Information Security Risk Management Standard

Revision Notes:	Last Updated:	Status: APPROVED
Version 1.0 - 6/2016 Revised & Approved By ISAC Ratified	06/2016	

Table of Contents

1. Objective:

The objective of this standard is to clearly define the required processes and controls needed to effectively identify, analyze, report, and manage information risks related to University information assets.

This standard also addresses control objectives outlined in sections 4.1.3 and 4.4.1 of the University Information Security Policy.

2. Scope:

This standard covers all University information resources including systems, data, and services. This standard is applicable to all Appalachian State University employees, students, and affiliates.

3. Requirements

3.1 - Information Security Risk Management Framework

Appalachian State University will utilize an information security risk management framework to define the method and logical interrelation of risk management activities.

3.1.1 - ISO 27005

The University information security risk management framework is guided by the ISO 27005:2011 standard (Information Technology - Security Techniques - Information security

risk management).

3.1.2 - Required Process Areas

The University information risk management methods and processes are divided into five required process areas (each of these areas is covered in more detail below):

Risk Process Area	Description	Conducted By
Risk Identification (section 3.8)	These processes are intended to help identify all risks that are relevant to University information assets.	ITS-OIS
Risk Analysis (section 3.9)	These processes are intended to establish the overall level of risk based on a determination of scope, impact, and likelihood.	ITS-OIS, Key Stake-Holders, Subject Matter Experts
Risk Evaluation (section 3.10)	These processes are intended to help determine if existing risk criteria are sufficient to determine a treatment option	ITS-OIS, Office of General Counsel
Risk Treatment (section 3.11)	These processes and steps are intended to have risk treatment options selected by appropriately parties.	Risk Owners
Risk Monitoring (section 3.12)	These processes and steps are intended to ensure that risk treatment options are validated for important risks on periodic basis.	ITS-OIS

3.2 - Risk Governance

All risks identified as relevant to University information assets will be managed by the institution. To effectively manage these risks the following roles and responsibilities have been established and agreed upon.

3.2.1 - Chancellor

The Chancellor has authority and responsibility for annually reviewing and approving the University Composite IT Risk Assessment and treatment plan related to those areas that present highest degree of risk (see 3.8.1).

3.2.2 - Chancellor's Cabinet

The Chancellor's Cabinet has authority and responsibility for overseeing processes needed to establish risk tolerance and selection of treatment options for extreme and serious risks that may be uncovered throughout the year. (see 3.11.2).

3.2.3 - Department Head / Unit Leads

University department heads have authority and responsibility for overseeing processes

needed to evaluate and enable treatment options for appreciable and minor level risks. (see 3.7 + 3.11.2)

3.2.4 - Chief Information Officer

The University Chief Information Officer has authority and responsibility for ensuring the alignment of IT services with institutional risk tolerance levels, communicating extreme and serious risks to executive leadership, and reviewing the annual risk assessment and treatment plan (see 3.8.1)

3.2.5 - Chief Information Security Officer

The University Chief Information Security Officer has the authority and responsibility to develop and oversee risk management processes needed to identify, analyze, and monitor information security risks that may impact the efficient conduct of the University mission.

3.2.6 - Information Security Advisory Council

The University Information Security Advisory Council is responsible for periodically reviewing and providing advisement and recommendations concerning university information security risks.

3.2.7 - Computer Security Incident Response Team

The Computer Security Incident Response has the authority and responsibility to review incident information and threat intelligence to help evaluate risks pertaining to technical IT defenses and related processes (see 3.8.3).

3.3 - Risk Scope

Information risks will be scoped according their applicability and origin. The scoping of information risk utilizes three tiers to differentiate risks and identify risk treatment responsibilities (see section 3.11.2).

3.3.1 Enterprise Information Risks

Enterprise risks are issues that are derived from a shared policy/compliance state, common organizational behavior, or central control deficiency that impact a large number of University units. These risks are often inherited due to their nature.

3.3.2 Unit Level Information Risks

Unit level risks are issues that are derived from a behavior, business practice, or control deficiency that is relevant to a single campus unit.

3.3.3 IT System Level Risks

System level risks are issues that stem from a technical or configuration weaknesses related to IT software or hardware.

3.4 - Risk Categories and Control Mappings

Risks will be categorized based on the eleven ISO 27002:2013 information security standard control categories to allow for correlation between risks and gaps analysis review and comparatives to varied IT security standards and risk frameworks (COBIT, NIST, PCI-DSS). The risk categories will include:

- Organizational / Management Risks
- Human Resource Risks
- Asset Management Risks
- Access Control Risks
- Cryptography Risks
- Physical and Environmental Risks
- Operational Risks
- Communications Risks
- System Acquisition, Development, and Maintenance Risks
- Supplier Relationship Risks
- Information Security Incident Management Risks
- Business Continuity Management Risks

3.5 - Risk Impact

Risk impact levels are established based on both quantitative (financial) and qualitative risks as listed below:

Impact Level	Description
Critical	Critical impact information risks represent dire threats to the university's mission including issues such as the sustainment of essential university services, solvency of the university's financial position, and the safety and well-being of university community. Quantitative Leveling: Critical impact risks would represent impact levels that exceed $1,000,000 in potential fiscal losses.
High	High impact information risks represent the potential for serious fiscal and reputational harm to the University. Quantitative Leveling: High impact risks present potential for fiscal losses between $100,000 - $1,000,000 dollars.
Medium	Appreciable information risks represent the potential for moderate fiscal and reputational harm to the University. Quantitative Leveling: Medium impact risks would present potential for losses between $10,000 - $100,000 dollars.
Low	Low impact information risks represent the potential for minor fiscal and reputational harm to the University.

	Quantitative Leveling: Low impact risks would present potential for losses between $100 - $10,000 dollars.

3.6 - Risk Likelihood

The risk likelihood represents the estimation of how likely a risk is to be realized within a given year. The following levels are utilized to differentiate varying degrees of probability.

Risk Likelihood	Annualized Rate of Occurrence	Description
Certain	75% to 100%	Risks with a ”Certain” likelihood have a very high chance of being realized each year.
Probable	30% - 75%	Risks with a ”Probable” likelihood have a fair chance of being realized every year.
Occasional	5% - 30%	Risks with an “Occasional” likelihood have a modest chance of being realized every year.
Rare	>0% - 5%	Risks with a “Rare” likelihood have a small chance of being realized each year.

3.7 - Risk Rating

Risks ratings will be calculated using the impact and likelihood assessments in order to classify and prioritize risks that present the greatest dangers to the institution.

……IMPACT……. …LIKELIHOOD…..	Critical	High Impact	Medium Impact	Low Impact
Certain	Extreme (E)	Serious (S)	Appreciable (A)	Minor (M)
Probable	Extreme (E)	Serious (S)	Appreciable (A)	Minor (M)
Occasional	Serious (S)	Appreciable (A)	Minor (M)	Minor (M)
Rare	Appreciable (A)	Minor (M)	Minor (M)	Minor (M)

3.8 - Risk Identification Processes

Risk Identification processes will be followed to determine the existence of potential risks that may require further analysis. The following processes will be conducted to support this process area:

3.8.1 - University Composite IT Risk Assessment

(Frequency: Annual; Scope: Enterprise Level)

3.8.1.1 - An overall risk assessment and treatment plan will be developed by the Chief Information Security Officer on an annual basis that includes a high level view

of the most significant risks uncovered throughout the year from identification processes (see 3.8.1.2) as well as recommended risk treatment strategies and plans.

3.8.1.2 - The risk assessment and treatment plan will be collaboratively reviewed by the University Information Security Advisory Council (see 3.2.6) to ensure that identified risks align with broad campus risk perceptions and that treatment recommendations are evaluated for effectiveness and cost.

3.8.1.3 - This annual assessment is reported to the Chancellor, Chancellor's Council, Chief Information Officer, and Chief Audit Officer.. The Chancellor and Chief Information Officer must review and sign and approve this assessment on annual basis.

3.8.1.4 Upon approval, the University Composite IT Risk Assessment is shared with University Internal Audit, UNC GA, and North Carolina Office of State Auditor.

3.8.2 - ISO 27002 GAP, Maturity, and Risk Assessment
(Frequency: Bi-Annual; Scope: Enterprise Level)

3.8.2.1 - ITS will bi-annually review ISO 270002 control areas to determine any areas that may be missing or underdeveloped. These controls areas will be analyzed and prioritized based on the maturity level of controls and related levels of risks associated with the control area.

3.8.2.2 - The top control areas with high risks and/or low maturity will be conveyed to the Information Security Advisory Counsel to ensure that risk area are reviewed and also reflect the broader view of risks held by representatives.

3.8.2.3 - These GAP assessments will be periodically submitted to the UNC IT Security Council for peer review and subsequent reporting to the NC Office of the State Auditor. This gap assessment will be used to determine risk review areas that may warrant more attention due to variance in control levels.

3.8.3 - Threat Review
(Frequency: Annual; Scope: System Level)

3.8.3.1 - The University Computer Security Incident Response team will at least annually review emerging technical threats in relation to performance of existing IT defenses against evolving attack threat trends/patterns and the tools, tactics and procedures (TTPs) of common threat actors.

3.8.4 - Vulnerability Scanning
(Frequency: Daily/Monthly; Scope: System Level)

3.8.4.1 - The ITS Office of Information Security has the authority and responsibility to conduct vulnerability scans of all networked university information systems.

3.8.4.2 - Internet facing servers and systems that store, process, or transmit confidential information must be scanned at least once each month.

3.8.4.3 - Exemptions from these scans must be requested and reviewed. The Chief Information Security Officer must approve exemption requests.

3.8.4.4 - Vulnerability scanning windows will be established to minimize potential conflicts with routine system operations or maintenance.

3.8.5 - Confidential Data Discovery and Loss Prevention

(Frequency: Daily/Monthly; Scope: Unit + System Level)

3.8.5.1 - The ITS Office of Information Security has the authority and responsibility to scan for the presence of University confidential data (see 5.2 + 5.3) in order to identify risks related to this data on systems that may have potential for system compromise or accidental disclosure .

3.8.6 - System Security Testing

(Frequency: As Needed; Scope: System Level)

3.8.6.1 - The ITS Office of Information Security has the sole authority and responsibility to conduct directed security tests to simulate attacks against University systems to determine their resiliency. This authority to test represents an exemption to relevant University standard computer and network usage policies so long as the requirements below are met.

3.8.6.2 - Security tests must be approved or requested by system owners. These approvals will be documented in a security testing approval form.

3.8.6.3 - Security tests must be coordinated with relevant system and application administrators to differentiate testing from actual attacks and to minimize potential conflicts with routine system operations.

3.8.7 - Post-Incident Analysis

(*Frequency: As Needed; Scope: All Scoping Levels* ***)***

3.8.7.1 - As part of the University's Information Security Incident Response plan, the ITS Office of Information Security will conduct post-incident analysis of security issues to determine their root-cause and any associated risks that may need to be reviewed.

3.8.8 - IT Procurement and Provider Review

(Frequency: As Needed; Scope: All Scoping Levels)

3.8.8.1 - The ITS Office of Information Security has the authority and responsibility to review any IT related services or software that may reasonably have the potential to introduce significant information risks.

3.8.8.2 - Campus Technology Portfolio Committees must complete the Infrastructure and Security Checklist to review whether the new solutions or projects entail information risks.

3.8.8.3 - The review criteria used to perform contractual and technical evaluations

will be established in partnership with Office of General Counsel and Materials Management.

3.8.8.4 - New or proposed IT solutions and providers that manage, store, transmit, or process University confidential data must always undergo a review.

3.8.8.5 - If significant risks are uncovered during the review process then a risk treatment review must be conducted by the appropriate risk owner prior to any purchasing decisions (see 3.11.2)

3.9 - Risk Analysis

The goal of risk analysis processes is to ensure that identified risks are consistently evaluated and scored in a common fashion. All identified risks must undergo the following steps:

3.9.1 - Risk Scoping Analysis

Each risk must be assessed as either enterprise level risks (see 3.3.1), unit level risks (see 3.3.2), or system level risk (see 3.3.3) in order to determine if risks are inherited from a central issue, system, or concern or whether the risk is singular to a particular department/unit, or system.

3.9.2 - Risk Impact Analysis

3.9.2.1 - Each risk will be assigned an impact level (see section 3.5) associated with the realization of a risk that must be calculated qualitatively and optionally may also be measured via quantitative estimation.

3.9.2.2 - Risk impact assignment must be done in concert with any key stakeholders or subject matter experts who have an understanding of business processes or adverse events associated with particular types of risks.

3.9.3 - Risk Likelihood Analysis

3.9.3.1 - Each risk must be assigned a likelihood value (see 3.6) associated with the estimated potential for a risk to be realized in the course of a year (annualized rate of occurrence).

3.9.3.2 - Risk likelihood assignment must be done in concert with any relevant key stakeholders or subject mater experts who have in depth understanding of threats that may lead to realization of risks.

3.10 - Risk Evaluation

The goal of the risk evaluation phase is to determine if legal, contractual, or policy requirements mandate certain treatment options related to identified risks.

3.10.1 - Legal and Compliance Review

Identified risks will be reviewed by the ITS Office of Information Security in consultation with the Office of General Counsel to determine their relevancy to any existing university contractual or legal requirements. If these obligations exist, then the terms of this agreement will be conveyed to the risk owner for awareness.

3.11 - Risk Treatment

The objective of risk treatment processes is to ensure that all risks are managed by an appropriate individual or group in an informed manner and that risk treatment decisions are executed.

3.11.1 - Risk Treatment Plans

All Extreme, Serious or Appreciable risks (see 3.7) must undergo a review and have a plan established for how the risk is to be treated. In some instances, risk treatment plans may include a combination of options. It is important to note that acceptance of risk is an acceptable plan when approved by Risk Owner (see 3.11.2).

Risk Treatment Option	Description
Accept	If risk rating is determined to be acceptable based on the cost of realizing a risk or addressing it (see below), then the decision can be made by an authorized University official (see 3.11.2) to accept the risk and not take additional actions.
Reduce	If risk rating is determined to be undesirable, then control measures can be implemented to lower the likelihood and/or impact of the risk.
Transfer / Sharing	If risk rating is determined to be undesirable, then risk may be evaluated for transferring or sharing components of this risk with a third-party (i.e., cybersecurity insurance).
Avoid	If risk rating is determined to be unacceptable in comparison to the cost of realizing a risk, addressing a risk, or the overall value of process, service, or area, then the decision can be made by an authorized University official (see 3.11.2) to discontinue the issue that originates the risk.

3.11.2 - Determining Risk Ownership

The risk rating associated with a risk determines the appropriate risk owner. Only the risk owner has authority to make risk treatment decisions. The risk rating also determines the reporting interval that risks must be conveyed. Any individual who has a question regarding risk reporting should contact their supervisor.

Risk Rating	Risk Owner	Time-frame to communicate risk
Extreme	Chancellor's Cabinet	As soon as possible.
Serious	Chancellor's Cabinet	< 30 Days
Appreciable	Department Head / Unit Lead	< 60 Days
Minor	Department Head / Unit Lead	< 60 Days

3.11.3 - Accountability and Roles For Enacting Risk Treatment

Risk Scope	Accountable For Risk Treatment	Responsible For Implementing	Consulted	Informed
Enterprise Level Risk	VC or equivalent leadership position who oversees relevant area.	Varies	Key business process stakeholders.	ITS Office of Information Security; Office of Internal Audits; Office of General Counsel
Unit Level Risk	Department Head/Chair, Unit Lead	Departmental Staff	N/A	ITS Office of Information Security; Office of Internal Audits; Office of General Counsel
System Level Risks	System Owner	System Administrators	Key system stakeholders	ITS Office of Information Security; Office of Internal Audits; Office of General Counsel

3.12 - Risk Monitoring

The goal of risk monitoring processes is to ensure that risks treatment options are validated for important risks on a periodic basis.

3.12.1 - IT Risk Inventory

The ITS Office of Information Security will maintain a risk inventory for all appreciable, serious, or extreme risks that include the risk owner and risk treatment plan. The risk inventory will be reviewed periodically to identify risks that may warrant future inspection.

3.12.2 - Key IT Control Testing

The ITS Office of Information Security will periodically review IT controls that have been implemented to modify extreme or serious risks to achieve approved residual risk levels.

3.12.3 - Change Management

Campus IT units will review significant changes, upgrades, and other modifications to IT systems associated with appreciable risks to determine if the proposed changes can alter former risk levels.

4. Definitions

4.1 - Risk

In the content of Information Security, risk is the exposure to potential reduction of Confidentiality, Integrity, and Availability of information assets such as information systems, data, user credentials, and other computing resources.

4.2 - Risk Owner

In the context of this standard, the risk owner is the group or role within the University who has the authority and accountability for selection of appropriate risk treatment options (see 3.11)

4.3 - Risk Assessment

The overall process of risk identification (see 3.8), risk analysis (see 3.9) and risk evaluation (see 3.10).

4.4 - Risk Impacts

Adverse outcomes that result when risks are realized.

4.5 - Control

A measure that modifies a risk.

4.6 - Risk Rating

The magnitude of a risk, expressed in terms of the combination of impact potential and their likelihood.

4.7 - Residual Risk

The amount of risk assessed to be remaining after the implementation of a control.

4.8 - Risk Management

The coordination of activities to direct and control an organization with regard to risk.

5. References

5.1 Appalachian Information Security Policy

5.2 University Data Management Standard

5.3 University Minimum Security Standard

5.4 ISO/IEC 27005:2011 Information security risk management standard