Compliance Component

DEFINITION	
Name	Risk Assessment
Description	Risk Assessment is the first step of the risk management process. The assessment identifies high impact assets, potential threats, and recommended controls.
Rationale	Risk Assessments identify the assets and recommend appropriate controls (controls or risk-reducing measures) for reducing or eliminating risk.
Benefits	• Helps to identify appropriate controls to reduce or eliminate risk which are implemented in Risk Mitigation • This allows agencies to make well-informed decisions to justify expenditures for Risk Mitigation, the second step for risk management.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Management Controls
List the Technology Area Name	Security Risk Management
List Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	

State the Guideline, Standard or Legislation	A Risk Assessment encompasses 8 steps
	• Step 1 - System Identification
	  • Define what comprises the system
	  o Define all critical data that needs to be protected
	  o Determine all software, hardware, etc. that handle it
	  o Include all input/output devices and networks
	Output from Step 1 – A diagram of the IT system environment and boundaries
	• Step 2 - Threat Identification
	  • Compile a list of the potential threats applicable to the specific system being evaluated
	  o A threat is any circumstance or event with the potential to cause harm to an IT system. Threats can be natural, human, or environmental
	  o Common threats include, but are not limited to:

- Fire
- Lightning
- Tornado
- Earthquake
- Ice
- Flood
- Theft/embezzlement/fraud/compromise
- Bomb threat
- Sabotage/alteration of data
- Denial of service
- User error
- Unauthorized access
- Misappropriation of services

- The list of potential threats should be tailored to the individual agency and its processing environment

Output from Step 2 – A list of threats that could exploit system vulnerabilities

- Step 3 - Threat Probability
  - For each asset, create a separate matrix and assign one of the below probability values to each threat:
    - Low = 0.1
    - Low to Medium = 0.4
    - Medium = 0.6
    - Medium to High = 0.8
    - High = 1.0

  Output from Step 3 - A matrix, such as the sample in Table 1 below, for each asset from Step 1, with a column assigning a Probability value to each potential threat

- Step 4 - Loss Impact
  - Loss Impact is the magnitude of harm to an agency mission that could be caused by a threat exploiting a vulnerability. The level of impact is governed by the potential mission impact and in turn produces a relative value for the IT assets and resources affected

  - For each threat to the asset, estimate the impact of the loss as if no controls were in place. Use the following number system:
    - Low = 1
    - Low to Medium = 3
    - Medium = 5
    - Medium to High = 7
    - High = 10

  - Loss Impact should take into consideration such things as:
    - loss of life or physical injury
    - public confidence and credibility
    - confidentiality and privacy requirements
    - criticality of the system to the agency mission
    - loss of tangible assets or resources

Output from Step 4 - A matrix, such as the sample in Table 1 below, for each asset from Step 1, with a column assigning a Loss Impact value to each potential threat

- Step 5 - Risk Factor
    - Determine Risk Factor by multiplying the Threat Probability and Loss Impact values for each threat. Risk Factors will vary between 0 and 10

  Output from Step 5 - A matrix, such as the sample in Table 1 below, for each asset from Step 1, with a column assigning a Risk Factor value to each potential threat

- Step 6 - Controls
    - List the Controls (safeguards) that are in place or could be put in place to reduce either the threat probability or loss impact.
        - Controls may be technical and/or non-technical
            - Technical controls are incorporated into computer hardware, software, or firmware
            - Non-technical controls are management and operational controls, such as policies and procedures
        - Controls may also be preventive and/or detective
            - Preventive controls inhibit attempts to violate security policy, e.g., access control enforcement, encryption, and authentication
            - Detective controls warn of violations or attempted violations of security policy, e.g., audit trails, intrusion detection methods, and checksums
    - List the cost of each control

  Output from Step 6 – A matrix, such as the sample in Table 1 below, for each asset from Step 1, with a column listing current or possible Controls, and a column listing the Control Cost for each

Applicable Threat	Threat Probability	Loss Impact	Risk Factor	Controls	Control Cost
Fire	0.1	10	1.0	Fire extinguisher	$20
Denial of Service	0.1	5	0.5	Firewall	$0
Theft	0.8	10	8.0	• Locking cable • Anti-theft software	$25 $40
User Error	1.0	3	3.0	Training	$70

Table 1 -- Laptops (Sample Asset Matrix)

- Step 7 - Control Recommendations
    - From the list of controls, select those which reduce the risk factor to an acceptable level. Consider such variables as:
        - Legislation and regulation requirements
        - Effectiveness (e.g., system compatibility)

	o Operational impact o Safety o Reliability o Organizational policy • For the recommended controls selected, conduct a cost-benefit analysis to demonstrate that the costs of implementation can be justified by the reduction in risk Output from Step 7 -- A list of Recommended Controls to mitigate risk • Step 8 - Documentation • The results from each step of the Risk Assessment should be documented in an official report Output from Step 8 -- A Risk Assessment Report that defines the IT system and its assets, lists potential threats, their respective risk factors to each asset, the potential controls and their costs, along with a list of recommended controls • The Risk Assessment Report is used in the Risk Mitigation phase of the Security Risk Management process
Document Source Reference #	NIST SP 800-18 and SP 800-30 www.csrc.nist.gov/publications/nistpubs) CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/); Peltier, Thomas R. (2001). *Information Security Risk Analysis*. Boca Raton, FL: CRC Press LLC.

Standard Organization			
Name	Carnegie Mellon University, CERT/Coordination Center (CERT/CC)	*Website*	www.cert.org
Contact Information	cert@cert.org		

Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		

KEYWORDS	
List all Keywords	Control, safeguard, mitigation, threat, impact, vulnerability, cost-benefit, ROI

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*

Rationale for Component Classification	
Document the Rationale for Component Classification	

Conditional Use Restrictions			
Document the Conditional Use Restrictions			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	03/09/2006	*Date Accepted / Rejected*	03/14/2006
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			