ISO BASIC TRAINING RESOURCES LIST

GENERAL INFORMATION

Resource: **Office of Information Security (OIS) Website**
Acronym: OIS Website
What: Central resource that provides links to policies, standards, guidelines, and best practices regarding information security.
Link: https://cdt.ca.gov/security/

Resource: **California IT Directory**
Acronym: NA
What: Information Security Officers (ISO), Technology Recovery Coordinator, Privacy Program Coordinator, and State AIO/CIO leader lists. Contact list to assist with networking and peer support.
Link: https://cdt.ca.gov/security/resources/#California-IT-Directory

Resource: **State Administrative Manual**
Acronym: SAM
What: SAM is a reference source to statewide management policy. The California Department of Technology (CDT), OIS policies can be found in Section 5300.
Link: http://sam.dgs.ca.gov/TOC/5300.aspx

Resource: **Statewide Information Management Manual**
Acronym: SIMM
What: SIMM contains standards, instructions, forms and templates that State entities must use to comply with Information Technology (IT) policy.
Link: https://cdt.ca.gov/policy/simm/

Resource: **National Institute of Standards and Technology**
Acronym: NIST
What: NIST Special Publication (SP) subseries provide state entities with computer/cyber/information security and guidelines, recommendations and reference materials; referenced in SP 800, SP 1800, and SP 500.
Link: http://csrc.nist.gov/publications/PubsSPs.html

Resource: **OIS Foundational Framework**
Acronym: NA
What: Security controls and objectives an entity must focus on first for an information security program.
Link: https://cdt.ca.gov/wp-content/uploads/2017/06/SIMM-5330_B-Foundational-Framework.pdf

ISO BASIC TRAINING RESOURCES LIST

AUDITS, ASSESSMENTS, AND ADVISORY SERVICES

Resource: **Information Security – Oversight Website**
Acronym: NA
What: Provides expertise to evaluate compliance with state security and privacy policies, by validating security systems, procedures and practices are in place and working as intended.
Link: https://cdt.ca.gov/security/oversight/

Resource: **Information Security Program Audit Website**
Acronym: NA
What: Provides expertise to evaluate compliance with state security and privacy policies, by validating security systems, procedures and practices are in place and working as intended.
Link: https://cdt.ca.gov/services/information-security-program-audit/

Resource: **The California Military Department**
Acronym: CMD
What: Assists Department of Defense, Federal, State, Local Government partners and Critical Infrastructure providers to provide confidentiality, integrity, and availability of critical network infrastructure.
Link: http://www.calguard.ca.gov/J6/Pages/Cyber-Network-Defense.aspx

Resource: **State of California Independent Security Assessment Criteria**; **Phase – II Version 1, dated 2/27/2017**
Acronym: NA
What: In accordance with Assembly Bill 670, enacted on October 6, 2015 Agencies are required to undergo an Independent Security Assessment in accordance with the agreed upon standards set forth by the California Information Security Office. This criterion details the areas of assessment, components evaluated, and standards for compliance determination. Assessed agencies may achieve one of three possible scores for each sub-component.
Link: http://www.calguard.ca.gov/J6/Documents/ISA_Ph_II_v1_0.pdf

COMPLIANCE REPORTING

Resource: **California State Government- Executive Branch Organizational Chart**
Acronym: Org Chart
What: The Executive Branch org chart identifies all state entities under the jurisdiction of the Governor's office; identifying the state entities required to report to CDT.
Link: https://cold.govops.ca.gov/File/OrganizationalChart

ISO BASIC TRAINING RESOURCES LIST

Resource: **Schedule of Required Reporting Activities**
Acronym: SAM 5330.2
What: Outlines the reporting schedule that each state entity must adhere to when submitting compliance documents to CDT.
Link: https://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5330.2.pdf

Resource: **Status of Required Security Reporting Activities**
Acronym: NA
What: Report published on CDT website to provide broader transparency and accountability in reporting government activities by state entities.
Link: https://cdt.ca.gov/security/policy/#Policy-Resources

Resource: **Summary of Required Information Technology Reports and Activities**
Acronym: SIMM 05-A
What: Outlines the reporting requirements that each state entity must adhere to when submitting reports and activities to CDT.
Link: https://cdt.ca.gov/wp-content/uploads/2017/03/SIMM_05A_Required_IT_Reports_and_Activities.pdf

Resource: **Government Code 11546.1**
Acronym: NA
What: Designates CDT to improve the governance and implementation of information technology by standardizing reporting relationships, roles, and responsibilities for setting information technology priorities.
Link: http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=11546.1.&lawCode=GOV

Resource: **Government Code 11546.2**
Acronym: NA
What: Instructs each entity to submit to CDT a summary of telecommunication and information security costs.
Link: http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=11546.2.&lawCode=GOV

Resource: **Government Code 11546.3**
Acronym: NA
What: Establishes responsibilities of the Chief Information Officer (CIO) for each state entity.
Link: http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=11546.3.&lawCode=GOV

ISO BASIC TRAINING RESOURCES LIST

INCIDENT MANAGEMENT

Resource: **California Compliance and Security Incident Reporting System**
Acronym: Cal-CSIRS
What: State policy requires state entities to make notification to OIS and the California Highway Patrol (CHP) immediately following discovery of an incident through Cal-CSIRS.
Link: https://calcsirs.rsam.com/default.aspx

Resource: **Cal-CSIRS Designee Request (Incident Management)**
Acronym: NA
What: Form to be submitted to OIS in order to designate Cal-CSIRS incident management users for your state entity.
Link: https://cdt.ca.gov/wp-content/uploads/2017/05/Cal-CSIRS_Designee-Request-Incident-Management.xlsx

Resource: **Malicious Code Analysis Platform Service**
Acronym: MCAP
What: Once account is created, you may login and upload the file for analysis at https://mcap.cisecurity.org/. Additional free education and awareness material provided at https://www.cisecurity.org/training/.
Contact: mcap@cisecurity.org

Resource: **DDoS System Vulnerability Testing**
Acronym: NA
What: The following websites will assist your state entity with conducting testing for systems vulnerable to DDoS.
Link: http://openresolverproject.org/ (Open Resolvers – DNS)
http://openntpproject.org/ (NTP)
http://openssdpproject.org/ (Simple Service Discovery Protocol)
http://opensnmpproject.org/ (SNMP)

Resource: **Department of Justice, Privacy Enforcement and Protection Unit**
Acronym: **NA**
What: This unit is tasked with enforcing state and federal privacy laws, empowering Californians with information on their rights and strategies for protecting their privacy, encouraging businesses to follow privacy-respectful best practices, and advising the Attorney General on privacy matters.
Link: www.privacy.ca.gov

Resource: **Multi-State Information Sharing and Analysis Center**
Acronym: MS-ISAC

ISO BASIC TRAINING RESOURCES LIST

What: Free services available to state, local, tribal and territorial governments to assist with malware analysis, computer forensics, network forensics, incident response, and onsite assistance.
Contact: 1-866-787-4722 or soc@msisac.org

Resource: **United States Computer Emergency Readiness Team**
Acronym: US-CERT
What: US-CERT strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world.
Link: http://www.us-cert.gov/

Resource: **FIRST**
Acronym: NA
What: FIRST is the global Forum for Incident Response and Security Teams.
Link: https://www.first.org/

Resource: **Escal Institute of Advanced Technologies**
Acronym: SANS Institute
What: Critical log review checklist for security incidents through the SANS – Incident Handling Reading Room.
Link: https://www.sans.org/reading-room/whitepapers/incident

Resource: **NIST (Incident Handling)**
Acronym: NIST
What: NIST SP subseries provide state entities with computer security incident handling guidelines, malware incident prevention and handling, and sample incident response exercises; referenced in SP 800-61, SP 800-83, and SP 800-84.
Link: http://csrc.nist.gov/publications/PubsSPs.html

Resource: **Homeland Security Information Network**
Acronym: HSIN
What: HSIN is the trusted network for United States Department of Homeland Security mission operations to share sensitive but unclassified information.
Link: https://www.dhs.gov/homeland-security-information-network-hsin

ISO BASIC TRAINING RESOURCES LIST

PRIVACY MANAGEMENT

Resource: **SAM 5310 through 5310.7**
Acronym: SAM 5310
What: SAM is a reference source to statewide management policy. IT – OIS policies for Privacy, specifically, can be found in Section 5310 through 5310.7.
Link: https://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5310.pdf

Resource: **Privacy Statement and Notices Standard**
Acronym: SIMM 5310-A
What: SIMM contains standards, instructions, forms and templates that State agencies must use to comply with IT policy. This SIMM is related to Privacy Policy Statements and Notices on Collections.
Link: https://cdt.ca.gov/wp-content/uploads/2017/02/SIMM5310_A.pdf

Resource: **Privacy Individual Access Standard**
Acronym: SIMM 5310-B
What: SIMM contains standards, instructions, forms and templates that State agencies must use to comply with IT policy. This SIMM is related to Privacy and the individual's access to their own personal information.
Link: https://cdt.ca.gov/wp-content/uploads/2017/02/SIMM5310_B.pdf

Resource: **Risk Management and Privacy Program Compliance Certification**
Acronym: SIMM 5330-B
What: This SIMM is a certification regarding compliance with all Risk Management and Privacy Program requirements in SAM 5300.
Link: https://cdt.ca.gov/wp-content/uploads/2017/02/SIMM5310_B.pdf

Resource: **Requirements to Respond to Incidents Involving a Breach of Personal Information**
Acronym: SIMM 5340-C
What: SIMM contains standards, instructions, forms and templates that State agencies must use in responding to an incident involving a breach of personal information
Link: https://cdt.ca.gov/wp-content/uploads/2017/02/SIMM-5340-A-Rev-05-2016.pdf

Resource: **Privacy Control Catalog, SP 800-53 Appendix J, Revision 4**
Acronym: Appendix J NIST 800-53 Rev 4
What: NIST publication and catalog of security controls which the State of California has adopted. Controls are based on the Fair Information

ISO BASIC TRAINING RESOURCES LIST

Practices Principles embodied in the Privacy Act of 1974 and other federal policies.

Link: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Resource: **Information Practices Act**
Acronym: IPA
What: The laws set forth in the Information Practices Act of 1977, Civil Code section 1798 et seq. are a set of California laws regarding privacy guarantees and limitations on the collection, use, maintenance, sharing and destruction of personal information.
Link: http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.&lawCode=CIV

Resource: **Health Information Portability and Accountability Act**
Acronym: HIPAA
What: Federal Laws regarding the privacy of health information.
Link: http://www.hhs.gov/ocr/privacy/

Resource: **Privacy Laws Listing**
Acronym: NA
What: The webpage on the California Office of the Attorney General provides contains links to some of the major privacy protection laws at the State and federal level.
Link: https://oag.ca.gov/privacy/privacy-laws

Resource: **HIPAA Privacy Rule**
Acronym: NA
What: The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.
Link: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

Resource: **California Public Records Act**
Acronym: PRA
What: The California Public Records Act signed into law in 1968 requiring inspection or disclosure of governmental records to the public upon request, unless exempted by law.
Link: http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=6251.&lawCode=GOV

ISO BASIC TRAINING RESOURCES LIST

RISK MANAGEMENT

Resource: **Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publication 199**
Acronym: FIPS 199
What: Publication which guides entities on how to properly categorize their information systems based on impact to an entity.
Link: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Resource: **Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53, Revision 4**
Acronym: NIST 800-53 Rev 4
What: NIST publication and catalog of security controls which the State of California has adopted. Controls are selected based off a system's categorization per the FIPS 199 process.
Link: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Resource: **Security Control Search**
Acronym: NIST 800-53
What: NIST searchable website which organizes and details out the security controls in the 800-53 SP.
Link: https://nvd.nist.gov/800-53/

Resource: **Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53, Revision 4**
Acronym: NIST 800-53 Rev 4
What: NIST publication and catalog of security controls which the State of California has adopted. Controls are selected based off a system's categorization per the FIPS 199 process.
Link: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Resource: **Guide for Developing Security Plans for Federal Information Systems, SP 800-18, Revision 1**
Acronym: NIST 800-18, Rev 1
What: Publication which guides entities on the process and structure of developing a system security plan.
Link: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

ISO BASIC TRAINING RESOURCES LIST

Resource: **Health Insurance Portability and Accountability Act of 1996**
Acronym: HIPAA
What: Federal law regarding the privacy and security of protected health information (PHI).
Link: https://www.hhs.gov/hipaa/for-professionals/index.html

Resource: **Payment Card Industry (PCI) Data Security Standard**
Acronym: PCI DSS
What: Security standards which governs the user or storage of payment card information.
Link: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

Resource: **Criminal Justice Information Services Security Policy**
Acronym: CJIS
What: The Federal Bureau of Investigation's policy on the use of Criminal Justice Information Services.
Link: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

TECHNOLOGY RECOVERY MANAGEMENT

State's Resources for Business Continuity and Technology Recovery Planning:

Resource: **Business Continuity Plan (BCP) with Technology Recovery Plan (TRP)**
Acronym: SAM 5325 - BCP and TRP Policy
What: Policy requirements for the state's Business Continuity with Technology Recovery Policy.
Link: https://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5325.pdf

Resource: **Technology Recovery Plan**
Acronym: SAM 5325.1 - TRP Policy
What: Policy requirements for the TRP Policy.
Link: https://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5325.1.pdf

Resource: **Technology Recovery Training**
Acronym: SAM 5325.2 - TRP Training Policy
What: Policy requirements for the Technology Recovery Training Policy.
Link: https://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5325.2.pdf

Resource: **Technology Recovery Testing**
Acronym: SAM 5325.3 - TRP Testing Policy

ISO BASIC TRAINING RESOURCES LIST

What: Policy requirements for the Technology Recovery Testing Policy.
Link: https://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5325.3.pdf

Resource: **Alternate Storage and Processing**
Acronym: SAM 5325.4 - TRP Alternate Storage and Processing Site Policy
What: Policy requirements for the Technology Recovery Alternate Storage and Processing Site Policy.
Link: https://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5325.4.pdf

Resource: **Technology Recovery Telecommunications Services**
Acronym: SAM 5325.5 - Telecommunications Services Policy
What: Policy requirements for the Technology Recovery Telecommunications services Policy.
Link: https://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5325.5.pdf

Resource: **Information System Backups**
Acronym: SAM 5325.6 - Backup Policy
What: Policy requirements for the Technology Recovery backup services.
Link: https://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5325.6pdf

Technology Recovery Plan Documents in SIMM:

Resource: **TRP Instructions**
Acronym: SIMM 5325-A
What: Detailed Instructions and guidance on the TRP content supporting SAM 5325 TRP.
Link: https://cdt.ca.gov/wp-content/uploads/2017/02/SIMM5325_A.pdf

Resource: **Technology Recovery Program Certification**
Acronym: SIMM 5325-B
What: Detailed Instructions and guidance on the TRP content supporting SAM 5325 TRP.
Link: https://cdt.ca.gov/security/policy/#Technology-Recovery-Management

Resource: **Schedule for Submission of Technology Recovery Plans**
Acronym: NA
What: State Policy, pursuant to SAM Section 5325.1, requires each agency to file a copy of its TRP with OIS in accordance to the TRP schedule.
Link: https://cdt.ca.gov/security/policy/schedule-for-submission-of-technology-recovery-plans/

ISO BASIC TRAINING RESOURCES LIST

Continuity Planning Resources:

Resource: **Governor's Office of Emergency Services' (CalOES) Continuity Planning**
Acronym: NA
What: Link to the CalOES's Continuity Planning resources
Link: http://www.caloes.ca.gov/cal-oes-divisions/planning-preparedness/continuity-planning

External Resources for Business Continuity and Technology Recovery Planning:

Resource: **NIST Special Publication 800-34 Rev.1**
Acronym: NA
What: NIST Contingency Planning guide for Federal Information Systems.
Link: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Resource: **Disaster Recovery Journal**
Acronym: DRJ
What: Excellent information resource dedicated to Business Continuity cause. The organization holds conferences, training, and webinars and publishes journal. Good information source.
Link: https://www.drj.com/about/editorial-advisory-board.html

Resource: **Disaster Recovery International**
Acronym: DRI
What: Excellent information resource dedicated to Business Continuity training and certification. The organization holds conferences, training and is a good source of information.
Link: https://www.drj.com/about/editorial-advisory-board.html

Resource: **Federal Emergency Management Agency**
Acronym: FEMA
What: Resource for Emergency Management training
Link: https://www.fema.gov/

TRAINING & OTHER RESOURCES

Resource: **Federal Virtual Training Environment**
Acronym: FedVTE
What: No cost online and on-demand cybersecurity training system available to state, local, tribal and territorial governments. Courses range from beginner to advanced levels and is accessible from most common web browsers.
Link: https://fedvte.usalearning.gov/

ISO BASIC TRAINING RESOURCES LIST

Resource: **Inter-Agency Security Group**
Acronym: NA
What: Comprised of state employees (only) whose job duties deal directly or indirectly with information security.
Contact: Helen Woodman at (916) 431-4698 or helen.woodman@state.ca.gov

Resource: **Software Engineering Institute/Carnegie Mellon University**
Acronym: NA
What: Papers on Incident Management
Link: http://resources.sei.cmu.edu/library/results.cfm?as_q=inmeta:gsataxonomyoutput~Incident%20Management

Resource: **Stay Safe Online/National Cyber Security Alliance**
Acronym: NA
What: Free education and awareness material.
Link: https://staysafeonline.org/

Resource: **Texas A&M Engineering Extension Service**
Acronym: NA
What: Free online courses.
Choose Course Option: Cybersecurity

CYB101 - Cybersecurity for Everyone – Non-Technical
- AWR-168-W Cyber Law and White Collar Crime
- AWR-174-W Cyber Ethics
- AWR-175-W Information Security for Everyone

CYB201 - Cybersecurity for IT Professionals - Technical
- AWR-138-W Network Assurance
- AWR-139-W Digital Forensics Basics
- AWR-173-W Information Security Basics
- AWR-178-W Secure Software

CYB301 - Cybersecurity for Business Professionals/Managers
- AWR-169-W Cyber Incident Analysis and Response
- AWR-176-W Business Information Continuity
- AWR-177-W Information Risk Management

Link: https://teex.org/Pages/Program.aspx?catID=231&courseTitle=Cybersecurity