
	PINAL COUNTY Information Security Risk Management		
	DATE: 02/03/2021 REVISED:	PAGES: 11	POLICY NUMBER: 11.010

Information Security Risk Management Standard

Table of contents

PURPOSE	1
AUTHORITY	2
SCOPE	2
RESPONSIBILITY	2
COMPLIANCE	2
STANDARD STATEMENTS	3
Information Security Risk Management	3
Information Security Training and Awareness	8
CONTROL MAPPING	9
DOCUMENT CHANGE CONTROL	10

1. PURPOSE

	PINAL COUNTY Information Security Risk Management		
	DATE: 02/03/2021 REVISED:	PAGES: 11	POLICY NUMBER: 11.010

1.1. **Information Security Risk Management Standard** — The purpose of this standard is to define the key elements of the county’s information security risk assessment model to enable consistent identification, evaluation, response and monitoring of risks facing IT processes. IT processes will be identified, evaluated and continuously improved as needed to protect the county’s assets and business continuity.

2. AUTHORITY

2.1. Pinal County provides that “Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all departments and offices shall adhere to the policies, procedures and objectives established by the Information Security Department with respect to activities concerning information technology.”

3. SCOPE


3.1. This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of the county. The document applies to all departments including boards, commissions, divisions, councils, bureaus, offices and vendors. Other county entities that voluntarily use or participate in services provided by the Information Technology Department, such as Pinalcountyaz.gov, must agree to comply with this document, with respect to those services, as a condition of use. All departments and offices are required to implement procedures that ensure their personnel comply with the requirements herein to safeguard information.

4. RESPONSIBILITY

- 4.1 The Information Security Department is responsible for the development and ongoing maintenance of this standard.
- 4.2 The Information Security Department is responsible for this standard and may enlist other departments to assist in the monitoring and maintenance of compliance with this standard.
- 4.3 Any inquiries or comments regarding this standard shall be submitted to the Information Security Department by sending an email to [mailto: ITSecurity@Pinal.gov](mailto:ITSecurity@Pinal.gov).
- 4.4 Additional information regarding this standard may be found at <https://www.pinalcountyaz.gov/HR/Pages/PoliciesProceduresRules.aspx>.

5. COMPLIANCE

5.1. Compliance with this document is mandatory for all departments and offices including all boards, commissions, divisions, councils, bureaus, offices and vendors. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the county. Exceptions to any part of this document must be requested via email to the Information Security Department(<mailto:ITSecurity@Pinal.gov>). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the County Chief Information Security Officer (CISO).

	PINAL COUNTY Information Security Risk Management		
	DATE: 02/03/2021 REVISED:	PAGES: 11	POLICY NUMBER: 11.010

6. STANDARD STATEMENTS

6.1. Information Security Risk Management

Information security risks that could compromise the confidentiality, integrity or availability of the county's IT processes shall be identified, analyzed and mitigated to an acceptable level to meet organizational objectives and compliance requirements. The steps involved in creating information security risk management standards are as follows:

6.1.1 Risk identification

The objective of risk identification is to produce a comprehensive list of risks that could impact the county.

6.1.1.1. The Risk Management department shall develop a Process, Risk and Control framework. The framework will incorporate IT processes, risks and common control objectives mapped to authoritative sources, applicable regulatory requirements and county controls.

6.1.1.2. The county must establish process owners to support the risk assessment process and to determine the appropriate risk treatment.

6.1.2 Information security risk assessments

Information Security risk assessments aid in identifying key Information Security risks within the county environment and how these Information Security risks may affect the county's ability to achieve the overall organizational objectives.

6.1.2.1. Information security risk assessments must be conducted on an annual basis and the results reported to the IT Security Department. The report, targeting all County Offices and departments, shall include identified risk levels to the standard set of IT processes, new risks identified and status of risk remediation efforts underway to reduce the risks to an acceptable level.

6.1.2.2. County Offices and Departments must implement a risk-based management process that weighs a potential risk's impact and likelihood against the organizational resource cost of mitigating or minimizing the risk to an acceptable level.

6.1.3 Information security risk assessment model

County Offices and Departments must consider the likelihood and impact when evaluating risks to county IT processes. As a part of the risk assessment process, county Offices and Departments will evaluate both the inherent and residual risks to their IT processes.

The risk level is determined using ratings for impact and likelihood.

6.1.3.1 Impact

6.1.3.1.1 County Offices and Departments must ensure that process owners will be assigned to each IT process and will be responsible for determining the impact of the identified risk.

6.1.3.1.2 Impact categories and definition: The impact of a risk is based on the financial, reputational, legal and regulatory, and operational impact which a risk may have if realized against a specific IT process. Impact categories include:

Impact Categories	Definition
Financial	Financial impact to the county based upon a risk being realized.
Reputational	Impact of a loss of confidence from its personnel, constituents, business partners and regulators, which would degrade the county's reputation.
Legal and regulatory	Impact could result in exposure to liability, enforcement, observations, recommendations and/or comments from other county entities and/or federal oversight departments and/or regulators, or violations of contracts with third parties.
Operational	The operational impact to processes, people and technology in which the county employs to achieve its strategy and normal business operations.

6.1.3.1.3 Impact criteria: The IT Security department shall develop an impact criteria to align to each impact category based upon the below risk scale.

Impact Rating	Impact Measurement
Critical	4
High	3
Moderate	2
Low	1

6.1.3.2 Likelihood

6.1.3.2.1 A Process Owner must be assigned to each IT process and will be responsible for determining the likelihood of occurrence of the identified risk.

6.1.3.2.2 The Process Owner will determine Inherent Likelihood by taking into consideration the likely exposure to a risk in the absence of controls.

6.1.3.2.3 Likelihood Rating and Measurement: Likelihood rating is the probability of a risk occurring over a predefined time period.

Below are the qualitative criteria used for assessing the likelihood of a risk occurring:

Likelihood Rating	Likelihood Measurement	Description
Highly Likely	4	Greater than 75% chance of the risk occurring.
Likely	3	The chance of the risk occurring is greater than 50% and less than/equal to 75%
Possible	2	The chance of the risk occurring is greater than 25% and less than/equal to 50%
Unlikely	1	The chance of the risk occurring is less than/equal to 25%

6.1.4 Control effectiveness

6.1.4.1 Control effectiveness is a measure of how effective a control is at meeting the control objective within the county's IT environment. This measurement is leveraged to determine the reduction of inherent likelihood to residual likelihood.

6.1.4.2 Control effectiveness is determined by the control owner based upon the effectiveness of the control to meet its intended control objective and minimize the likelihood of a risk to be realized.

6.1.4.3 Control effectiveness rating:

Control Effectiveness Rating	Control Effectiveness Measurement	Description
Effective	1	Mitigating controls substantially prevent exploitation of the vulnerability or limit the scope of impact to a low level.
Partially Effective	2	Mitigating controls prevent most cases of exploitation of the vulnerability or limit the scope of impact to a moderate level.
Ineffective	3	Mitigating controls do not substantially prevent exploitation of the vulnerability, nor do they effectively limit the scope of impact of exploitation.

6.1.5 Calculation of risk

The level of risk to a process is based on the likelihood of a risk being realized and the severity of the impact that the risk would present to the county's IT systems.

6.1.5.1 Inherent risk factor: Inherent risk is the impact and likelihood of a risk to be realized in absence of controls. An inherent risk can be calculated by the following calculation: Impact * Likelihood = Inherent risk.

6.1.5.2 Residual *risk* factor: Using the impact, likelihood and control effectiveness rating, the residual *risk* can be determined as follows: $\text{Impact} * (\text{Likelihood} * \text{Control effectiveness reduction}) = \text{Residual risk}$.

6.1.5.2.1 Control effectiveness reduction can be derived from the below table.

Control Effectiveness Rating	Control Effectiveness Measurement	Reduction in Likelihood Rating
Effective	1	50%
Partially Effective	2	25%
Ineffective	3	0%

6.1.6 Risk response


The Risk Response or Risk Treatment Plan is prepared after the inherent risk is calculated and prioritized to determine if treatment is needed to manage the risk to an acceptable level. Treatment approaches include accepting the risk, mitigating the risk by applying controls, transferring the risk or avoiding the risk.

6.1.6.1 Risk acceptance: county offices and departments shall identify the level of risk that the organization is willing to accept while prioritizing to pursue strategic objectives and risk mitigation/approach.

6.1.6.1.1 County offices and departments must ensure that risk tolerance is defined at an agency level while taking into consideration the organizational impact and likelihood for the various types of risks (e.g., financial, safety, compliance or reputation).

6.1.6.1.2 The IT Security Department will have final say on whether an established risk tolerance is acceptable to the county as an organization. This determination shall be informed by the organizations role in critical infrastructure and its sector of function.

6.1.6.1.3 Residual acceptance and tolerance: county offices and departments must ensure that the Process Owner shall be made aware of any residual risks, which are deemed “Critical” or “High”.. The IT Security department shall provide recommendations to reduce the risk to a reasonable and appropriate level. If the Process Owner fails to observe IT Security team’s recommendation or implements alternate mitigating controls, County Offices and Departments must ensure that the Process Owner is accountable and must sign off that they accept the residual risk to their agency.

	PINAL COUNTY Information Security Risk Management		
	DATE: 02/03/2021 REVISED:	PAGES: 11	POLICY NUMBER: 11.010

6.1.6.1.4 The IT Security Department must be informed and approve risk acceptance of any “Critical” or “High” residual risks.

6.1.6.2 Risk mitigation: The IT risk has been acknowledged and corrective action will be implemented to mitigate or reduce the IT risk.

6.1.6.2.1 Identify mitigating controls: County Offices and Departments must ensure that the Process Owner, in coordination with the IT Security Department, must identify and propose the implementation of supplemental controls to reduce or eliminate the risk to county processes commensurate with the impact and determined residual risk. Control types shall include:

6.1.6.2.1.1 Preventive — prevents the risk by reducing the likelihood of a threat exploiting vulnerabilities.

6.1.6.2.1.2 Detective — monitors and/or alerts on success factors to stem further losses.

6.1.6.2.2 Develop a remediation plan: For residual risks that are unacceptable to the organization, County Offices and Departments must ensure that the Process Owner must develop a remediation plan in coordination with the IT Security Department.

6.1.6.2.3 The remediation plan must be approved by the IT Security Department.

6.1.6.3 Risk transfer: The IT risk has been acknowledged and the IT risk is insured across the organization.

6.1.6.4 Risk avoidance: The IT risk is avoided entirely and the organization ceases to perform the activity/activities that causes the IT risk to materialize.

6.1.7 Risk reporting

County offices and departments must ensure that the IT Security Department in collaboration with the Process Owner(s) shall produce a risk assessment report to provide necessary information to the IT Security team, including:

6.1.7.1 Overall Executive dashboard that depicts the critical IT residual risks, management’s response and the associated action plan(s).

6.1.7.2 Recommended changes listed by priority, with approximate levels of effort/cost to implement.

6.1.7.3 IT Risk response actions — e.g., by division, Inherent Risk rating, by Residual Risk rating, etc.

6.1.7.4 Trending of IT risk assessment results — e.g., comparison of previous IT risk assessment results vs. current IT risk assessment results to:

6.1.7.4.1. Determine changes in Inherent Risk and Residual Risk ratings.

6.1.7.4.2. Use IT risk criteria/attributes to help prioritize and determine how often to conduct the IT risk assessments.

6.1.7.5 Level of residual risk that would remain after the recommended changes are implemented.

At a minimum, all IS risks rated as “Critical” and “High” must be reported to the IT Security team. The risk ratings shall be expressed using the following levels:

Residual Risk		Likelihood			
		Highly Likely (4)	Likely (3)	Possible (2)	Unlikely (1)
Impact	Critical (4)	Critical (16)	Critical (12)	High (8)	Moderate (4)
	High (3)	Critical (12)	High (9)	Moderate (6)	Low (3)
	Moderate (2)	High (8)	Moderate (6)	Moderate (4)	Low (2)
	Low (1)	Moderate (4)	Low (3)	Low (2)	Low (1)


6.2. Information Security Training and Awareness

The objective of the county information security training is to educate users on their responsibility to help protect the confidentiality, availability and integrity of the county’s information assets. County Offices and Departments must ensure that all personnel are trained on all relevant rules and regulations for cybersecurity.

6.2.1 Implement an enterprise-wide information security awareness and training program.

6.2.1.1 Develop appropriate training materials in collaboration with Human Resources and Legal based on the users role and position in the organization (*i.e.* Executive training should be focused on the executive roles and involvement).

6.2.1.2 Conduct periodic refresher training for personnel and, where relevant, contractors and temporary staff.

	PINAL COUNTY Information Security Risk Management		
	DATE: 02/03/2021 REVISED:	PAGES: 11	POLICY NUMBER: 11.010

6.2.1.3 The training shall:

- 6.2.1.3.1 Explain acceptable use of information technology.
- 6.2.1.3.2 Inform personnel about relevant policies and standards.
- 6.2.1.3.3 Detail each individual’s accountability for each of the provisions of all policies and the underlying procedures based on their role in the organization.
- 6.2.1.3.4 Test each individual’s understanding of all policies and of his or her role in maintaining the highest ethical standards.
- 6.2.3.5. Include physical security responsibilities and standards

6.2.2 Initial education and training applies to personnel who transfer to new positions or roles with substantially different information security requirements, not just to new starters, and should take place before the role becomes active.

6.2.3 New Hire Security Awareness Training: All new personnel must complete an Initial Security Awareness Training course. This course shall be conducted via web-based learning or in class training and shall be included in the new hire orientation checklist. The New Hire Security Awareness course must be completed within 6 months of new hire orientation.

6.2.4 Annual Security Awareness Training: All personnel will be required to complete Annual Security Awareness Training. Once implemented, automatic email reminders will be sent to personnel 12 months after course completion, alerting personnel to annual refresher training completion deadlines.

6.2.5 The awareness program shall be updated regularly by the Information Security Department so that it stays in line with organizational policies and procedures, and shall be built on lessons learned from information security incidents.

6.2.6 Ensure that all principles, policies, procedures and training materials are accessible by all personnel as appropriate.

6.2.7 All county personnel must complete the annual information security training. completion rates will be tracked and reported to personnel managers and IS leadership.

6.2.8. The awareness program will contain testing campaigns and security bulletins periodically to remind users of best practices and procedures that will address issues that they may encounter.

7. CONTROL MAPPING

This chart is used to provide an efficient way to cross-reference this policy’s components with the different industry standard information security controls.



Section	NIST SP800-53 R4 (1)	CIS 20 v6	NIST CSF
6.1 Information Security Risk Management	RA-1	-	ID.GV-1
	RA-2	-	ID.AM-5
	RA-3	CSC 4	ID.RA-1
	CA-1	-	ID.GV-1
	RA-5	CSC 4	ID.RA-1
	CA-5	-	-
	CA-6	-	-
	PM-4	-	ID.RA-6
	PM-9	-	ID.GV-4
	PM-12	-	ID.RA-3
	SI-2	CSC 4	ID.RA-1
	SI-4	CSC 4	ID.RA-1
	SI-5	CSC 4	ID.RA-1
	CA-2	CSC 4	ID.RA-1
	CA-7	CSC 4	ID.RA-1
		CSC 4	ID.RA-2
		-	ID.RA-4
		-	ID.RA-5
	-	ID.RM-1	
	-	ID.RM-2	
	-	ID.RM-3	
	RA-4	-	-
6.2 Information Security Training and Awareness	AT-1	-	ID.GV-1
	AT-4	-	-
	AT-5	-	-
	PM-16	CSC 4	ID.RA-2
	PM-14	CSC 19	PR.IP-10
	PM-16	CSC 4	ID.RA-2

8. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
1.0	Jerry Keely	08/26/2020	Approved by Board of Supervisors
1.1	Chris Bracken	02/03/2021	Added Section 6.2.8 Regarding Phishing Testing



PINAL COUNTY
Enriching Lives Beyond Expectation

PINAL COUNTY
Information Security Risk Management

DATE: 02/03/2021	PAGES: 11	POLICY NUMBER: 11.010
REVISED:		