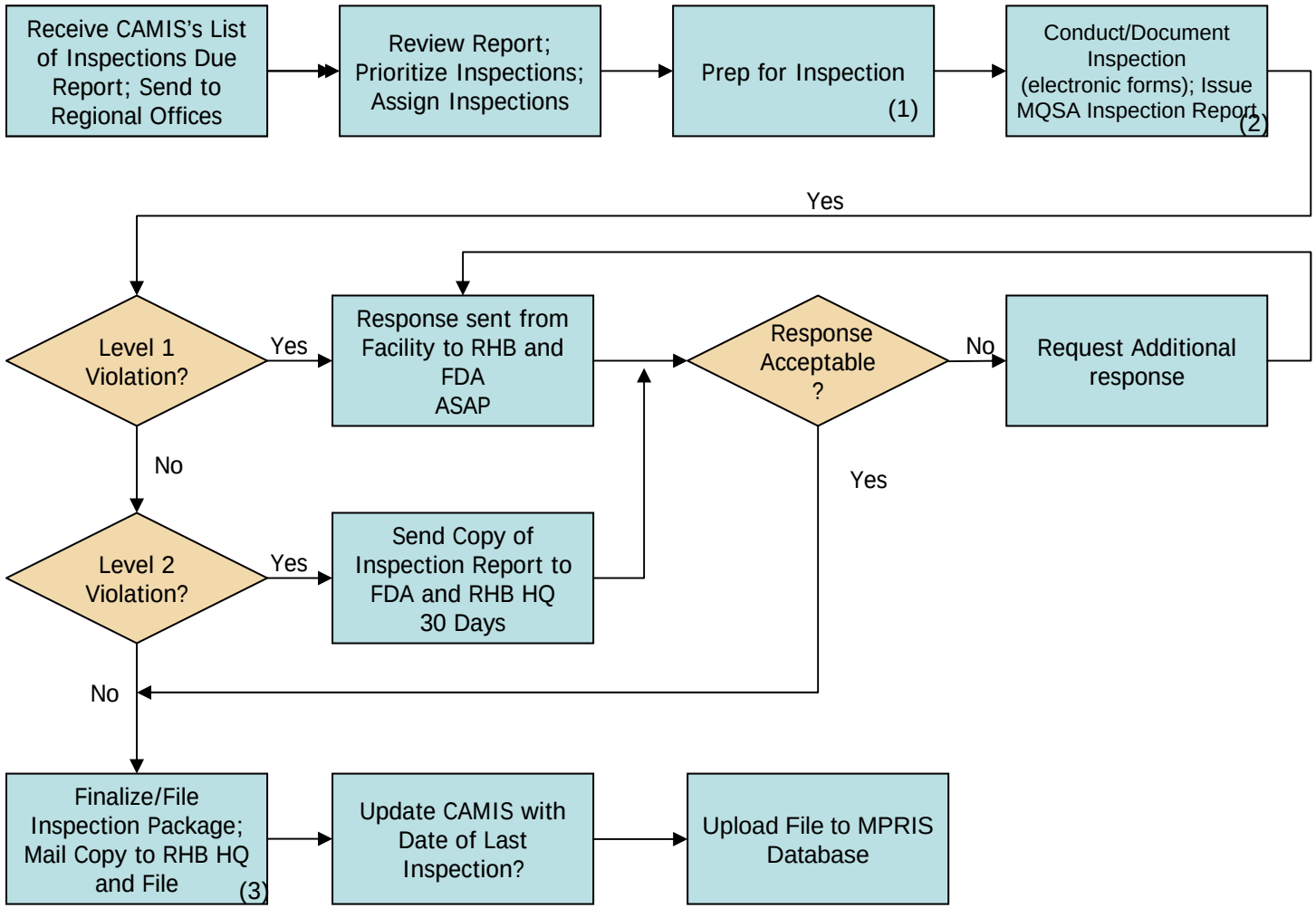
NOTES: (1) Includes scheduling appt, obtaining/reviewing file, making travel arrangements, obtaining info from RCMS, etc. (2) Includes Sr. HP review/approval

Perform Mammography Machine Inspection (State)



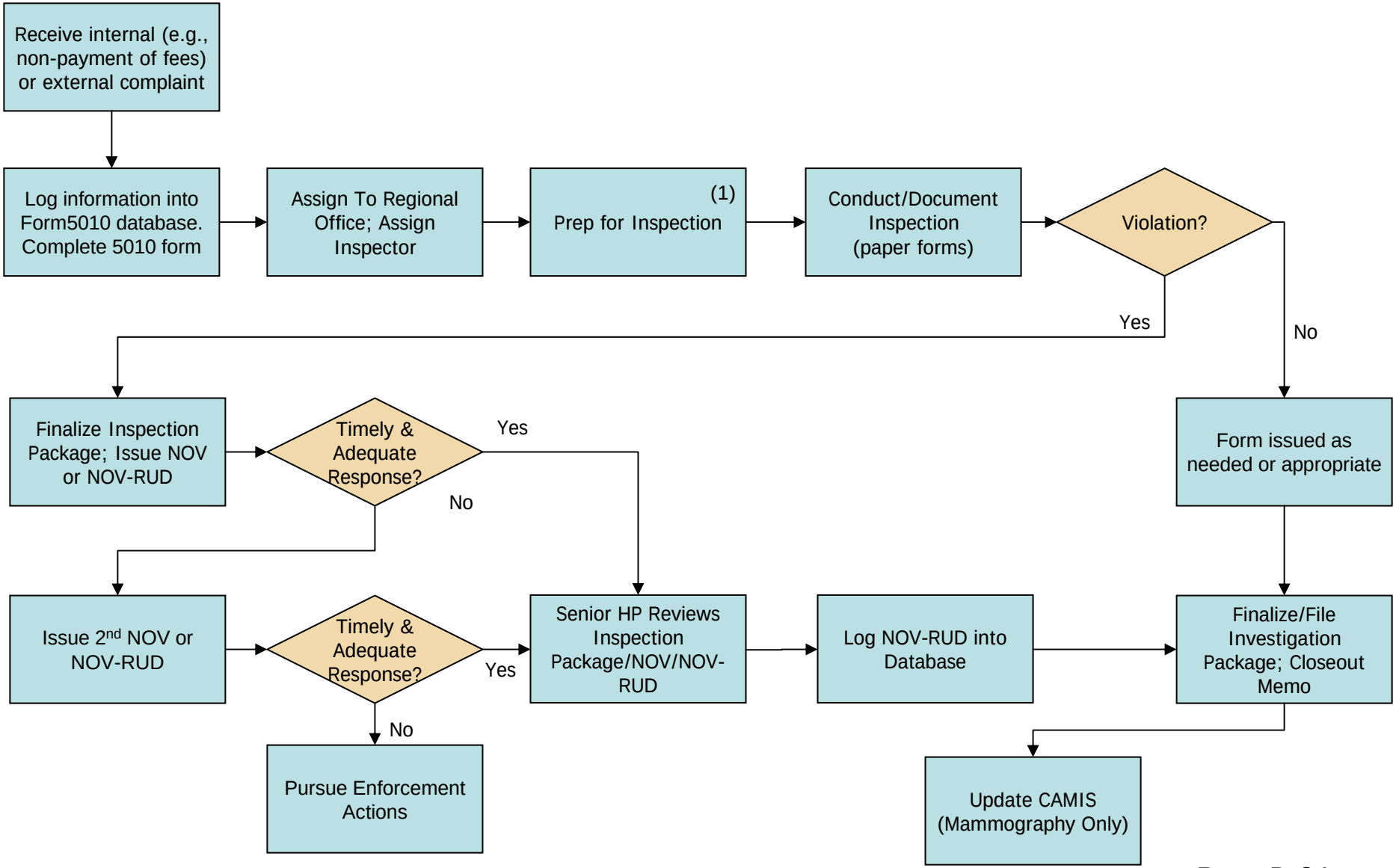
NOTES: (1) Includes scheduling appt, obtaining/reviewing file, making travel arrangements, obtaining info from RCMS, etc.
(2) Includes Sr. HP review/approval

Perform Mammography Machine Inspection (MQSA)



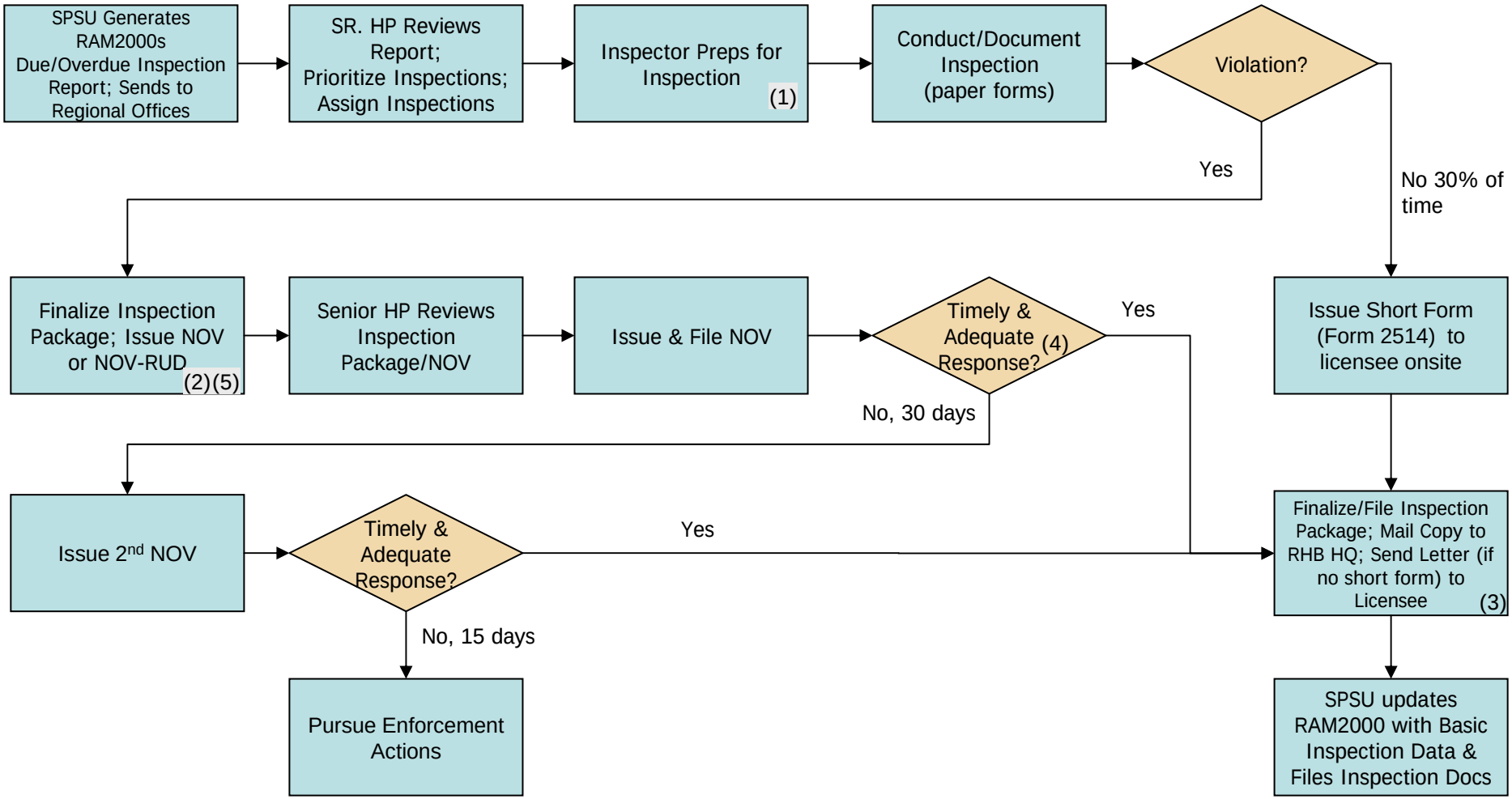
NOTES: (1) Includes scheduling appt, obtaining/reviewing file, making travel arrangements, obtaining info from FDA database, etc. (2) Sometimes the only finding is lack of required documentation provided by Registrar at time of inspection; Licensee forwards info to Inspector post-inspection; if not received, violation cited (3) Includes QA Review review/approval

Perform Radiation Machine Investigation



NOTES: (1) Includes scheduling appt, obtaining/reviewing file, making travel arrangements, obtaining info from RCMS, etc.
(2) Includes Sr. HP review/approval

Perform Radioactive Materials Inspection



NOTES: (1) Includes scheduling appt, obtaining/reviewing file, making travel arrangements, obtaining info from RCMS, etc.

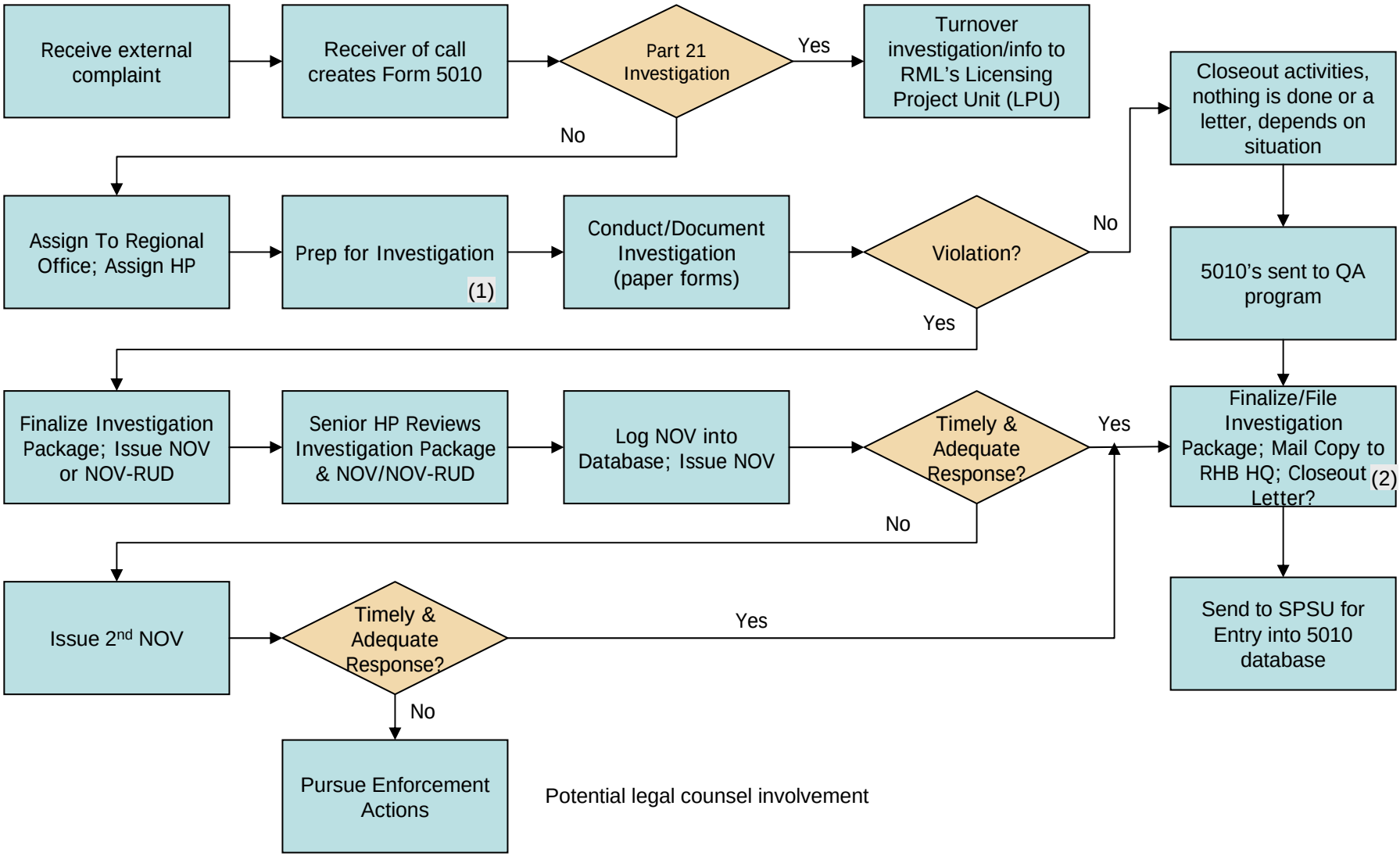
(2) Activities that may be included: contacting the RML or SPSU for info, providing samples to labs for analyses, request more info from licensee, etc.

(3) Includes Sr. HP review/approval and QA/QC Review, if no violation a letter is sent if no form was given onsite

(4) May include need for a licensing action; Inspector will contact RML to pursue

(5) NOV-RUD are issued onsite and are essentially Cease & Desist orders; obtain signature from licensee to comply; await for licensee proof of remedy

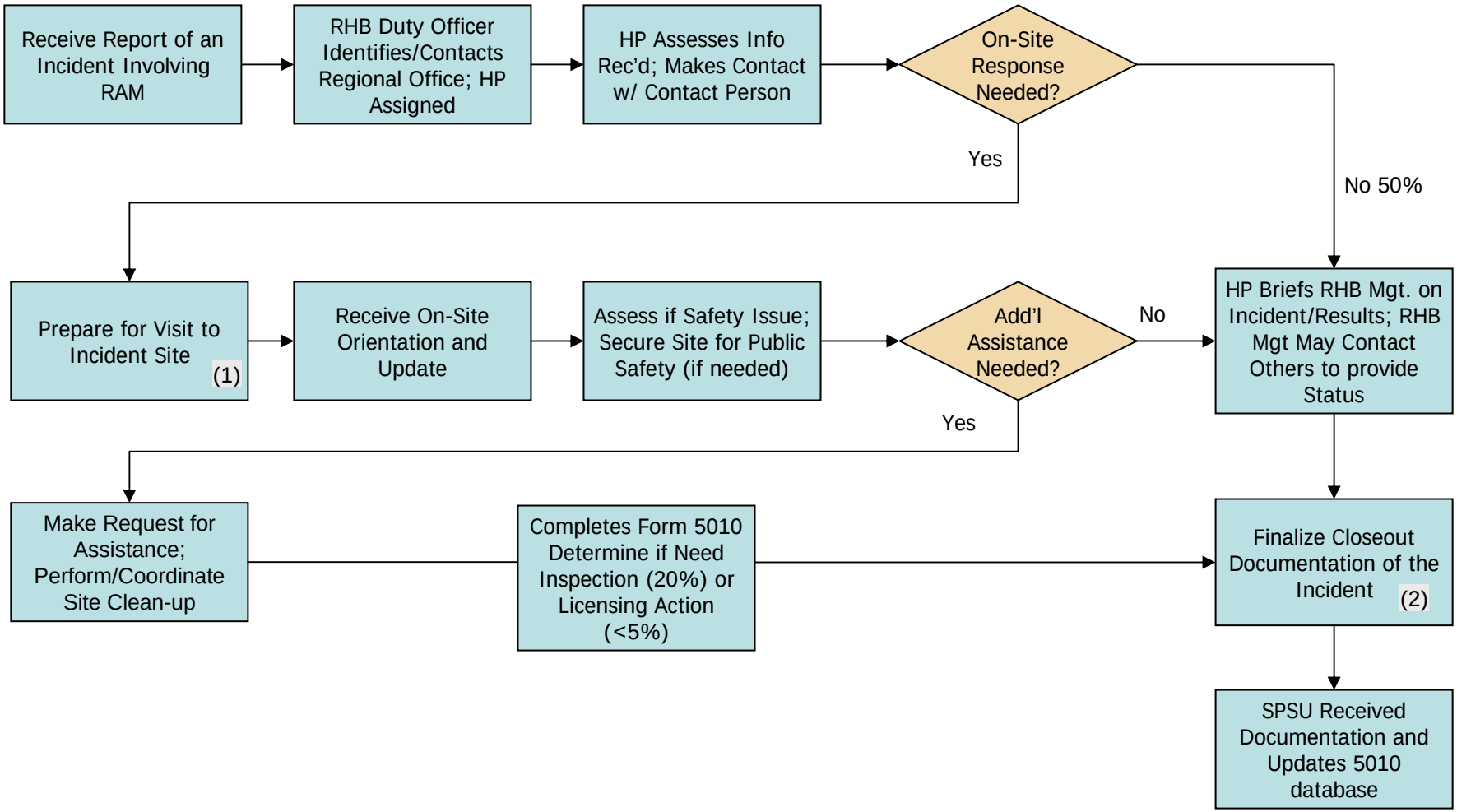
Perform Radioactive Materials Investigation



NOTES: (1) Includes scheduling appt, obtaining/reviewing file, making travel arrangements, obtaining info from RCMS, etc.

(2) Includes Sr. HP review/approval and QA/QC Review

Perform Incident Response

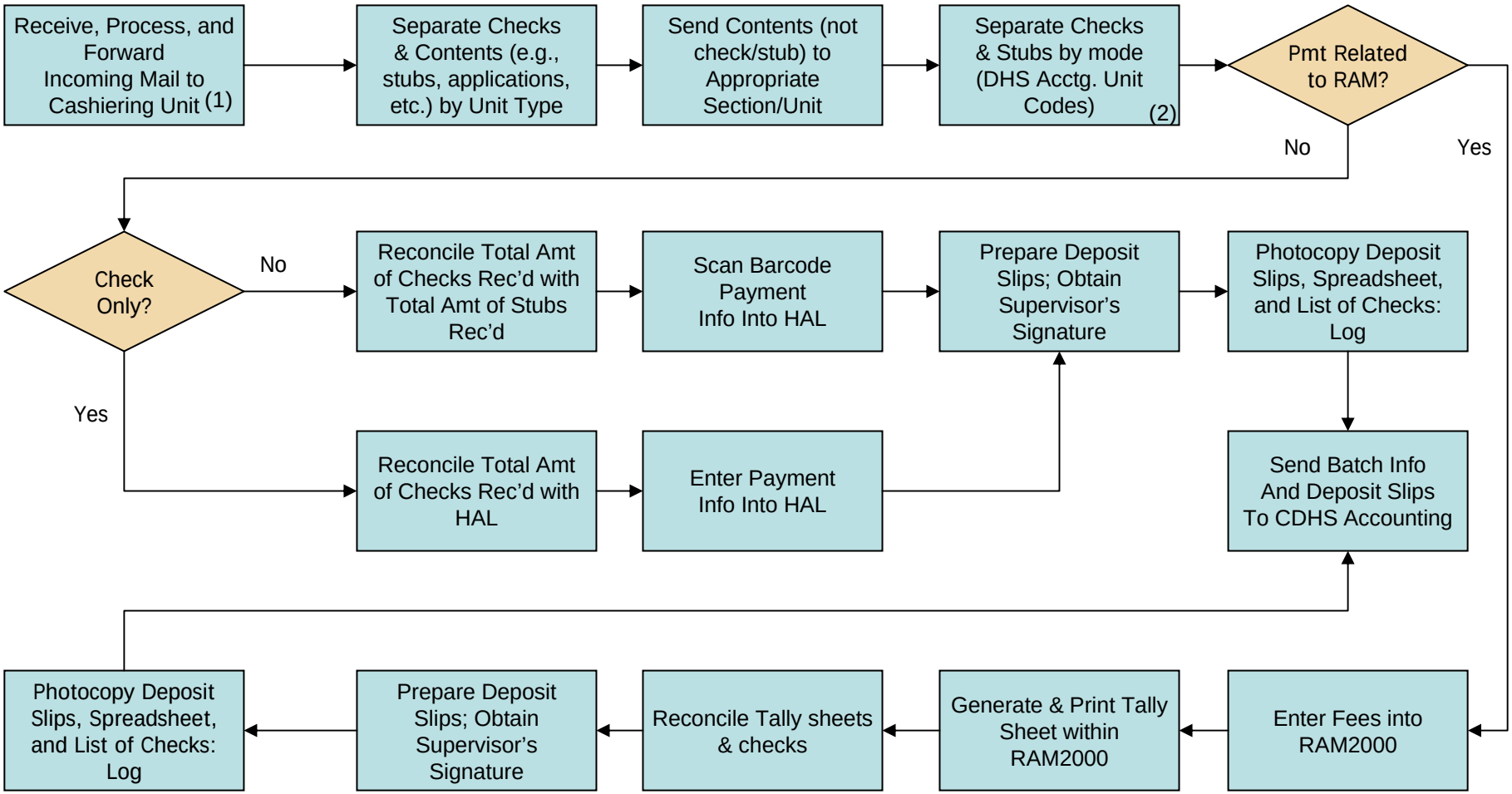


NOTES: (1) Includes determining site location, obtaining equipment, travel to site, contact licensee (if needed), etc.

(2) Activities that may be included: updating/completing Form 5010; developing Investigation Closeout Memo; issuing NOV (if required); contacting NRC (if needed)

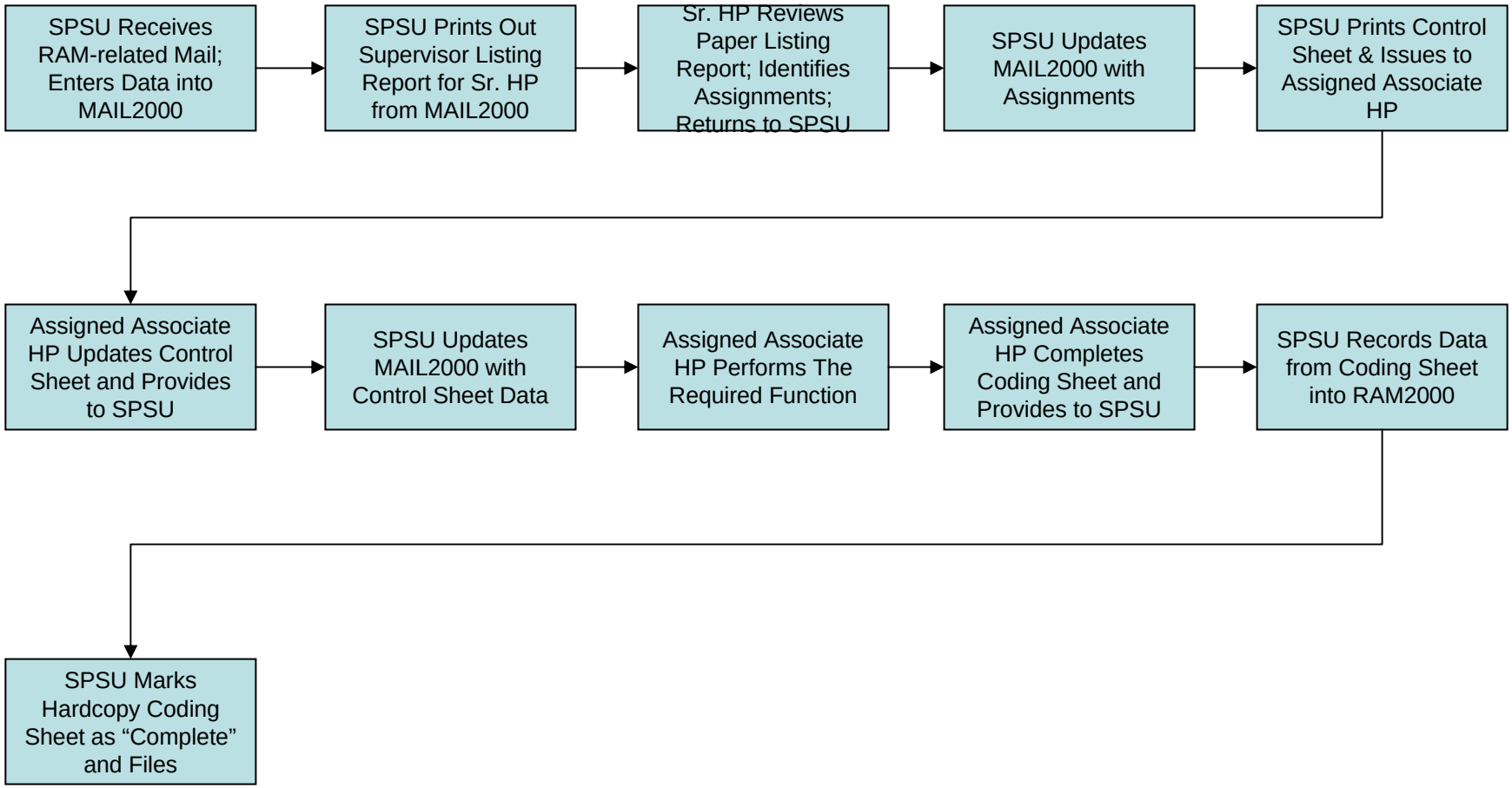
Perform Cashiering

All Tasks Performed by Database Support Unit

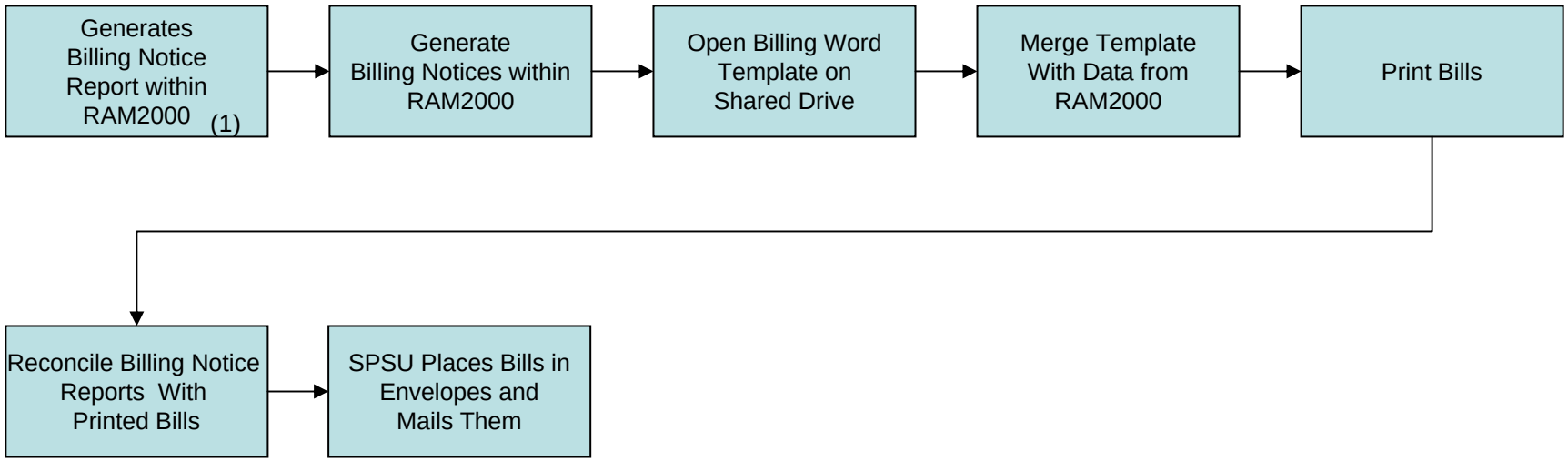


NOTES: (1) Activities including opening, date stamping, and sorting mail; (2) RAM bill payments do not include a stub since generated by RAM2000

Track Radioactive Materials Correspondence



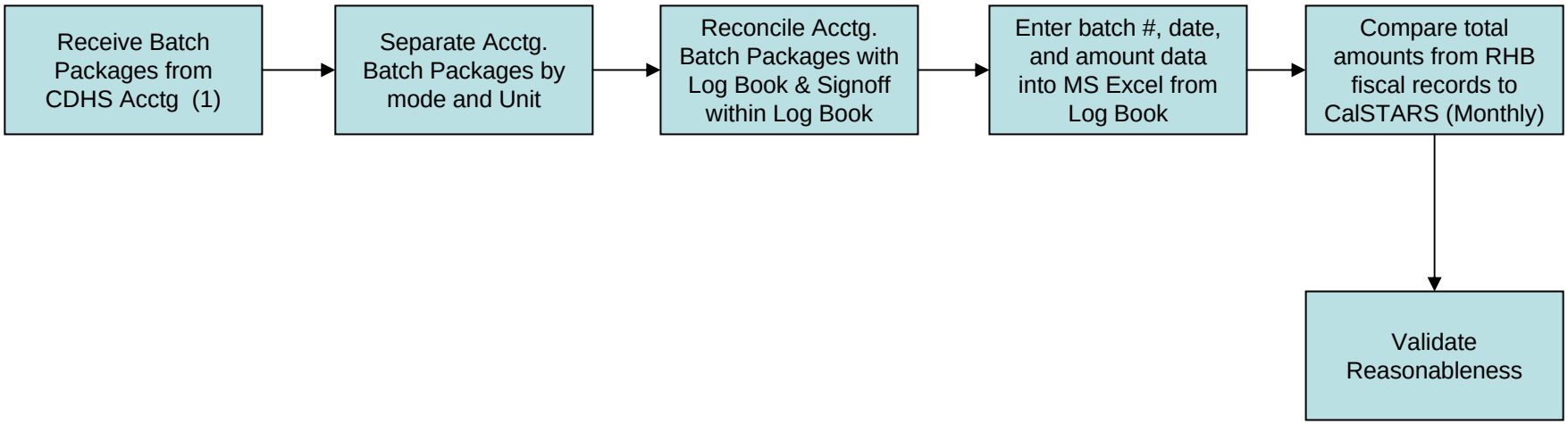
Issue Radioactive Materials Billing Notices



NOTES: (1) First Notices are printed 60 days prior to due date; RAM2000 can also generate 2nd Notices, Overdue Notices, and Final Notices. The Billing Notice content varies, but the process is the same for all types of notices.

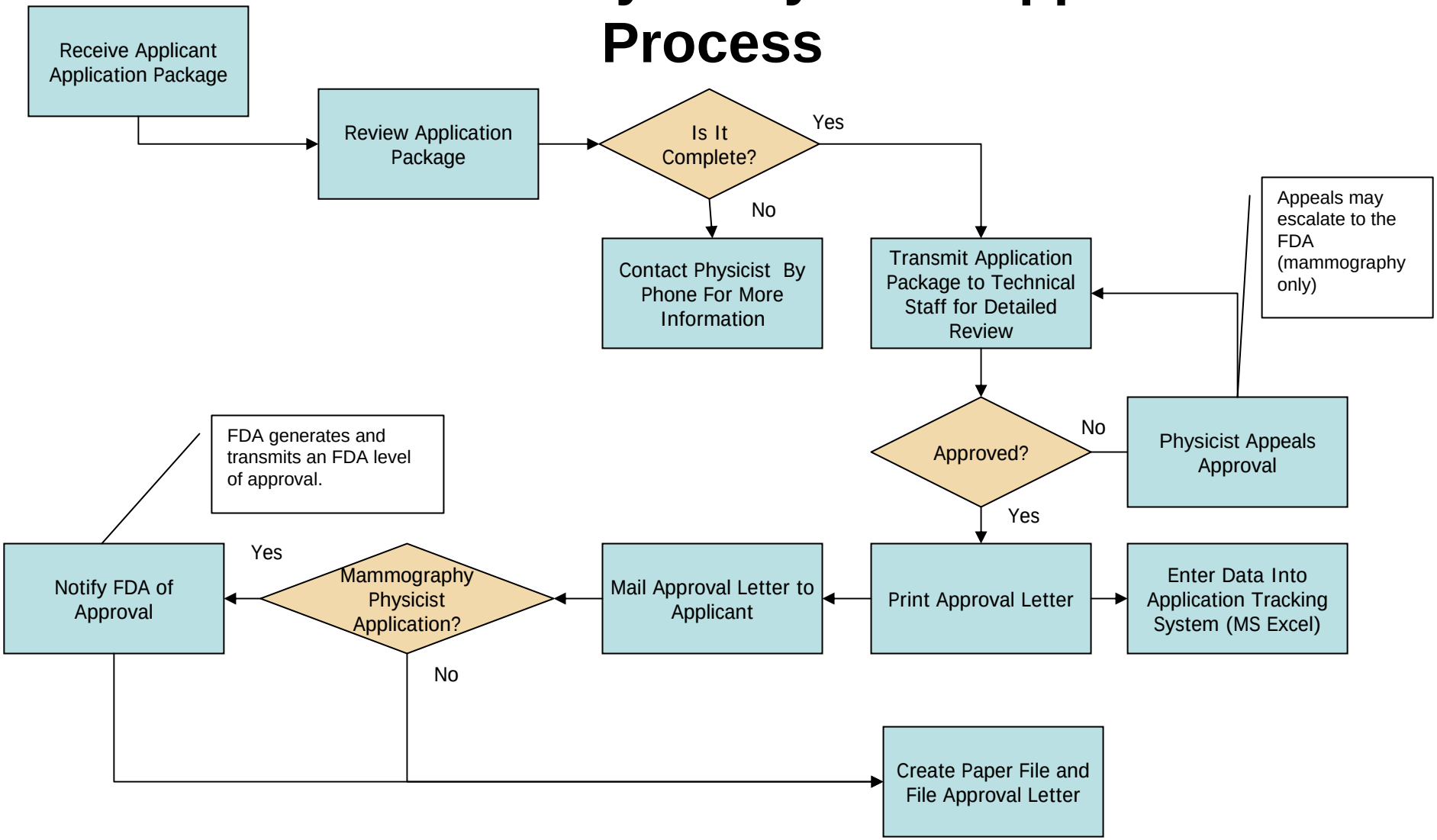
NOTE: Bills for radiation machines and individuals licensed to operate these machines are automatically generated by ITSD using HAL based on licensee expiration date; RHB is not actively involved in the process of issuing billing notices for Radiation Machines.

Reconcile Deposits



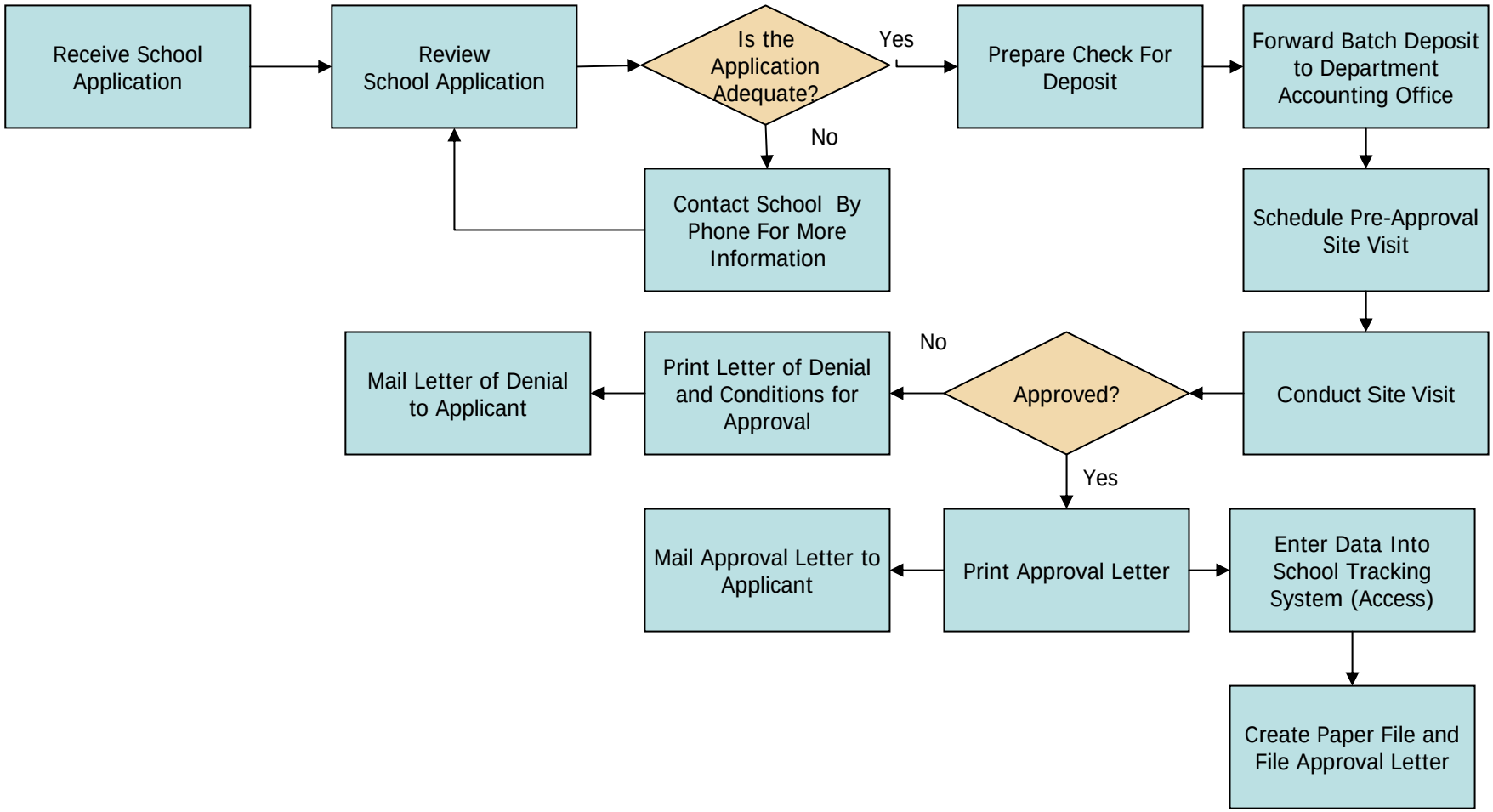
NOTES: (1) Include official bank deposit slip, RHB deposit slip, and tally sheet

Radiation Safety – Physicist Approval Process



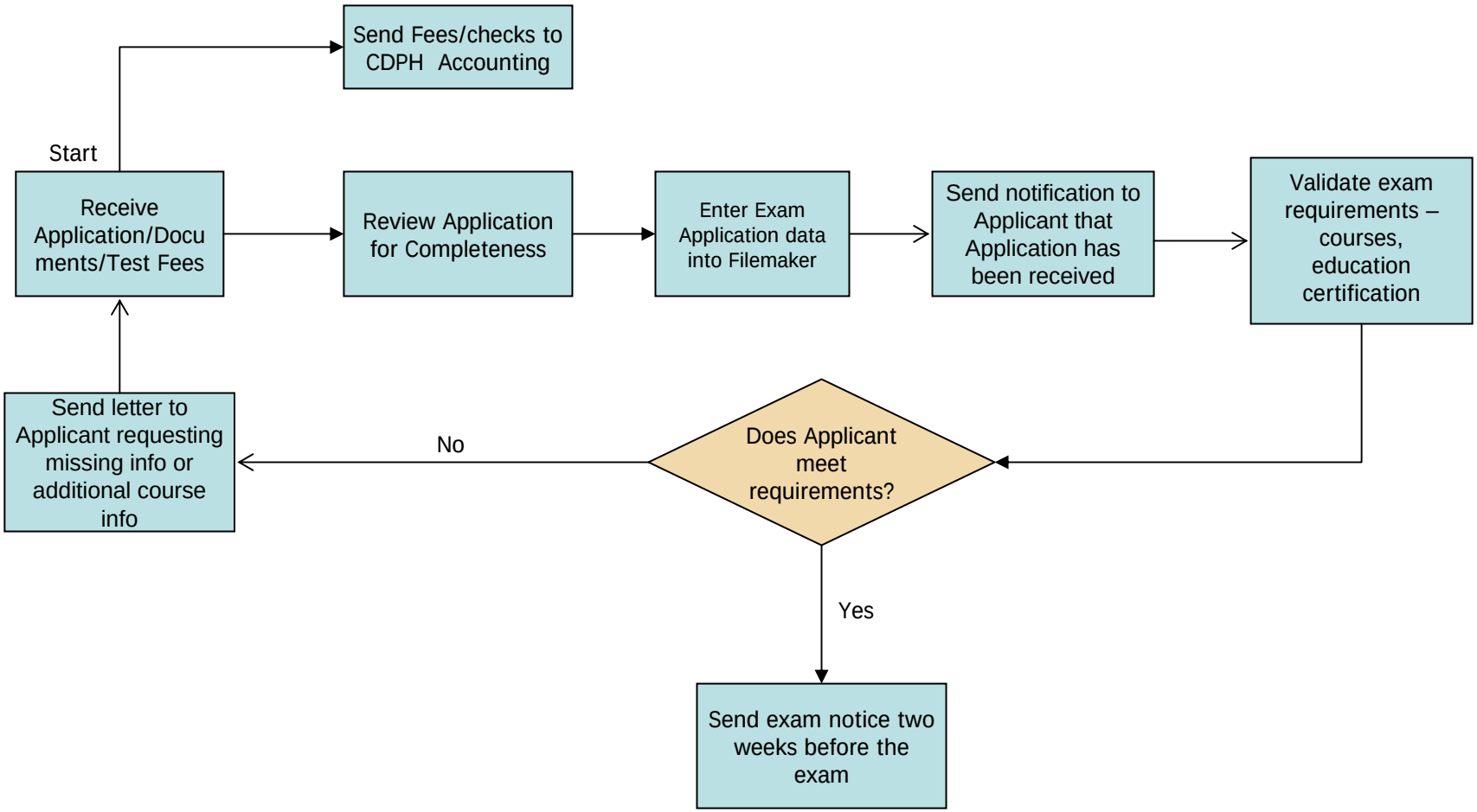
Approval process applies to both Mammography Physicist and Therapy Physicists – application requirements vary; mammography physicists renew approval after three years; therapy physicists have no renewal requirements.

Radiation Safety – Radiologic Technician School Approval

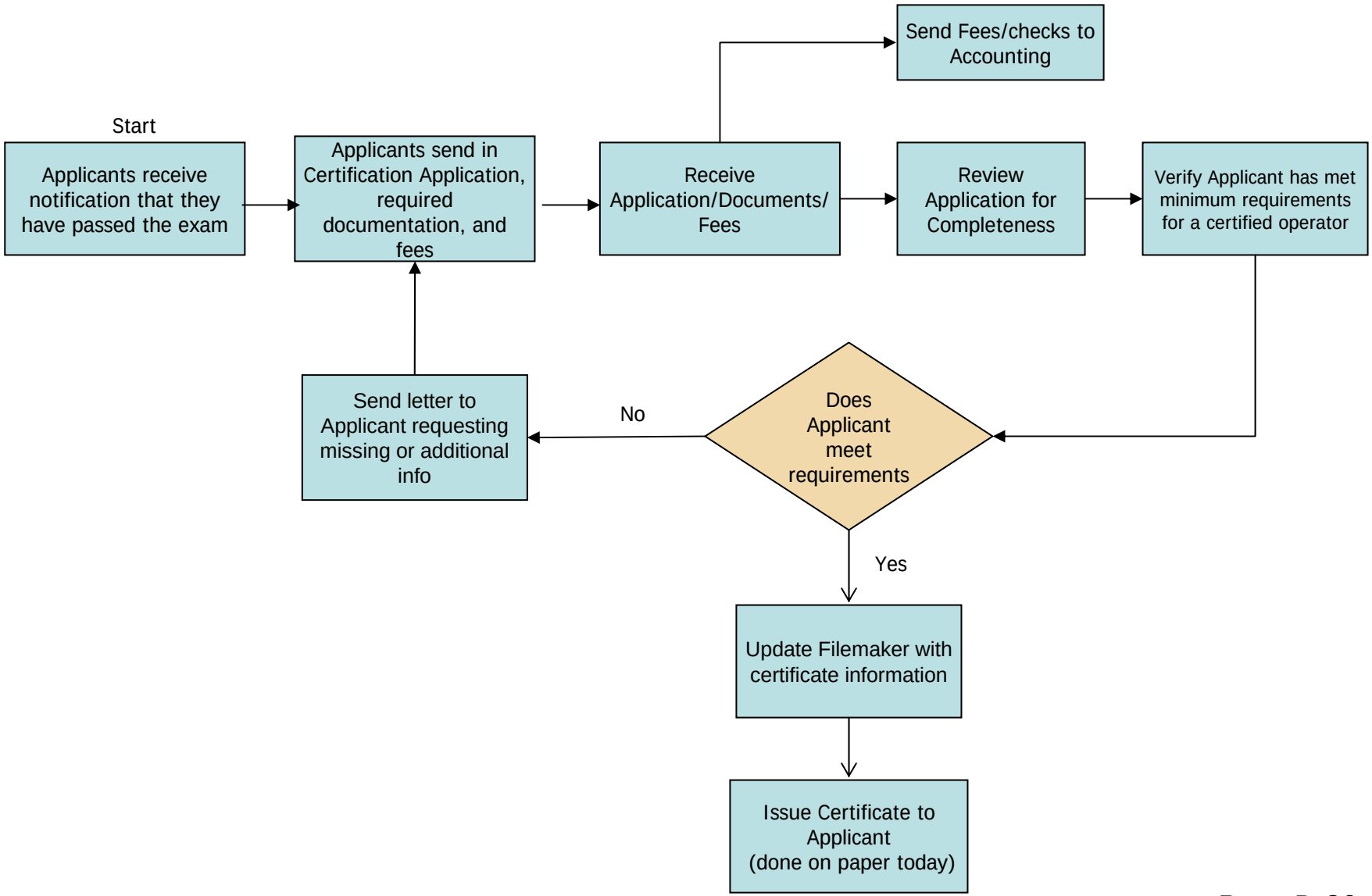


Drinking Water Operator Certification Program

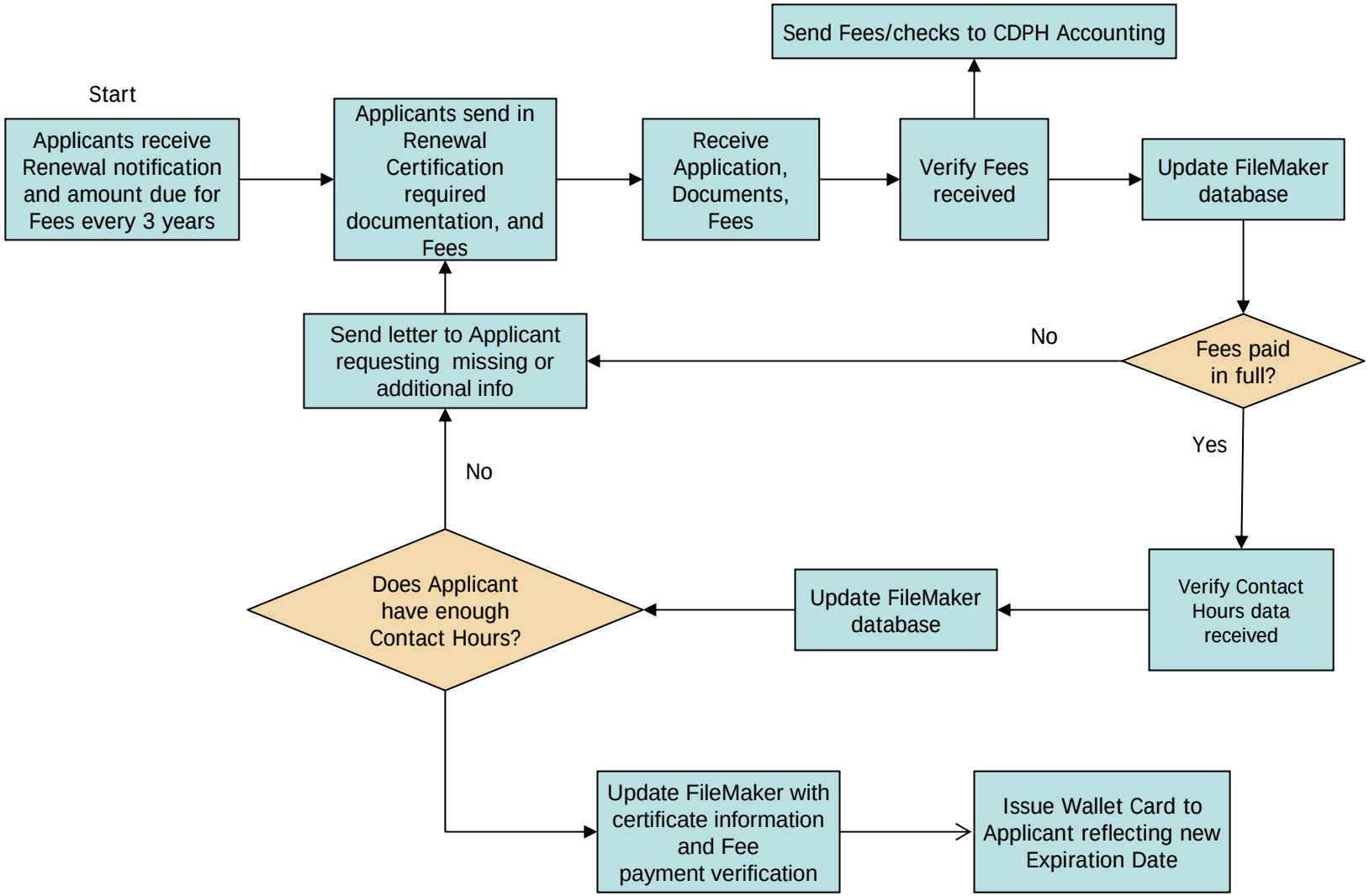
Water Operator Exam Application



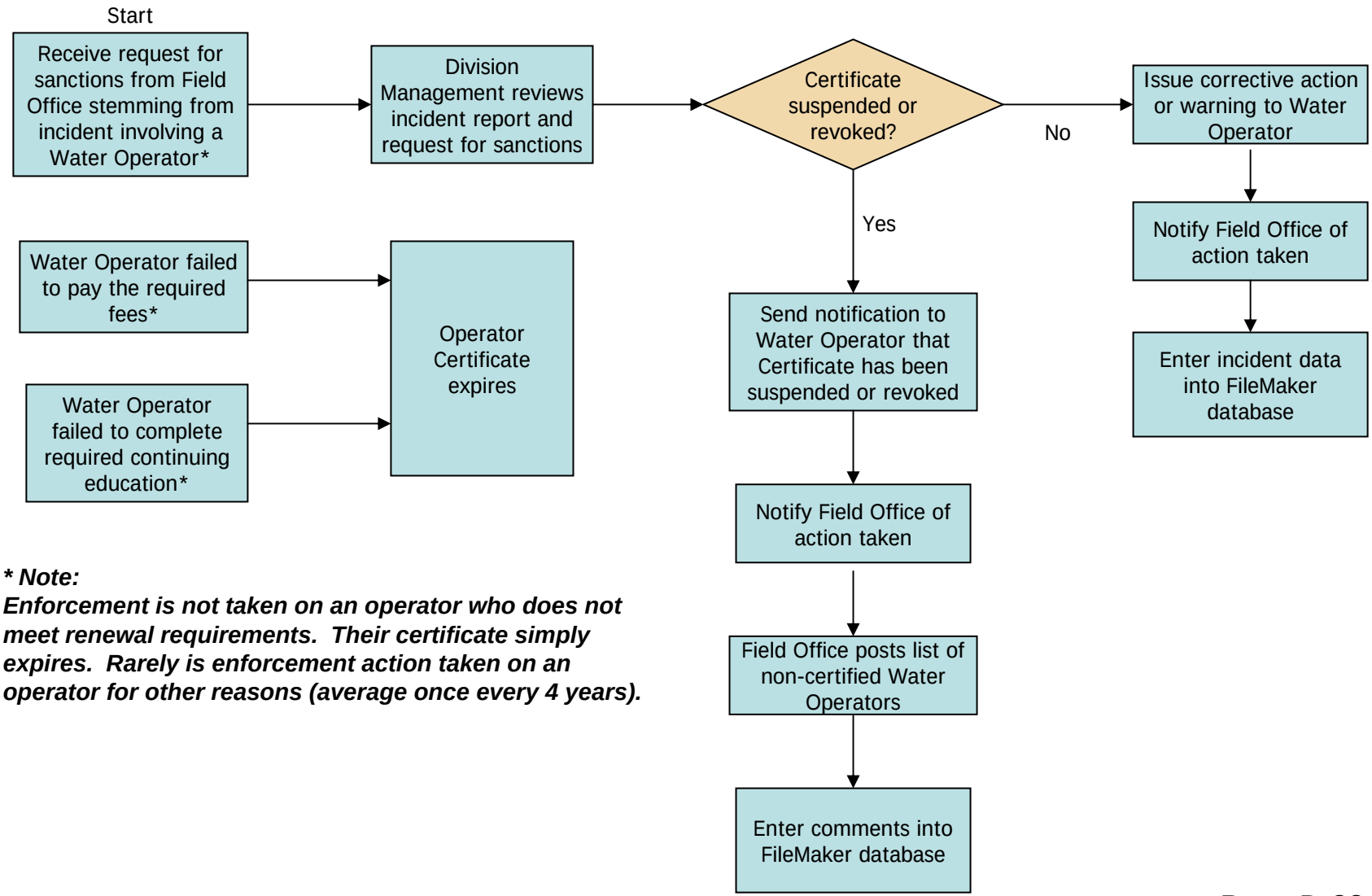
Water Operator Certification



Water Operator Certification Renewal



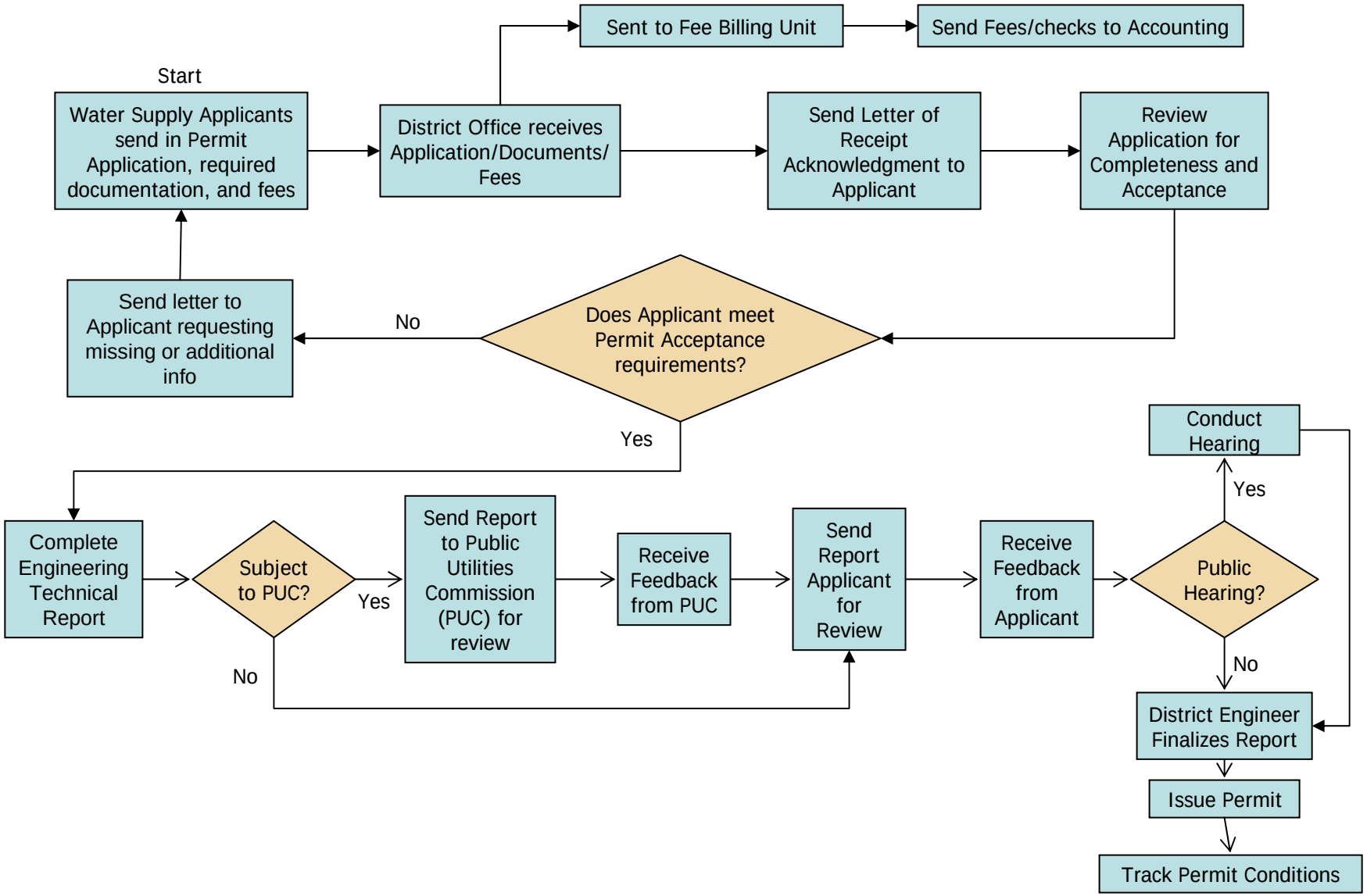
Water Operator Certificate Enforcement



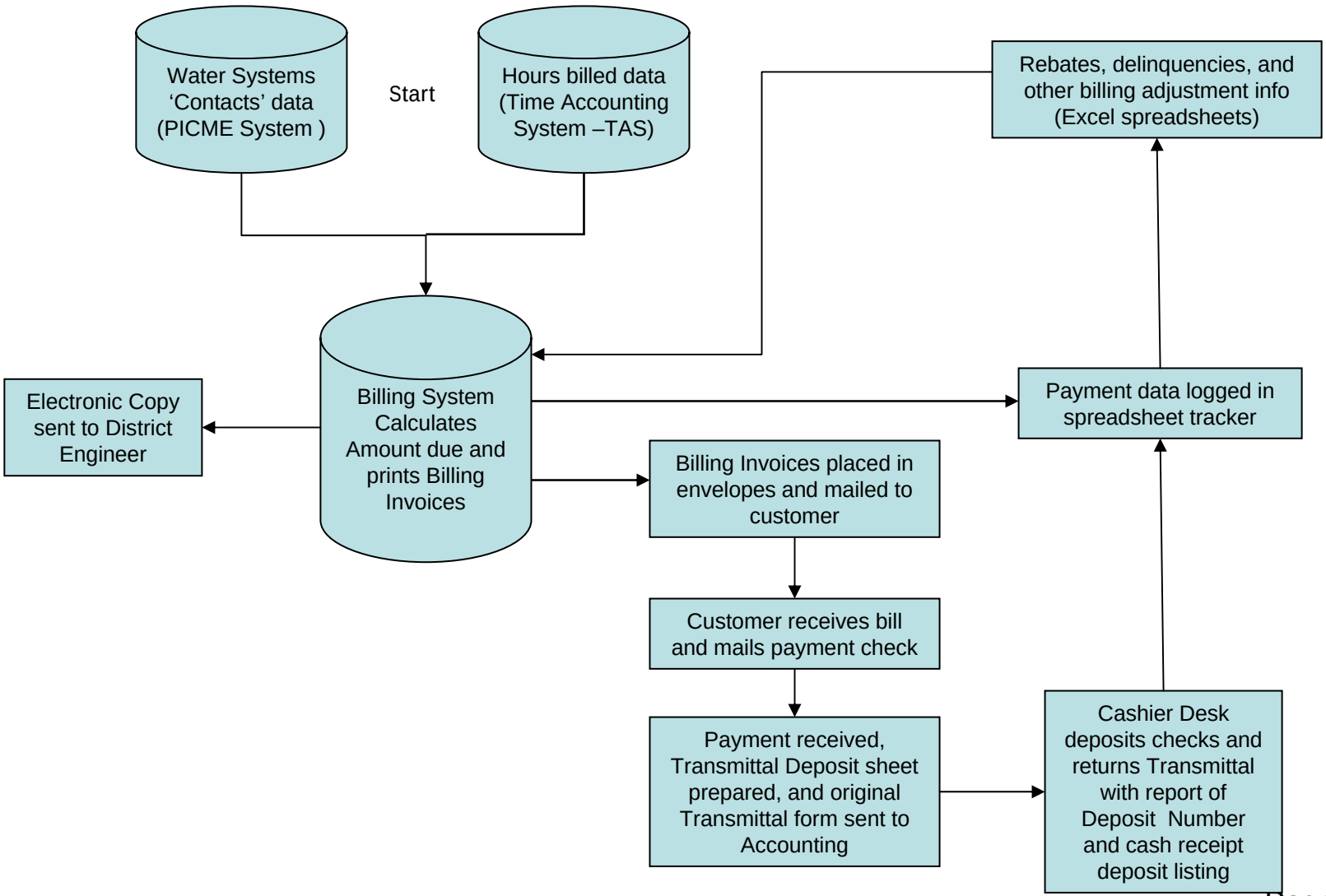
**** Note:***
Enforcement is not taken on an operator who does not meet renewal requirements. Their certificate simply expires. Rarely is enforcement action taken on an operator for other reasons (average once every 4 years).

Safe Drinking Water Systems

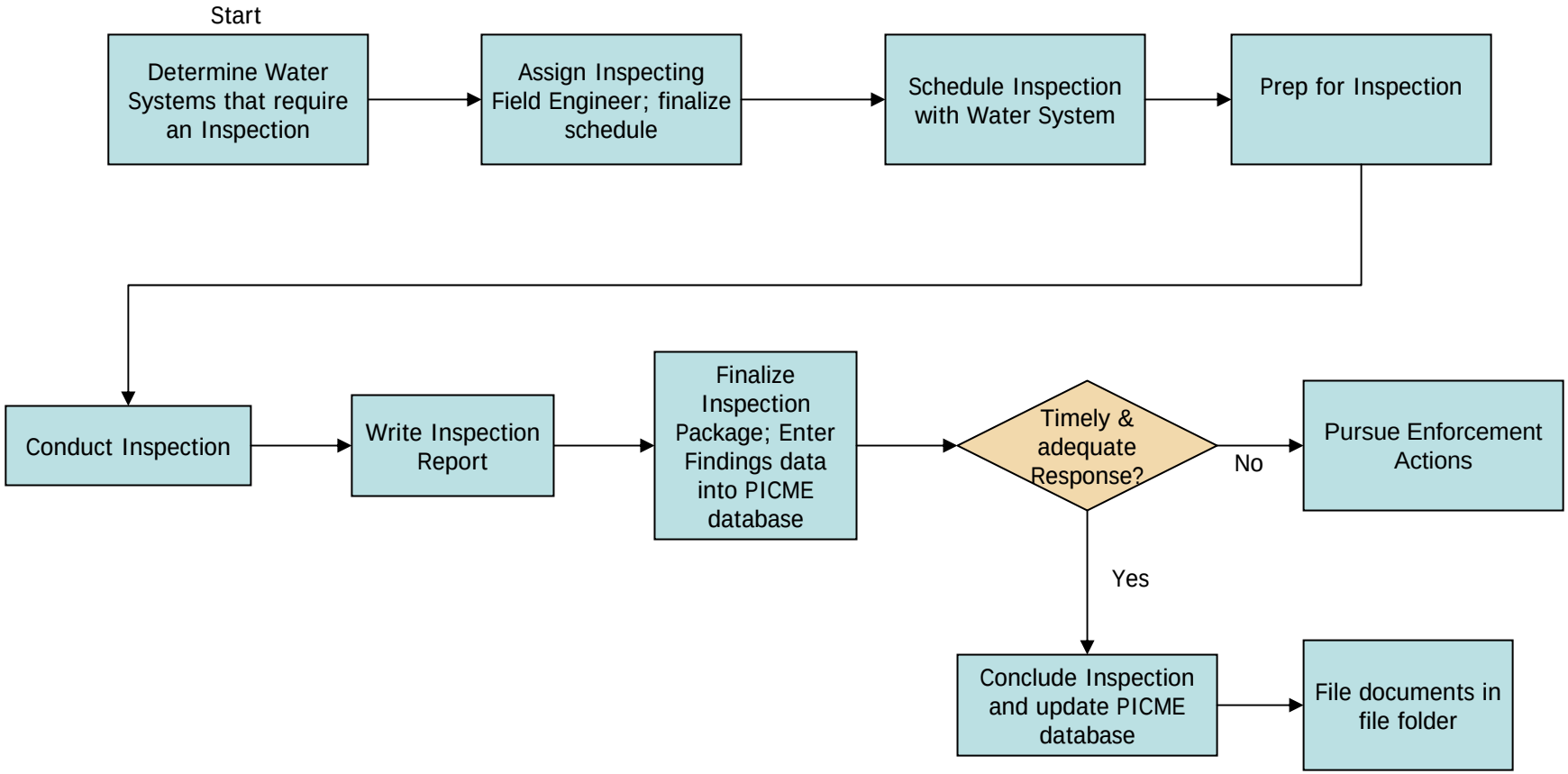
Water Supply Permit Application



Issue Water System Billing Notices

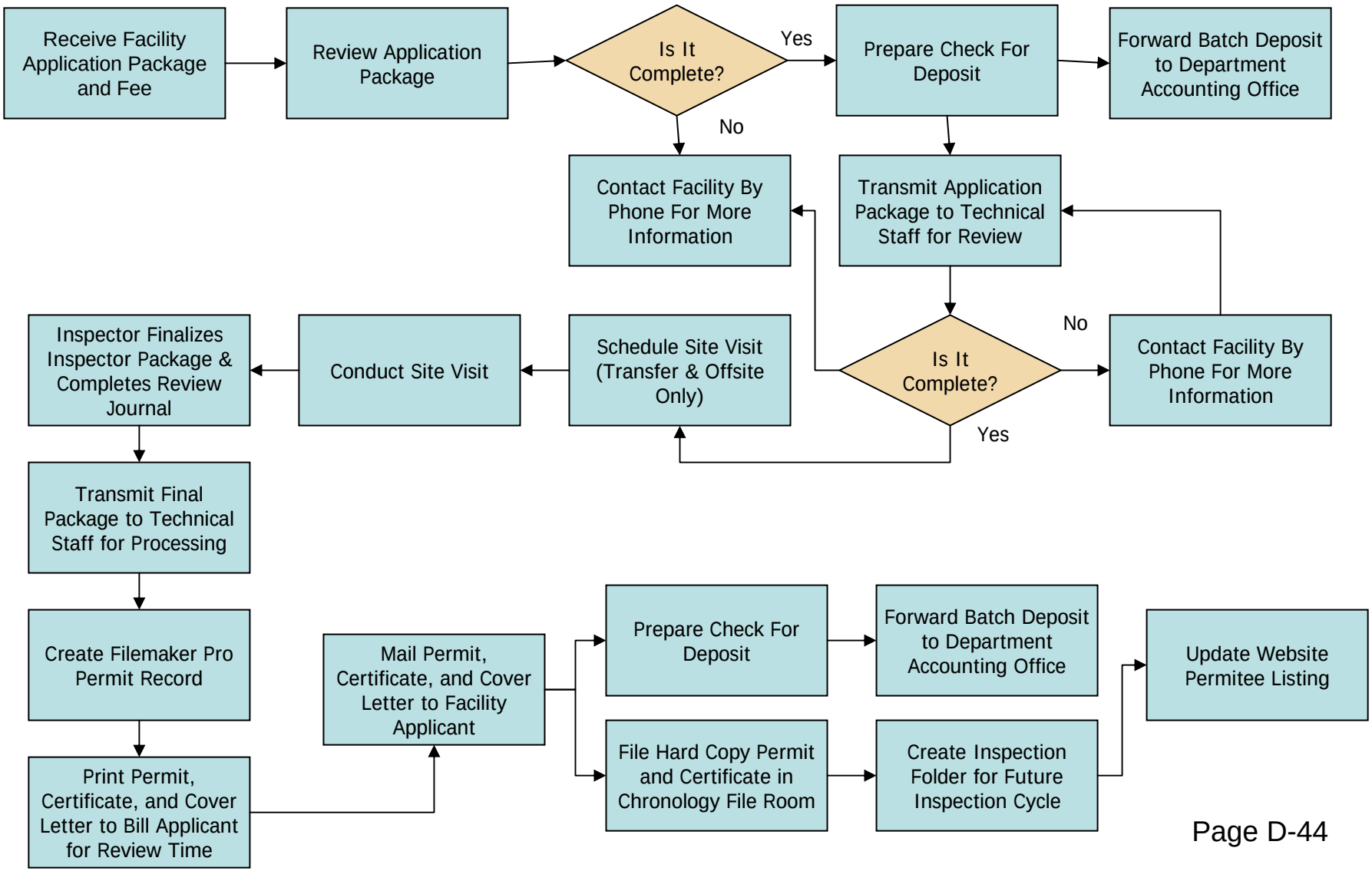


Perform Water System Inspection

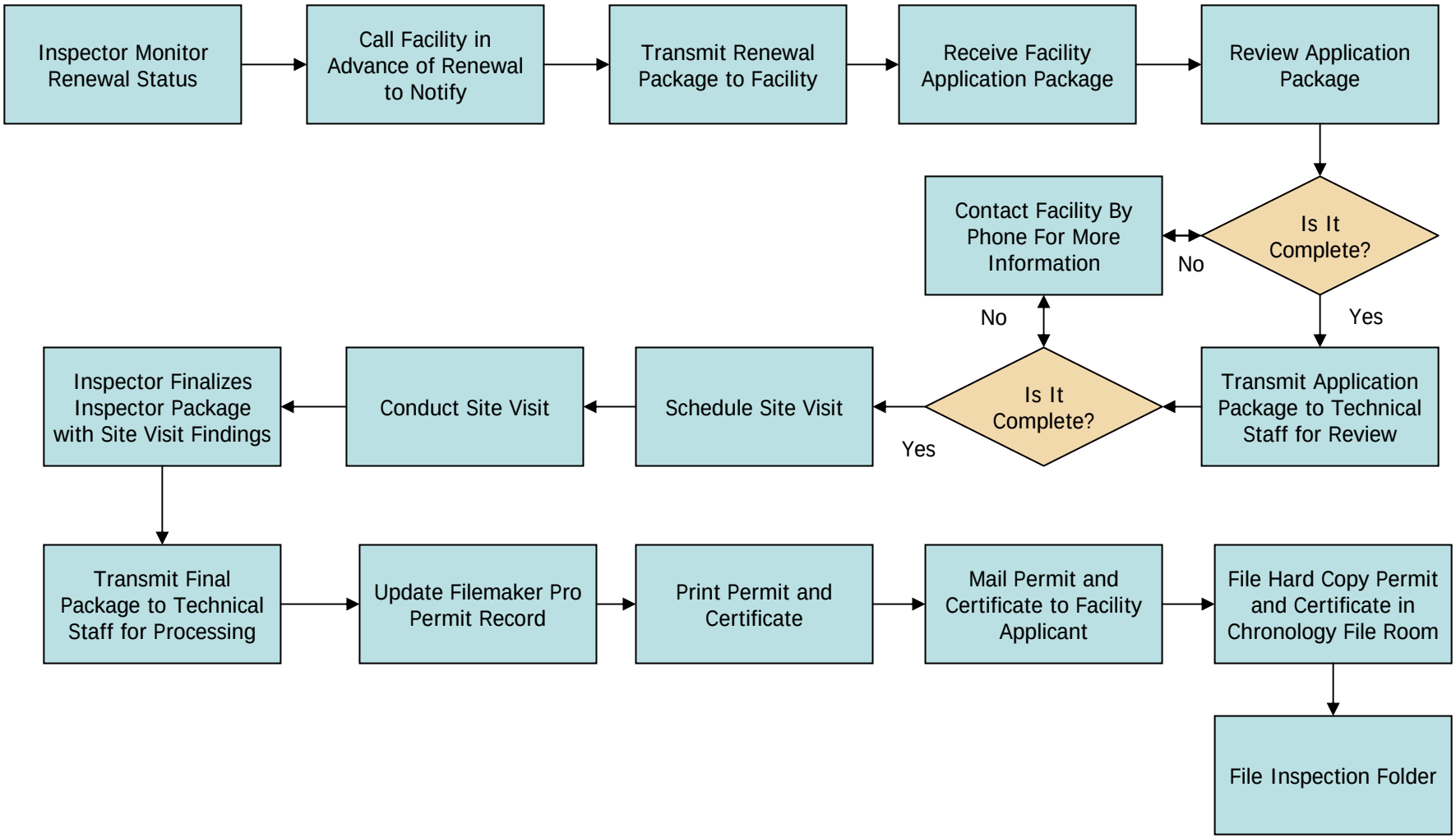


Medical Waste Management Program

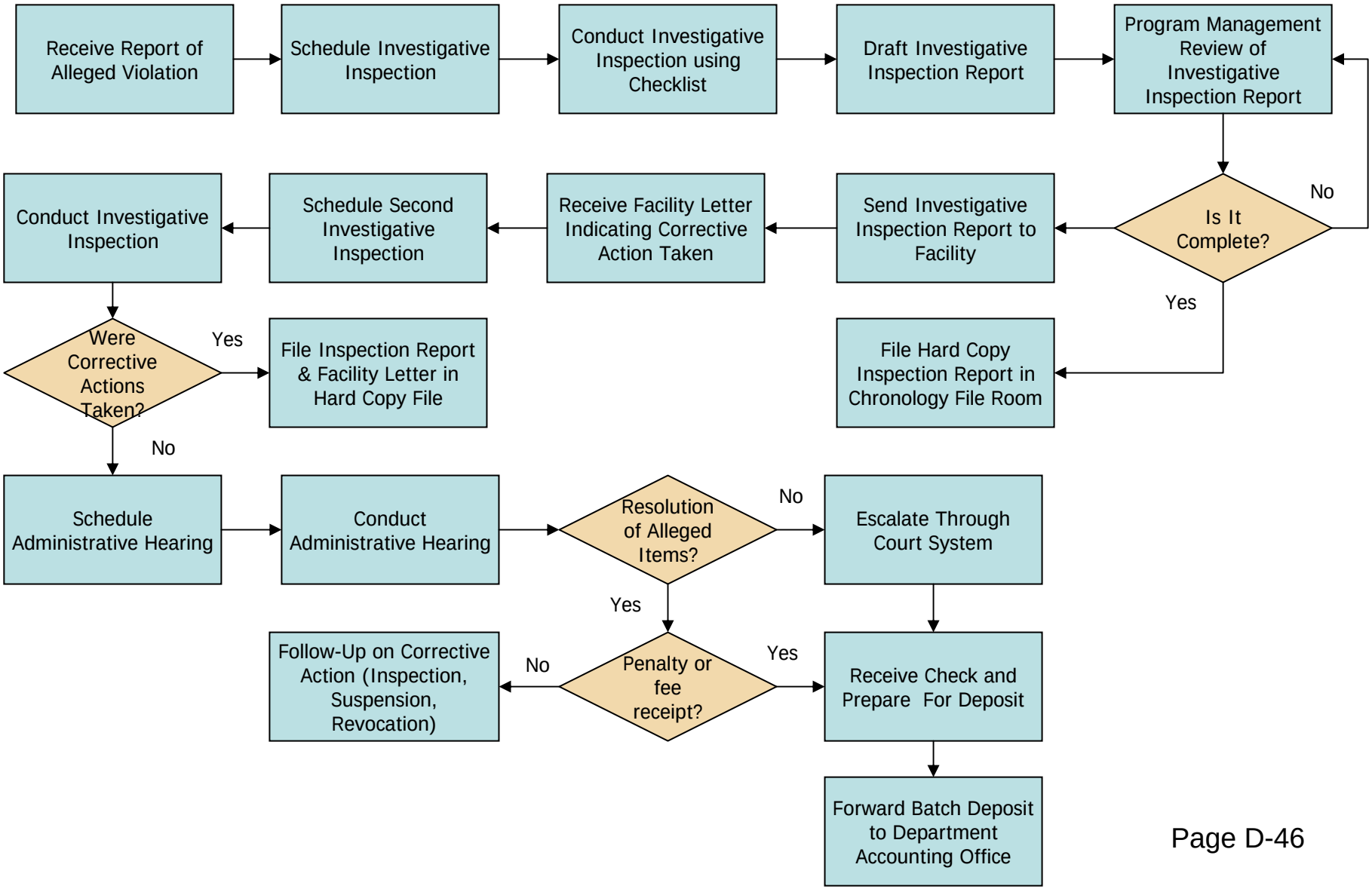
MWMP – Transfer Station/Off-Site Treatment Facility/Alternative Technology New Permit



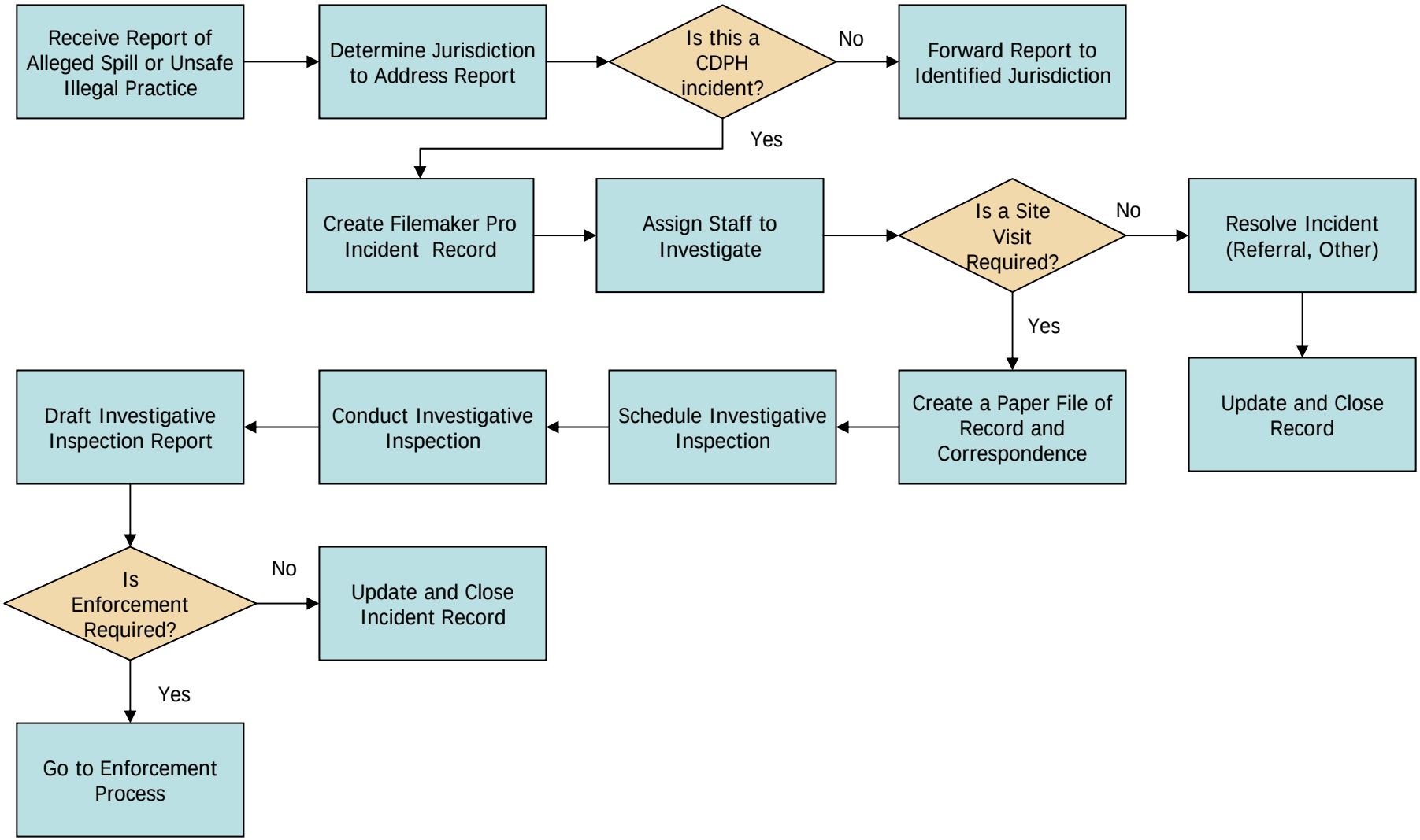
MWMP – Transfer Station/Off-Site Treatment Facility/Alternative Technology Permit Renewal



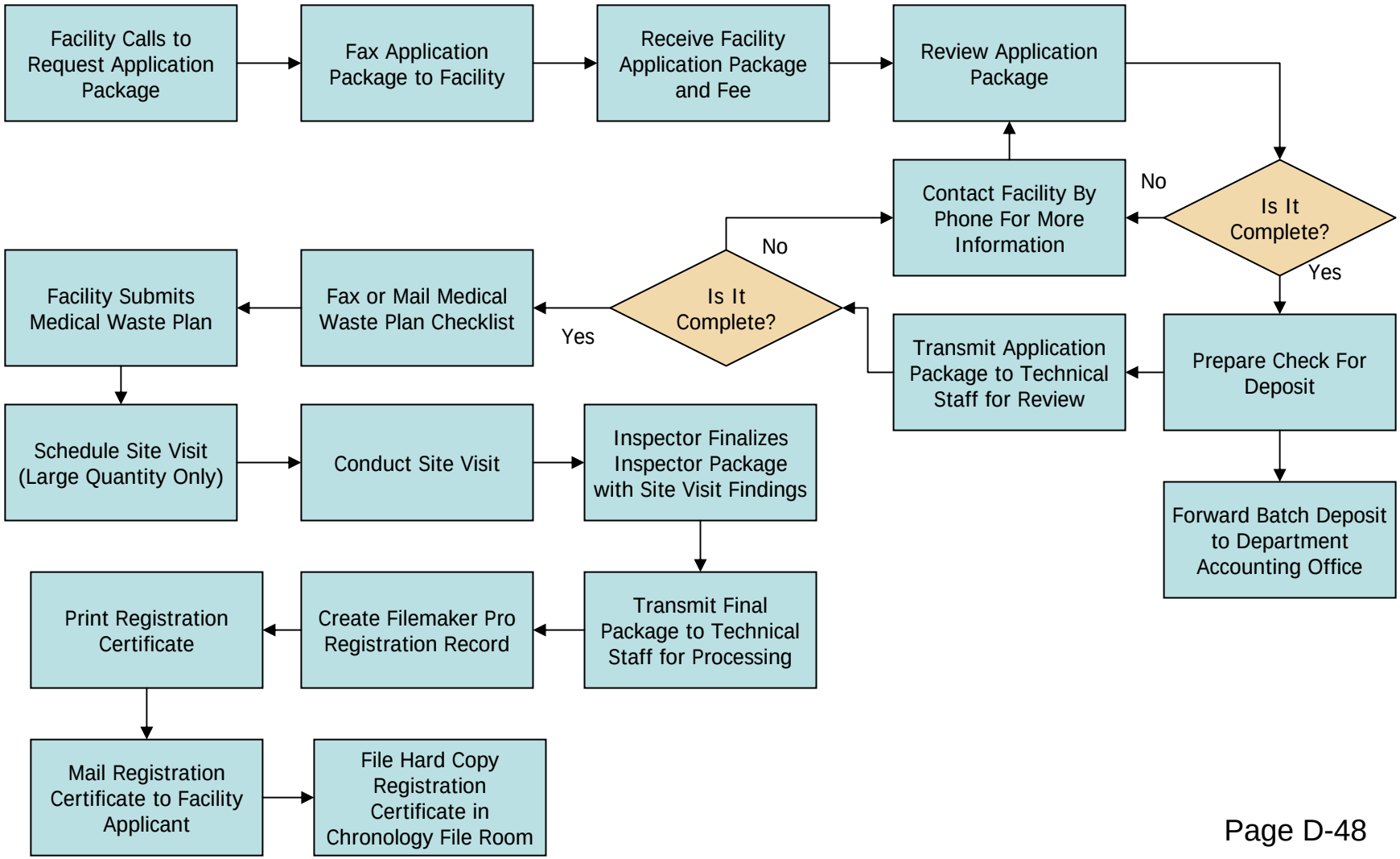
MWMP – Enforcement Process



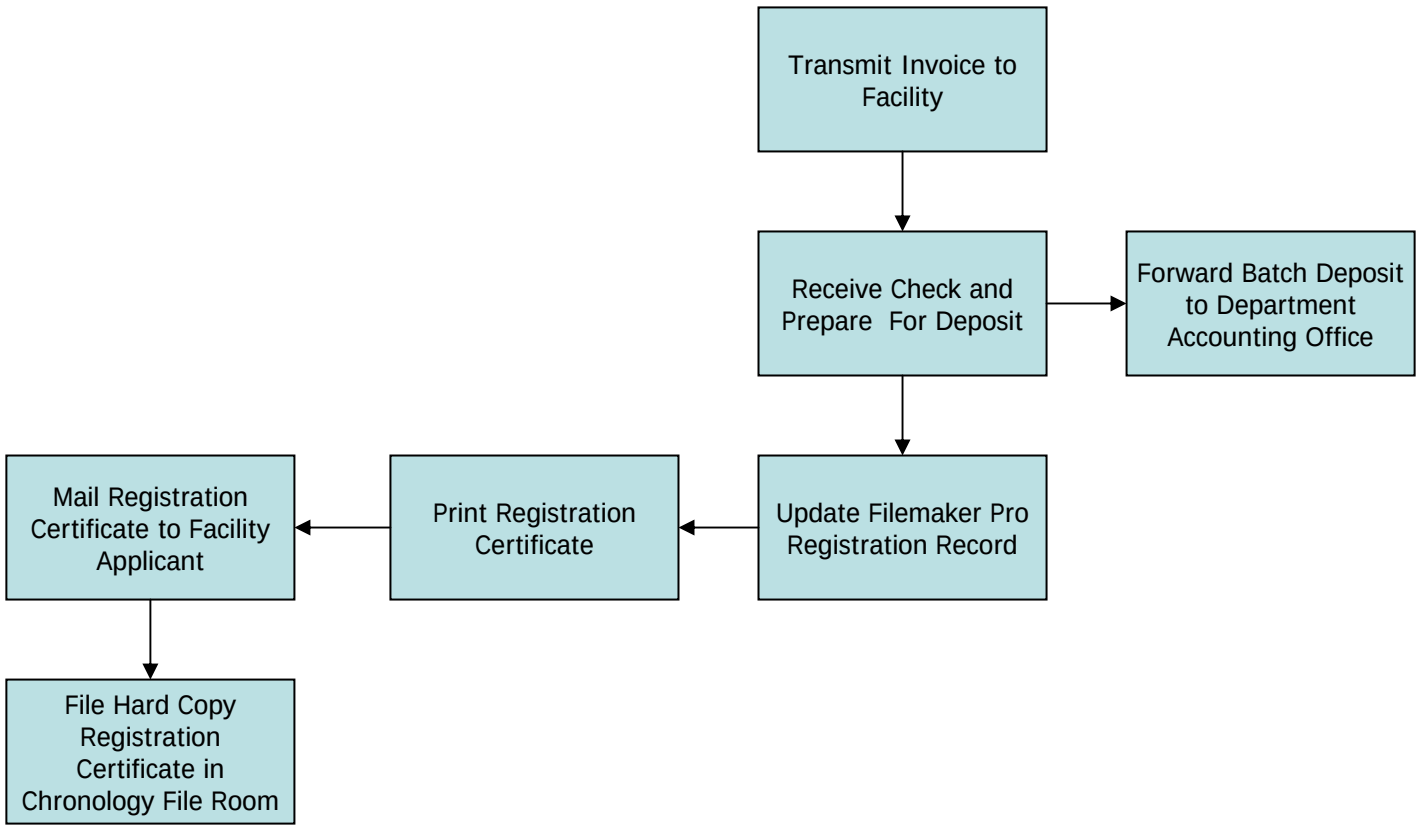
MWMP – Complaints/Incidents Process



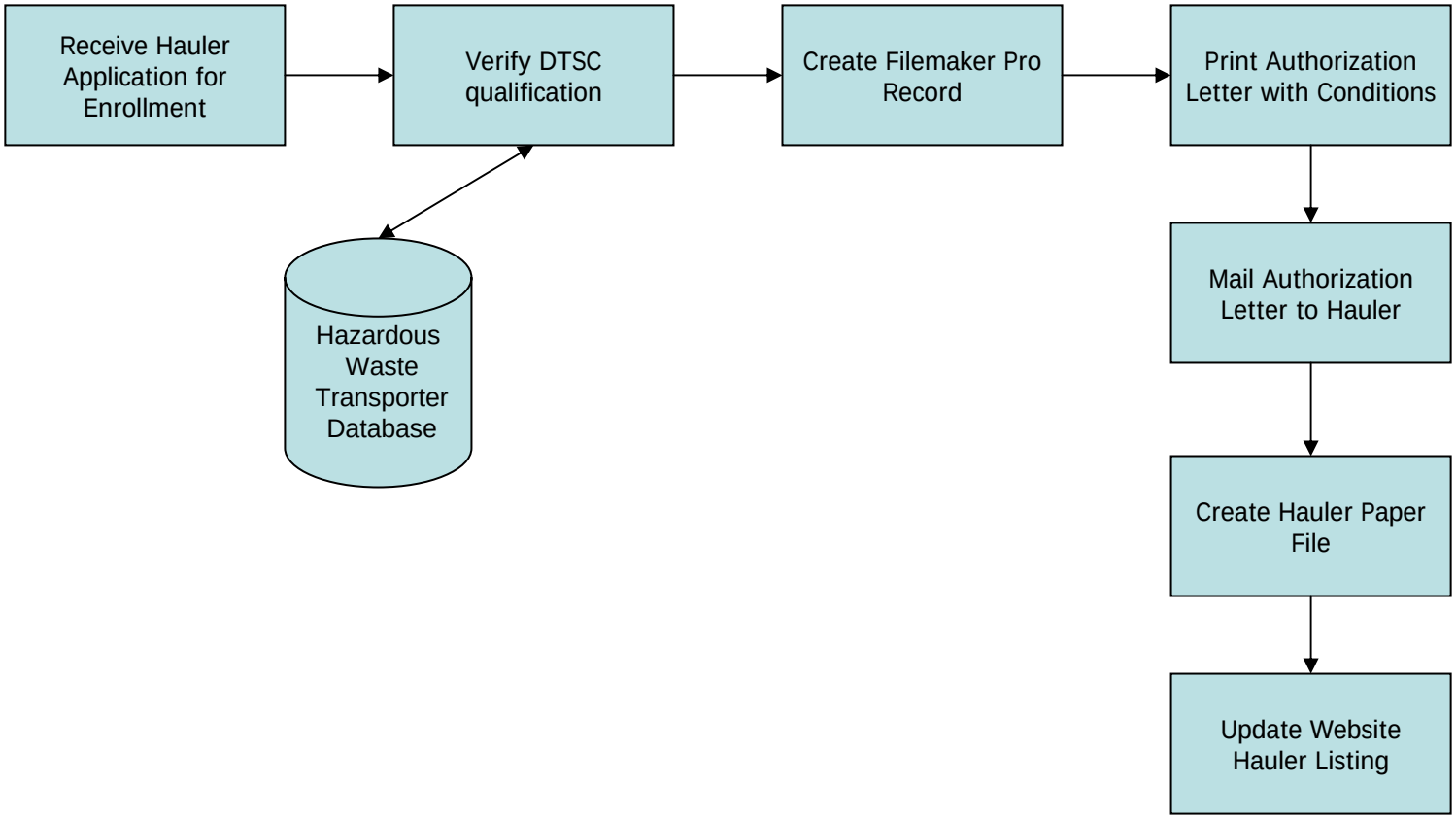
MWMP – Waste Generation Facilities/Trauma Scene Practitioners New Registration Process



MWMP – Waste Generation Facilities/Trauma Scene Practitioners Registration Renewal Process



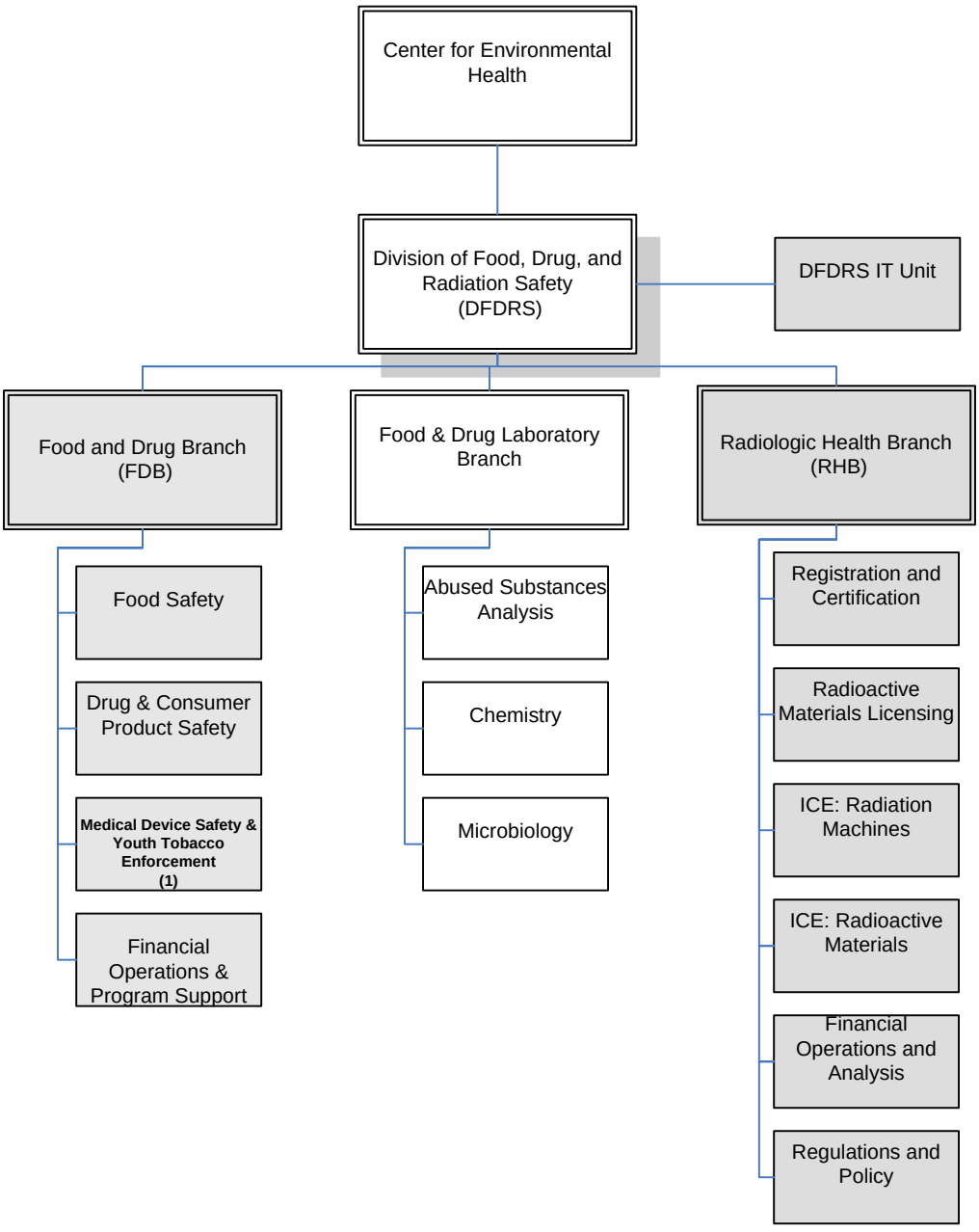
MWMP – Authorize Waste Hauler Process



Appendix E:

Participating Programs Organizational Structures

Food & Drug Branch
Radiologic Health Branch



NOTE: (1) Youth Tabacco Enforcement is not within the FSR scope.

Medical Waste Management Program
Drinking Water Operator Certification Program
Safe Drinking Water Systems Program