Attachment 17

Risk Assessment Policy - ITAM-0625

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	RISK ASSESSMENT POLICY	ITEM NUMBER:	ITAM-0625
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/20YY
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/20YY
VERSION:	1.0	PAGE:	PAGE **1** OF **5**

I. Purpose

To ensure that County Information Technology (IT) performs risk assessments in compliance with County IT security policies, standards, and procedures.

II. Audience

The primary audience for this policy is Information Technology Professionals (County executives, managers, employees, contractors, vendors, and third parties) whose responsibilities including managing, administering, and operating County networks or systems.

III. Scope

This policy applies to any Information System that electronically generates, receives, stores, processes or transmits County-owned data, whether the system is hosted on the County network or by a third-party provider. Additionally, these provisions apply to anyone doing business as the County and/or in support of the County that is provisioned access to County Networks or systems. This includes employees, contractors, consultants, temporaries, and other workers at the County, including all personnel affiliated with third parties, collectively referred to hereafter as “agents”.

IV. Definitions

See ITAM-0602, Glossary of Definitions

V. Policy

It is the policy of the County Board of Supervisors that:

Risk Management refers to the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. A risk management program is an essential management function and is critical for any department to successfully implement and maintain an acceptable level of security. A risk management process must be implemented to assess the acceptable risk to department IT systems as part of a risk-based approach used to determine adequate security for their systems. Proper risk management requires steps to be taken to reduce the risk level to an acceptable level. These steps include the initial assessment, risk mitigation and evaluation.

Risk assessment is the first process of risk management. Departments must use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its System Development Life Cycle (SDLC). The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. NIST SP 800-30 (R1) Guide for Conducting Risk Assessments provides guidance for carrying out each of the steps in the risk assessment process, such as planning, executing, communicating results, and maintaining the assessment.

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Controls are defined as IT processes and technologies designed to close vulnerabilities, maintain continuity of operation at specified performance levels, and achieve and document compliance with policy requirements. The controls presented in this section are designed to mitigate risks and are required to comply with this policy.

The third process of risk management, evaluation, is ongoing and evolving. Evaluation emphasizes the good practice to develop an effective risk management program within the department's information security program. Not only should the risk management program drive changes to existing systems, but it should also integrate into the department's operational functions, as well as the SDLC for new systems and applications. The following outlines the minimum security control requirements which all information systems must adhere to in order to operate in a production environment:

1. SECURITY CATEGORIZATION

   County IT or Departmental IT shall:

   a. Apply proper security controls to data categorized as confidential by system owners, including Protected Health Information (PHI) and Personally Identifiable Information (PII), in accordance with applicable federal and state laws, directives, policies, regulations, standards, and guidance.

   b. Document the security controls (including supporting rationale) in the security plan for the information system.

2. RISK ASSESSMENT

   County IT or Departmental IT shall:

   a. Conduct (or have conducted by a qualified third-party) an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

   b. Document risk assessment results in annual IT Risk Assessment.

   c. Review risk assessment results quarterly.

   d. Disseminate risk assessment results to stakeholders.

   e. Update the risk assessment quarterly or whenever there are significant changes to the information system or environment of operation (including the

identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

3. VULNERABILITY SCANNING

County IT or Departmental IT shall:

a. Scan for vulnerabilities in the information system and hosted applications as frequently as possible given the existing tools and support services available and/or randomly and when new vulnerabilities potentially affecting the system/applications are identified and reported.

b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

i. Enumerating platforms, software flaws, and improper configurations.

ii. Formatting checklists and test procedures.

iii. Measuring vulnerability impact.

c. Analyze vulnerability scan reports and results from security control assessments.

d. Remediate legitimate vulnerabilities within one month in accordance with an organizational assessment of risk.

e. Share information obtained from the vulnerability scanning process and security control assessments with the “Chief Information Officer” or their equivalent to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

f. Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

g. Update the information system vulnerabilities scanned monthly, prior to a new scan, or when new vulnerabilities are identified and reported.

h. Ensure that information systems implement privileged access authorization to all systems for selected vulnerability scanning.

VI. Exceptions

See ITAM-0600, IT Security Program

VII. Non-Compliance

See ITAM-0600, IT Security Program

VIII. References and Sources

1. Applicable Rules, Laws, and Regulations:

   a. National Institute of Standards and Technology (NIST) Special Publications (SP):

      iv. NIST SP 800-53a – Risk Assessment (RA)

      v. NIST SP 800-12

      vi. NIST SP 800-30

      vii. NIST SP 800-39

      viii. NIST SP 800-40

      ix. NIST SP 800-60

      x. NIST SP 800-70

      xi. NIST SP 800-100

      xii. NIST SP 800-115

   b. NIST Federal Information Processing Standards (FIPS) 199.

   c. State of California State Administrative Manual (SAM) 5300 et seq.

   d. Statewide Information Management Manual (SIMM) et seq.

2. Related Policies:

3. Referenced Documents:

4. Revision History:

VERSION	CHANGE	AUTHOR	DATE OF CHANGE
1.0	Initial Release	CISO/Policy Committee	08/25/2021