Auditing Information Security

Lindsay M. Harris, CISA

California State Auditor's Office

September 13, 2016

Introduction/Agenda

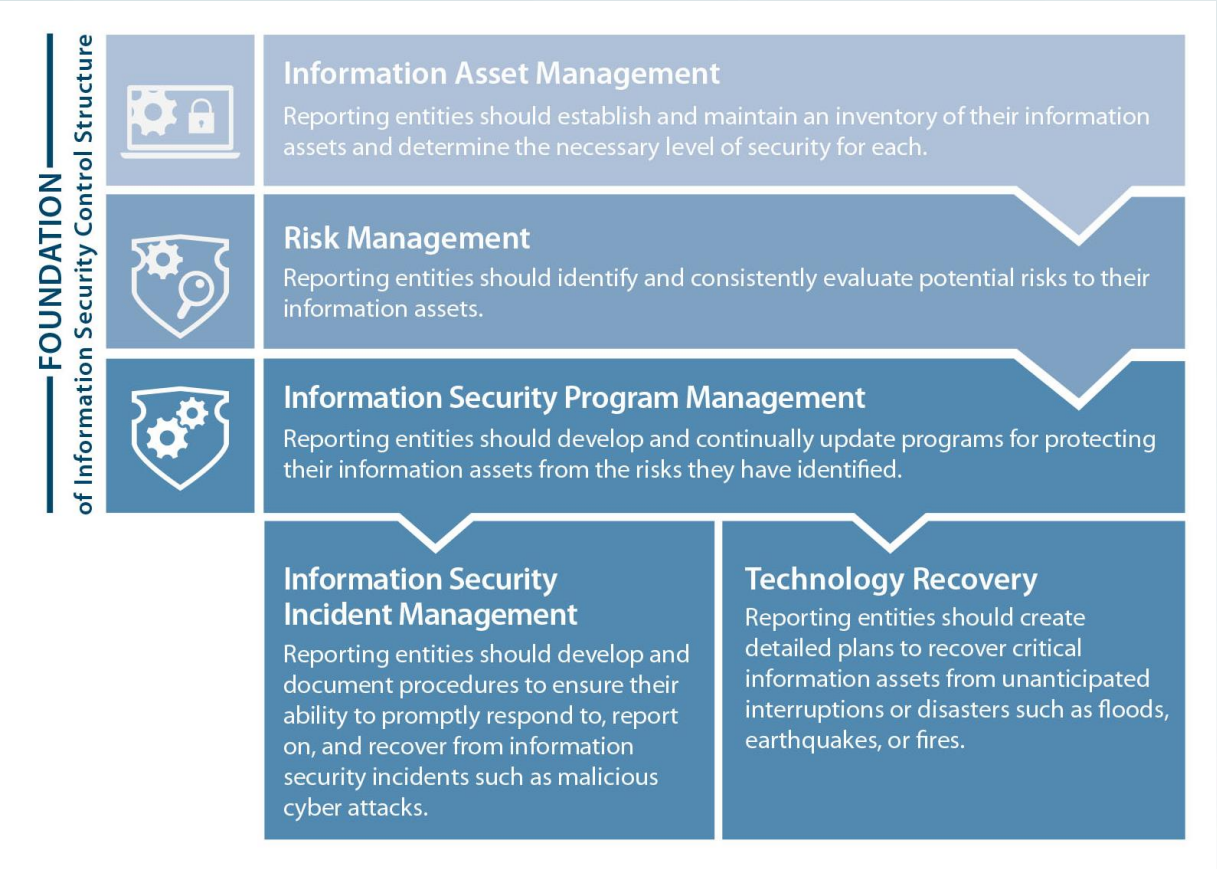
- Our Approach
- What We Found
- The Cause
- What We Recommended
- The Outcome

Our Approach

- Identified Certain Requirements to Test
  - Information Asset Management
  - Risk Management
  - Information Security Program Management
  - Information Security Incident Management
  - Technology Recovery

California State Auditor

Our Approach



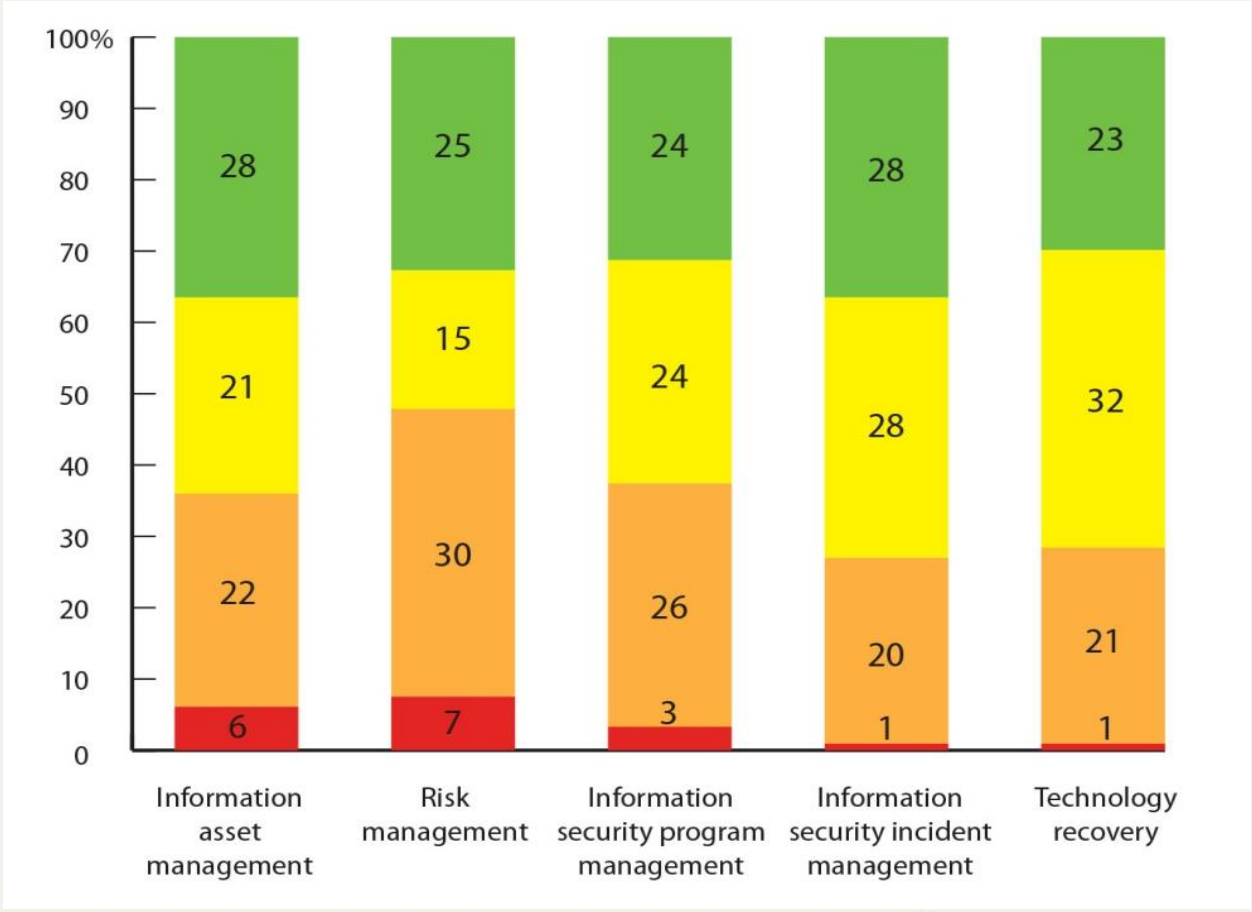
California State Auditor

Our Approach

- Reviewed Department Compliance Reports
  - Self-Reported Compliance Status
- Surveyed Over 100 State Entities
  - 77 Entities Responded

California State Auditor

Survey Says ....



What Is Really Going On?

- Selected Five Reporting Entities to Conduct On-site General Control Review
  - Collect, Store or Maintain Sensitive Data
  - Self-Reported Compliance in 2014
  - Diverse Sizes and Responsibilities

California State Auditor

What is Really Going On?

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					

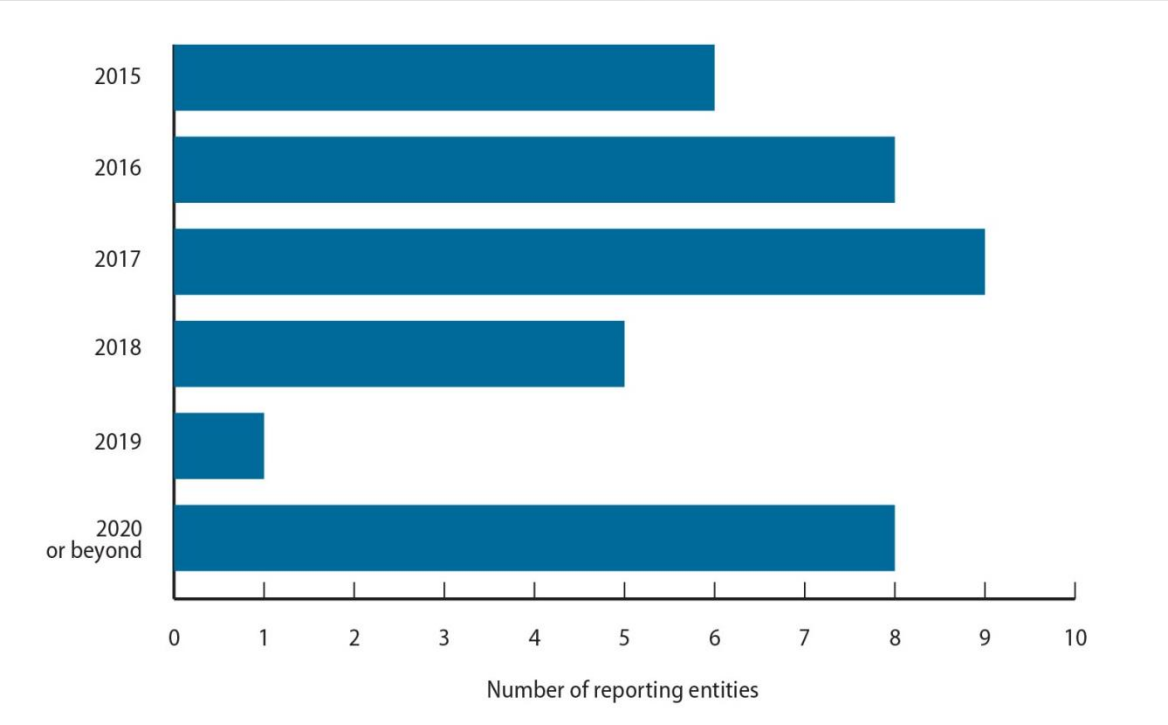
California State Auditor

Why?

- Lack of Effective Oversight
  - The Department of Technology Was Unaware
  - 37 of 41 Survey Respondents Had Certified Compliance to the Department
  - Some Entities' Weaknesses Persisted For Years
  - The Department of Technology Did Not Always Follow-up on Remediation Plans
- Lack of Guidance and Training

California State Auditor

When Do Entities Expect to Comply?



California State Auditor

What We Recommended

- Mandate Biennial Security Assessments
- Authorize the Department of Technology To Redirect Funds to Remediate Weaknesses
- Improve IT Oversight Practices at the Department of Technology

What Has Happened?

- Governor's Executive Order: California Cybersecurity Integration Center
  - To strengthen California's cybersecurity strategy and improve inter-agency, cross-sector coordination
  - Central hub for state government's cybersecurity
  - Coordinate information sharing
  - Broadly represented
  - Cyber Incident Response Team

California State Auditor

What Has Happened?

- Enacted AB 670
  - At Least 35 Security Assessments Annually
  - Establish Assessment Requirements
  - Entity Being Assessed Funds the Assessment
  - Share Results with California Office of Information Security and Office of Emergency Services

California State Auditor

What Has Happened?

- The Department of Technology Made Changes
  - Adopted Nationwide Cyber Security Review Self-Assessment
  - Established a Plan of Action and Milestone Tool
  - Expanded Ongoing Risk-Based Audit Program
  - Partially Implemented Other Recommendations

What Has Happened?

- Continual Legislative Interest
  - Legislation Passed
  - Legislative Oversight Hearings
  - Considering Future Audit Work

More Information?

- Report #2015-611, Details The Results of This High Risk Audit
- Report #2014-602, Designated Oversight of IT Projects a High Risk Issue
- Report #2013-601, Designated Oversight of IT Controls a High Risk Issue

» www.auditor.ca.gov

California State Auditor