INFORMATION TECHNOLOGY SERVICES

INFORMATION RISK MANAGEMENT PROGRAM

Developing a Unit Risk Management Program

Information Security & Privacy Office

June 8, 2017

Version 1.5.7

Risk Management at Florida State University

Risk assessments should identify functions, activities, products, and services and their relative importance to the university unit. Units should also evaluate the inherent cybersecurity risk presented by the people, processes, technology, and information that support the identified function, activity, product, or service and assess the existence and effectiveness of controls to protect against the identified risk. Thus, risk assessments can provide the basis for the selection of appropriate controls and the development of remediation plans so that risks and vulnerabilities are reduced to a reasonable and appropriate level.

***FSU Phase 1*:** The risk management strategy for ISPO is concentrating on assisting units in completing steps 1 through 3 during the 2016/2017 engagements:

Step 1, your team will: (1) inventory and document the location of all information assets; (2) determine the strategic value of such assets; (3) classify the assets using FSU's information classification guidelines; (4) assign risk levels to the assets (See Appendix B). This information will be reported with your teams Risk Assessment Submission. ISPO has provided a template spreadsheet to use for this reporting.

Step 2 requires mapping physical and logical controls to the information items identified in Step 1 after determining a risk mitigation strategy for each item.

Step 3 is the implementation of the security controls and documenting how the controls are deployed within the information system and environment of operation

***FSU Phase 2*:** The ISPO risk management team will assist university units to complete the risk management framework steps 4 through 6

Step 4 is the assessment of the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Step 5 is approving the information systems/datasets identified in step one and moving it into a production environment based upon a determination of the risk to the university resulting from the operation of the information system and the decision on how to manage that risk.

Step 6 is monitoring and assessing selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials including the Unit Privacy Coordinator.

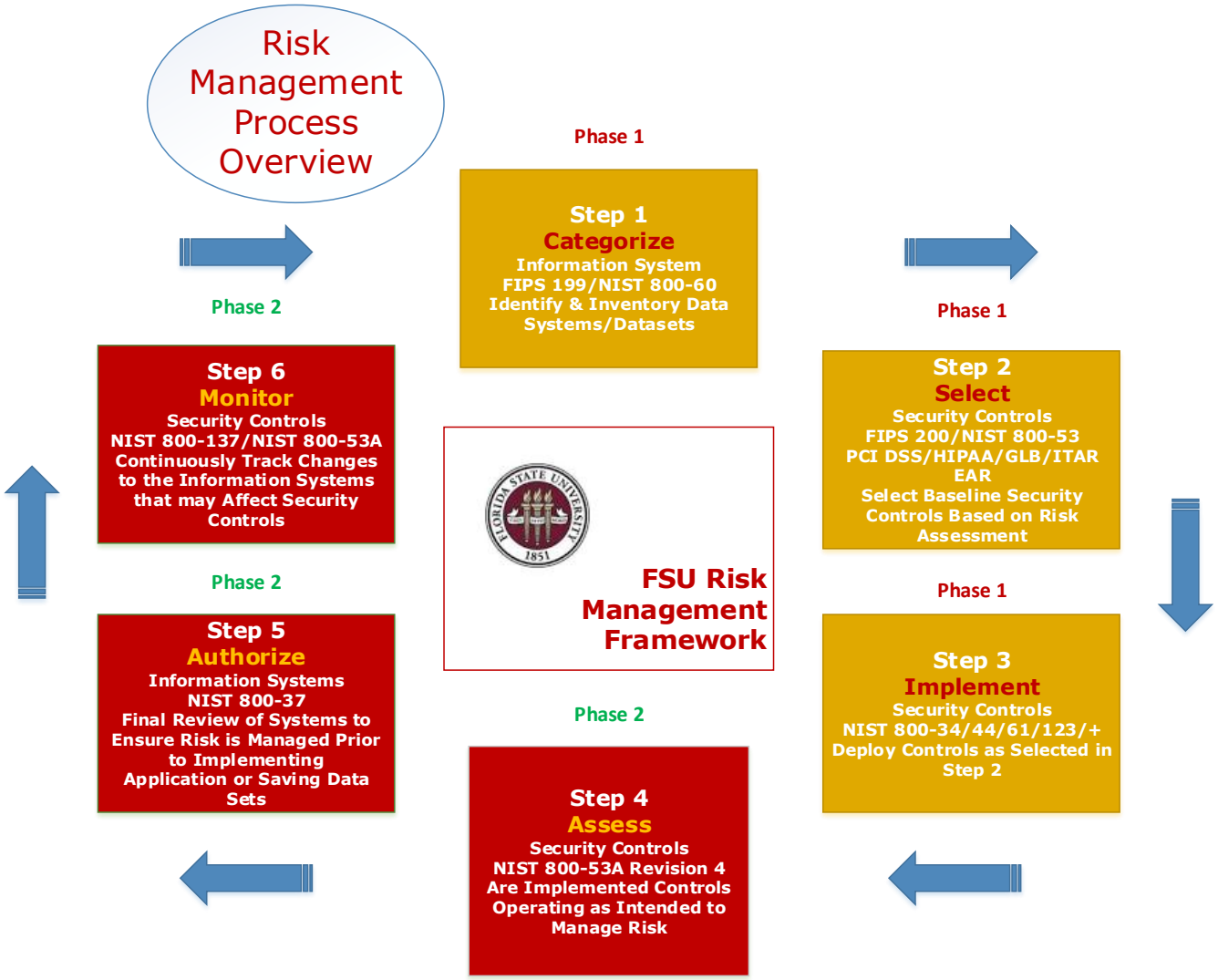
NOTE: Some units must have a full risk management program (Steps 1-6) in place to meet contracted compliance requirements including DFARS 252.204-7008/7012 and the NIST 800-171, FAR 52.204-21, FISMA Moderate/High, and legal requirements in HIPAA or GLBA.

The ***Risk Management Process*** follows and a ***Glossary of Terms*** (Appendix A) is included on the following pages to provide information to assist you with this effort.

The Risk Management Process

FSU has chosen to follow the NIST risk management framework. The framework is illustrated in Figure 1. See Appendix C for supporting reference documentation for each step.

Fig.1 FSU/NIST Risk Management Framework



FSU Phase 1

Step 1: Classification of Information Systems

TASK 1-1: Identify and categorize your data/information and supporting systems. Document the results of the security categorization in the ISPO provided inventory sheet.

Primary Responsibility: Information Owners; Data/Information Custodian.

Supporting Roles: Unit Privacy Coordinator; Information Security Manager; Data Owner; Information Security and Privacy Office Risk Manager.

Data Discovery Tools:

RPT Policy Privacy Tester: This application scans publicly facing unit websites, intranets, or unit SharePoint sites for protected or private informattion. The scan will determine if protected or private information is presented to public access without proper authorization/authentication controls. RPT will also assess an forms used to collect informaiton to ensure encryption is used to protect data transmissions.

IdentityFinder: IdentityFinder is a Data-at-Rest data discovery tool. The software quickly and effectively scans endpoints, servers, databases for sensitive data – data that can be anywhere and that most units do not even know still exists. With a number of configurations options, Beyond identification, the application also offers remediation capabilities to clean protected or private data discovered on unauthorized computing devices. This application is currently in a pilot phase by ISPO. We have limited seats available for units to become familiar with the application.

TASK 1-2: Describe the information system, document the description, and assign a risk level (see Appendix B) in the ISPO provided inventory sheet.

Primary Responsibility: Information Owners; Data/Information Custodian.

Supporting Roles: Data Owner, Unit Privacy Coordinator; Information Security Manager; Dean, Director, or Department Head; Information Security and Privacy Office Risk Manager.

Step 2. Select Security Controls

TASK 2-1: Identify specific controls that are currently in place or identified for addition to meet your risk mitigation strategy (See Appendix C for an example). You can engage ISPO Risk Management staff to assist in assigning specific controls to found data sets and systems. ISPO will defer to following engagements to assist you in mapping all pertinent NIST 800-53 controls for each identified application or data set to meet framework requirements. There are 17 control areas defined in NIST 800-53. The areas are closely

aligned with the minimum security requirements for information systems published in FIPS Publication 200 Minimum Security Requirements for Federal Information Systems and Operations.

AC - Access Control
AU - Audit and Accountability
AT - Awareness and Training
CM - Configuration Management
CP - Contingency Planning
IA - Identification and Authentication
IR - Incident Response
MA - Maintenance
MP - Media Protection
PS - Personnel Security
PE - Physical and Environmental Protection
PL - Planning
PM - Program Management
RA - Risk Assessment
CA - Security Assessment and Authorization
SC - System and Communications Protection
SI - System and Information Integrity
SA - System and Services Acquisition

Each family member above links to a list of sub controls.

The link below maps the 17 families of controls to a baseline of controls for systems identified by you as low, moderate, and high risk:

Minimum Security Controls
High-Impact Baseline
Moderate-Impact Baseline
Low-Impact Baseline

Primary Responsibility: Data/Information Custodians; Information Owner.

Supporting Roles: Unit Privacy Coordinator; Data Owner; Information Security and Privacy Office Risk Manager.

Step 3. Implement Security Controls

TASK 3-1: Develop a strategy to implement the security controls specified in Task 2 into your production environment. The controls were documented in the ISPO provided inventory sheet during Step 2.

Primary Responsibility: Information Owner or Data/Information Custodian.

Supporting Roles: Information Security Manager; Data Owner; Information Security and Privacy Office Risk Manager.

FSU Phase 2

Step 4. Assess Security Control Effectiveness

***TASK 4-1*:** Assess the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. ISPO supports multiple tools to monitor the effectiveness of security controls including:

Device Security Vulnerability Assessment

Nexpose: A vulnerability assessment tool capable of scanning endpoints, servers, and network devices to assess services and security patch levels of devices.

Primary Responsibility: Informtion Security Manager.

Supporting Roles: Authorizing Official or Designated Representative; Chief Information Officer; Senior Information Security Officer; Information System Owner or Common Control Provider; Information Owner/Steward; Information System Security Officer.

TASK 4-2: Prepare the risk mitigation documenation to detail the issues, findings, and recommendations from the security control assessment. Assess the security of the controls identitied in step 2 and implemented in step 3. Management periodically should review, or gain assistance in reviewing, security/privacy control activites to determine their continued relevance, and refresh them when necessary.

Primary Responsibility: Information Security Manager.

Supporting Roles: Information Security Manager, Unit Privacy Coordinator; Information Security and Privacy Office Risk Manager.

TASK 4-3: Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.

Primary Responsibility: Information Security Manager.

Supporting Roles: Information Owner, Unit Privacy Coordinator, Information Security and Privacy Office Risk Manager.

Step 5. Authorize Information Systems

TASK 5-1: Authorize information system operations and data/information acquisitions based upon risk assessment process in steps 1 through 4. NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems provides guidance for this step.

Primary Responsibility: Information Security Manager.

Supporting Roles: Information Owner, Unit Privacy Coordinator; Information Security and Privacy Risk Manager.

TASK 5-2: Inventory new systems (internally hosted or cloud hosted).

Primary Responsibility: Information Security Manager.

Supporting Roles: Information Owner, Unit Privacy Coordinator; Information Security and Privacy Risk Manager.

Step 6. Monitor Security Controls

TASK 6-1: Monitor and assess selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials. The higher the risk a system or data is assigned, the more often the controls protecting the system or data should be reviewed.

Primary Responsibility: Information Security Manager and Information Owner.

Supporting Roles: Data Owner; Information Security and Privacy Office Risk Manager.

TASK 6-2: Review and assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.

Primary Responsibility: Information Security Manager.

Supporting Roles: Data Owner; Information Owner; Information Security and Privacy Office Risk Manager.

APPENDIX A: The Risk Assessment/Management Glossary

Availability: refers to ensuring that authorized parties are able to access the information when needed.

Classification: The designation given to information from a defined category in the university's Information Classification Guidelines based on its sensitivity.

Confidentiality: Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question.

Controls: Countermeasures or safeguards needed to meet the requirements of policy, business process, state and federal laws or contractual obligations.

Data/Information Custodian: The person or team that has operational responsibility for the physical and electronic security of information. Data custodians for electronic data normally include database and system administrators.

Data Owner: The head of a unit - dean, director, department head - who is ultimately responsible for that unit's data resources.

Data Manager: The unit employee(s) the data owner has delegated as operational oversight for the unit's data resources. At FSU, this function is often performed by the Unit Privacy Coordinator (UPC).

Information: Any representation of facts, concepts or instructions created, stored, filed, produced or reproduced, regardless of the form or media.

Information Asset: Includes all categories of information including, but not limited to, data contained in records, files, and databases. These assets can be in either a physical or digital form.

Information Owner: An individual or a group of individuals that has responsibility for making classification and control decisions regarding use of information.

Integrity: Involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence to the unit.

Risk Assessment: The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.

Risk Management: The process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

Threats: Anything that has a possibility of causing harm. A threat can be assessed in terms of the probability of an attack. Looking at the nature of the threat. Its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in a risk assessment.

Vulnerability: A weakness of a system or facility holding information which can be exploited to gain access or violate (physical/logical) system integrity.

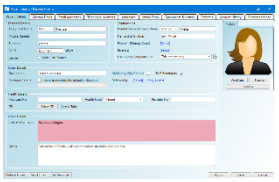
Appendix B – Example of Assigning Risk to a Data Set

Calculating Risk Levels

Risk levels are calculated by the impact (to the University) of a potential event/threat for the three security objectives. Each information item is reviewed by the "Security Objectives" presented on page 9 and a **Low**, **Moderate**, or **High** risk assigned to the Confidentiality, Integrity, and Availability of the information item reviewed. The assigned risk follows the information item regardless of its form including paper or digital to the point where it is transmitted, processed, or stored including file drawers, desks, application servers, database servers, a user's desktop or tablet, and cloud based computing solutions.

Examples:

Patient Health Record would be scored **High for Confidentiality**, **High for Integrity** (an altered record could cause catastrophic results), and **Low for Availability** if it was a backup record. ***The final risk would be High*** since that was the highest risk assessed for the three security objectives.



Class Syllabus might be assessed with a **Low for Confidentiality**, a **Moderate for Integrity**, and a **Low risk for Availability**. In this case, the overall ***risk rating would be Moderate*****.**

Student Financial Aid Record could be assessed as **High for Confidentiality**, **High for Integrity**, and **High for Availability**. The ***final risk level would be High***.

General Campus Maps might be assessed as **Low for Confidentiality**, **Low for Integrity**, and **Low for Availability**. The ***overall risk rating would be Low***.

Potential Impact ---------->

Security Objective	Low	Moderate	High
Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary university information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.
Integrity - Guarding against improper information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious adverse effect on organizational** operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.
Availability - Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have **a serious adverse effect** on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.

Appendix C – Example of Mapping Logical and Physical Controls to Information or Application

Data Set/Application Description	FSU Class	Risk Level	How are data/information/systems/databases safeguarded?
Unit-Academic Affairs	Public	Low	User Account Management, Malicious Code Protection, Information System Monitoring, Security, Alerts, Advisories, and Directives
Unit-Accounting	Private	Medium	User Account Management, Malicious Code Protection, Information System Monitoring, Baseline Configuration
Unit-Admin Dean's Office	Private	Medium	Transmission Confidentiality and Integrity, Public Key Infrastructure Certificates, User Account Management
Unit-Advising	Public	Low	User Account Management, Spam Protection, Security, Alerts, Advisories, and Directives
Unit-RTED	Protected	High	Cloud Service-Vendor controls for unit information are defined in the university security and privacy terms and conditions for contracted services (Controls for Unit Computing Devices Accessing Cloud Services) User Account Management, Security Awareness and Training Policy and Procedures, Physical Access Controls
Unit-Database	Public	Low	User Account Management, Malicious Code Protection, Information System Monitoring
Unit-Dean's Office	Public	Low	User Account Management, Malicious Code Protection, Information System Monitoring
Unit-Faculty Records	Private	Medium	User Account Management, Information Handling and Retention, Malicious Code Protection, Information System Monitoring, Monitor Security, Alerts, Advisories, and Directives
Unit-BCC Office	Public	Low	User Account Management, Malicious Code Protection, Information System Monitoring, Monitor Security, Alerts, Advisories, and Directives
Unit-Graduate Office	Protected	High	User Account Management, Security Awareness and Training Policy and Procedures, Software, Firmware, and Info Integrity(Vulnerability Management, Secure Baseline Server Configuration