Western and Pacific Northwest Intergovernmental Audit Forums Joint Meeting
Assessing Risk Information Technology

Oversight of Information Technology Controls: A High-Risk Issue for California

Presented by:
Michelle Baur, CISA, Audit Principal
Information Technology Audits
California State Auditor's Office

September 2, 2015
Oakland, California

California State Auditor

Agenda

- Background on California IT Controls Oversight
- Designating Oversight of IT Controls a High-Risk Issue for California
- Auditing IT Controls Oversight
- Planning for Future High-Risk Engagements

Background on California IT Controls Oversight

California is a Prime Target

- 8th largest economy in the world as of 2013
- Maintains a variety of sensitive information
- Data centers subject to thousands of hacking attempts each month

California Department of Technology

Primary state authority for ensuring certain state entities maintain the confidentiality, integrity, and availability of their information systems and protect the privacy of the State's information.

Information Security Standards

- Comprised of 64 compliance sections that reference additional federal requirements and needs that are unique to California:
  - National Institute of Standards and Technology (NIST) *Special Publication 800-53*
  - *Federal Information Processing Standards* (FIPS)
  - *Statewide Information Management Manual*

Ensuring Reporting Entity Compliance

- The Technology Department is responsible for ensuring reporting entities comply with its policies:
  - Independent security assessments or audits
  - Annual self-certification

Designating Oversight of IT Controls a High-Risk Issue for California

IT Oversight: A High-Risk Issue

Concern #1:

- Technology Department relies on self-certification and it performed little to no follow-up.

Concern #2:

- We identified deficiencies in the general information system controls at two entities:
  - Department of Corrections and Rehabilitation
  - Employment Development Department

IT Oversight: A High-Risk Issue

Conclusion:

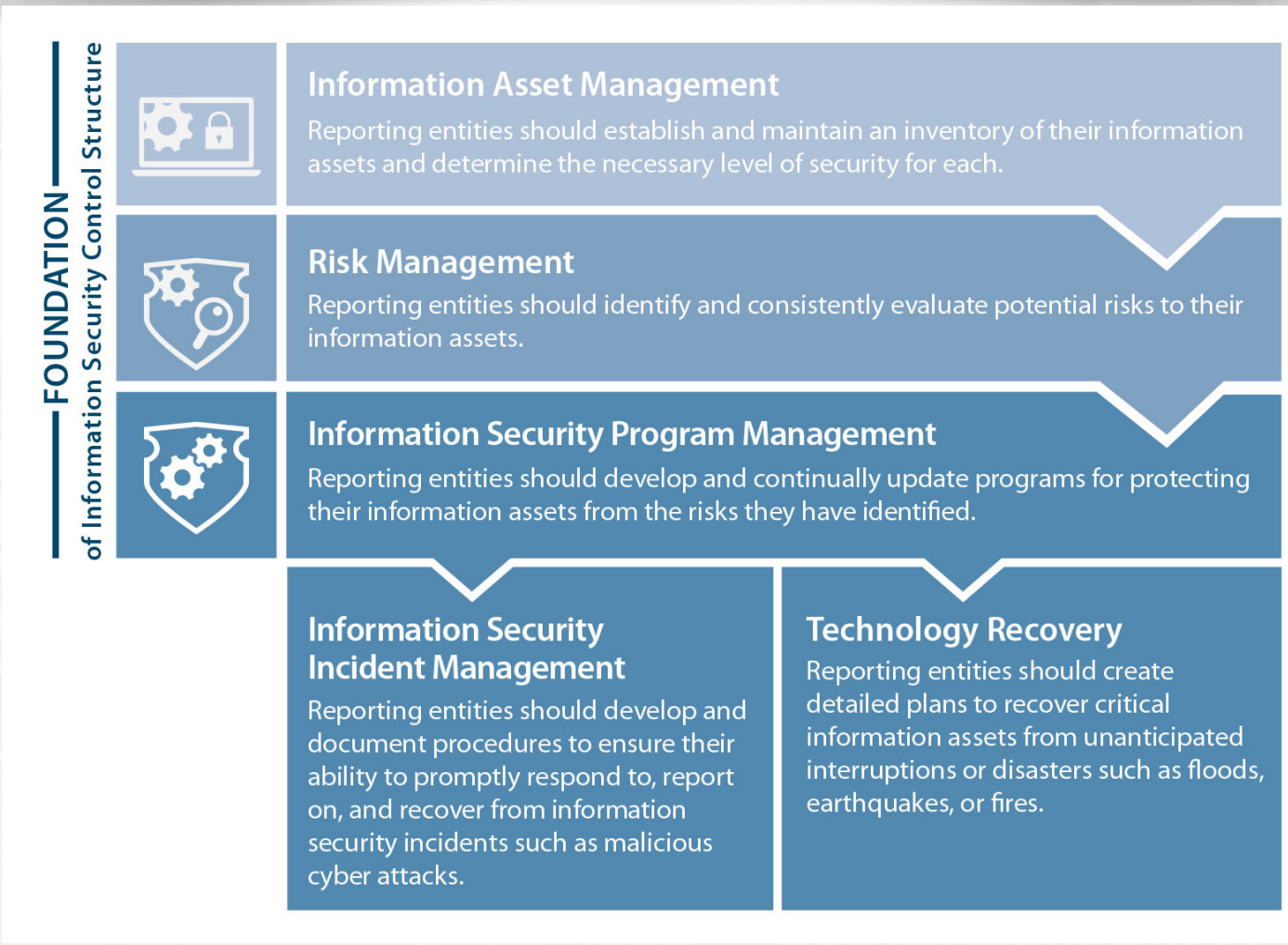
- The Technology Department's oversight of the general controls that reporting entities have implemented over their existing information systems should be designated as an issue of high risk for the State of California.

Auditing IT Controls Oversight

Depth of Testing

- Two Surveys
  - 101 reporting entities
  - Based on 2014 self-reported compliance status
- General control reviews
  - Five reporting entities

Which Requirements to Test



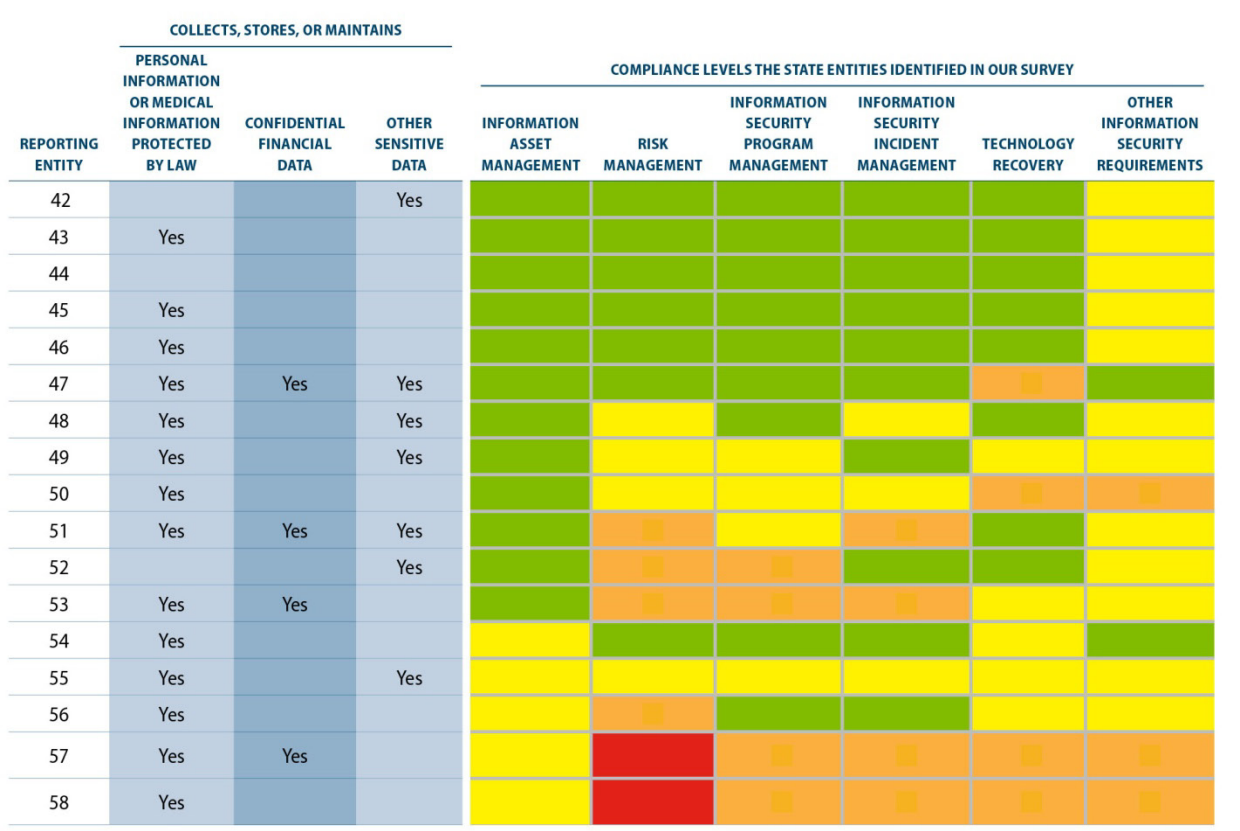
Which Entities to Test

- Collect, store, or maintain sensitive data
- Self-reported 2014 compliance status with the security standards
- Not included in the Technology Department's Pilot Audit Program
- Diverse sizes and responsibilities

		COLLECTS, STORES, OR MAINTAINS		
REPORTING ENTITY	ENTITY DESCRIPTION	PERSONAL INFORMATION OR HEALTH INFORMATION PROTECTED BY LAW	CONFIDENTIAL FINANCIAL DATA	OTHER SENSITIVE DATA
A	Provides critical state services	Yes	Yes	Yes
B	Administers federal and state programs	Yes	No	No
C	Oversees an entitlement program	Yes	Yes	Yes
D	Performs enforcement activities	Yes	No	Yes
E	Manages critical state resources	Yes	No	Yes

What Information to Report

- Did not include reporting entities names
- Aggregated reporting for each control area



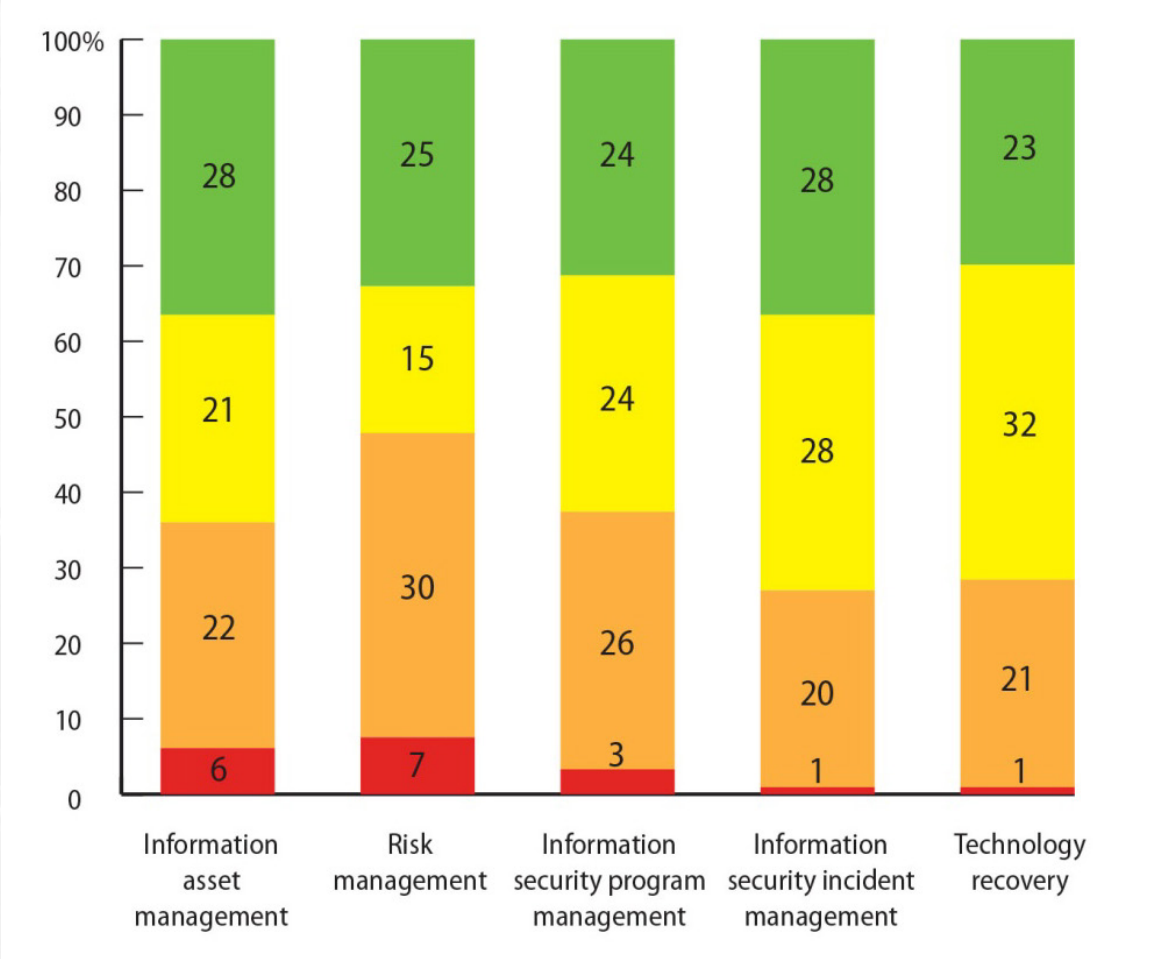
	COLLECTS, STORES, OR MAINTAINS			COMPLIANCE LEVELS THE STATE ENTITIES IDENTIFIED IN OUR SURVEY					
REPORTING ENTITY	PERSONAL INFORMATION OR MEDICAL INFORMATION PROTECTED BY LAW	CONFIDENTIAL FINANCIAL DATA	OTHER SENSITIVE DATA	INFORMATION ASSET MANAGEMENT	RISK MANAGEMENT	INFORMATION SECURITY PROGRAM MANAGEMENT	INFORMATION SECURITY INCIDENT MANAGEMENT	TECHNOLOGY RECOVERY	OTHER INFORMATION SECURITY REQUIREMENTS
42			Yes						
43	Yes								
44									
45	Yes								
46	Yes								
47	Yes	Yes	Yes						
48	Yes		Yes						
49	Yes		Yes						
50	Yes								
51	Yes	Yes	Yes						
52			Yes						
53	Yes	Yes							
54	Yes								
55	Yes		Yes						
56	Yes								
57	Yes	Yes							
58	Yes								

Control Review Findings

REPORTING ENTITY	ENTITY DESCRIPTION	COLLECTS, STORES, OR MAINTAINS: PERSONAL INFORMATION OR HEALTH INFORMATION PROTECTED BY LAW	COLLECTS, STORES, OR MAINTAINS: CONFIDENTIAL FINANCIAL DATA	COLLECTS, STORES, OR MAINTAINS: OTHER SENSITIVE DATA	INFORMATION ASSET MANAGEMENT	RISK MANAGEMENT	INFORMATION SECURITY PROGRAM MANAGEMENT	INFORMATION SECURITY INCIDENT MANAGEMENT	TECHNOLOGY RECOVERY
A	Provides critical state services	Yes	Yes	Yes					
B	Administers federal and state programs	Yes	No	No					
C	Oversees an entitlement program	Yes	Yes	Yes					
D	Performs enforcement activities	Yes	No	Yes					
E	Manages critical state resources	Yes	No	Yes					

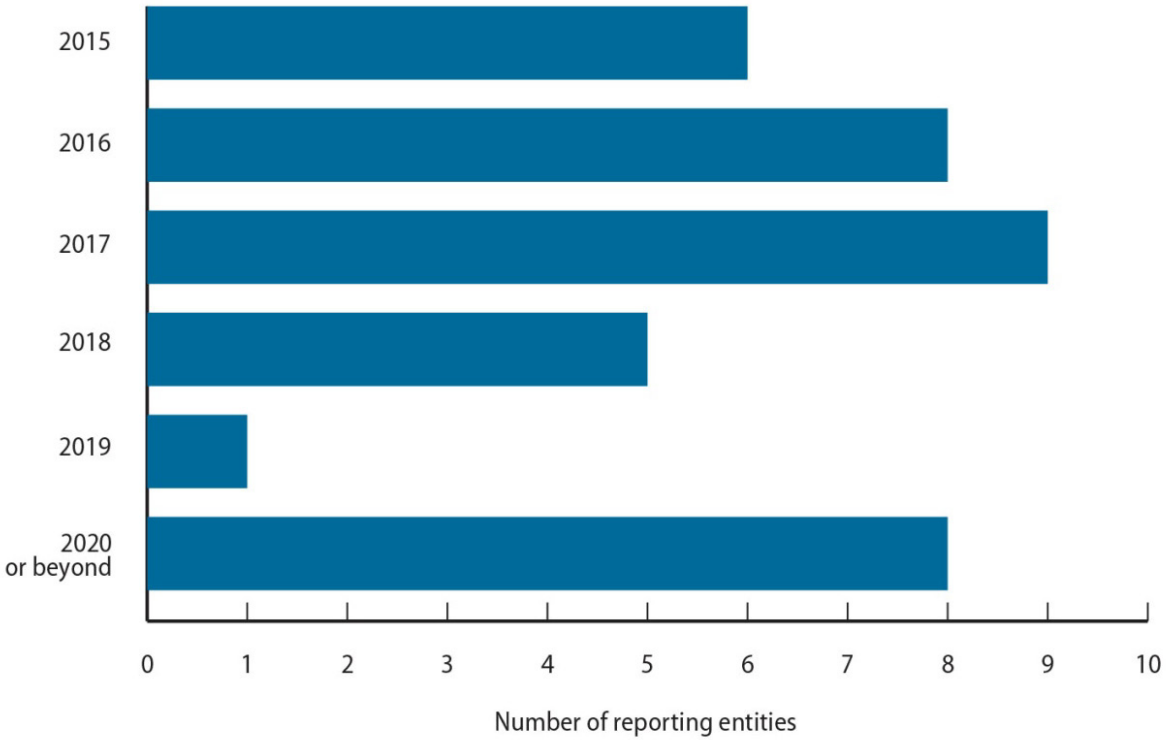
- = **Fully compliant:** The reporting entity is fully compliant with all the requirements in Chapter 5300 of the *State Administrative Manual* (security standards) we tested for the control area.
- = **Mostly compliant:** The reporting entity has attained nearly full compliance with all of the security standards we tested for the control area.
- = **Partially compliant:** The reporting entity has made measurable progress in complying, but has not addressed all of the security standards we tested for the control area.
- = **Not compliant:** The reporting entity has not yet addressed the security standards we tested for the control area.

Combined Survey Results



Non-Compliant Survey Results

The year by which reporting entities that self-reported non-compliance to the Technology Department expect to achieve full compliance with the security standards:



Planning for Future Engagements

Future High-Risk Work

- Non-reporting entities are not subject to the Technology Department's oversight
- Several of these entities maintain sensitive information and provide some of the most critical services in the State

Future High-Risk Work

- We identified significant deficiencies in the controls over two nonreporting entities' information systems.
  - Administrative Office of the Courts and the Superior Courts
  - California Public Utilities Commission

Future High-Risk Work

- The California State Auditor plans to assess the information security risks associated with nonreporting entities
- Depending on the results, we will consider whether to expand the high-risk issue of IT oversight to include them

California State Auditor Reports

- **Report #2013-601**, designated California's oversight of information technology controls a high-risk issue
- **Report #2015-601**, details the results of our high-risk audit

Available on the California State Auditor's web site at http://www.auditor.ca.gov/reports

Contact Information

Michelle J. Baur, CISA, Audit Principal
Information Technology Audits
California State Auditor
621 Capitol Mall, Suite 1200
Sacramento, California 95814

(916) 445-0255 extension 327

MichelleB@auditor.ca.gov