Effective Date: **May 1, 2026**

STANDARDS

EMPLOYMENT, INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Cyber Risk Assessment Standard

RESPONSIBLE OFFICE

Information Services and Technology

Purpose

The purpose of this standard is to establish an approach for identifying, evaluating, and prioritizing cybersecurity risks at Boston University. This ensures a consistent methodology for determining the severity of risks, which serves as a precursor to risk management decisions.

Scope

This standard applies to all university departments, schools, and personnel involved in managing or overseeing information systems, applications, and data. It encompasses risks to the confidentiality, integrity, and availability of university data.

Defined Terms

Risk: A semi-quantitative assessment of the risk of continuing to operate with an identified

vulnerability in an asset, system, service, or process after all compensating controls are considered. The risk may change over time as changes in threats and controls occur, including those outside of the asset, system, service, or process.

Risk Assessment: A formal document containing one or more identified risks.

Cyber Risk Register: A collection of all Risk Assessments maintained by Information Security.

Roles and Responsibilities

Risk Owner: The individual most directly accountable for remediation of an identified risk. This may be a service owner, project sponsor, business owner, unit lead, or any other individual who would commit resources to correct the risk. The risk owner collaborates with Information Security to provide details about assets, systems, services, or processes to enable risk to be understood in context and ensures timely participation in risk assessment activities.

BU Information Security: Overseen by the Chief Information Security Officer, this group is responsible for conducting risk assessments of identified assets, systems, services, or processes according to the defined procedure and developing methodologies to support that procedure. Information Security shall define and document risks that are identified, evaluate and prioritize the level of risk, and communicate findings to the Risk Owner.

Standards

1. Information Security may perform periodic risk assessments to understand the current risk to all organizational functions (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of University Data.

2. Information Security may perform a cyber risk assessment of any asset, system, service, service provider, vendor, or process to ensure that University Data is adequately protected. These assessments may be triggered by the launch of a new service or process, a significant change to a system, service, or physical environment, a cybersecurity event or emerging threat, a finding from a risk management process such

as a vulnerability scan or a penetration test, or upon request. These assessments will support informed decision-making regarding risk mitigation, transfer, or acceptance.

3. All identified risks will be documented and categorized as defined in the procedures section.

4. BU Information Security shall collaborate with Risk Owners to identify, evaluate, and prioritize risks and document them in a Risk Register.

5. A final version of a Risk Assessment will be communicated to the Risk Owner for triage under the Cyber Risk Management Standard and recorded in the Risk Register.

6. Risk Assessments are classified as Confidential documents and will be shared according to need-to-know.

Procedures

A risk assessment has three major steps:

- **Risk Identification:** Through a combination of interviews, reviews of documentation, and/or inspection of an asset, system, or service, the assessor will apply knowledge of current threats and vulnerabilities to identify risks that may result in a loss of confidentiality, integrity, or availability.
- **Risk Evaluation:** Having identified a risk, the assessor will consult with the Risk Owner and assign an impact and likelihood to arrive at a statement about risk severity.
- **Risk Registration:** A risk is formally documented and recorded in Information Security's Cyber Risk Register.

Risk Identification

The high-level process of identifying risks is to:

- Define the scope of the evaluation. Catalog assets, processes, and systems that relate to the asset, system, service, or process under assessment.
- Evaluate the quantity and types of sensitive data stored, processed, or transmitted by the

asset, system, service, or process under assessment that may be impacted.
- Identify potential threats and vulnerabilities.
- Consider compensating controls that may reduce the likelihood of a specific vulnerability being exploited.
- Identify any specific risk statements and concisely document them according to the Cyber Risk Assessment and Management Form maintained by Information Security. Risks may combine several similar threats and/or vulnerabilities. Categorize the risks according to Appendix B.

Risk Evaluation

- Before scoring, risks are reviewed with Risk Owners to ensure the context of the risk is understood, including any compensating controls.
- The risk scoring process is based on the university's Enterprise Risk Management scoring rubric, but the impact assessment criteria have been more tailored to IT risks.
- Each risk is scored by determining the most likely impact to occur and then calculating the likelihood of that event occurring one or more times in a 3-year period.
- The impact and likelihood are used to determine a resultant risk level for each risk.

Impact Assessment

In selecting an impact assessment, identify the most likely level of risk to occur based on any of the impact categories.

- Note that the scope is impact to the university, so in reviewing a scope that has limited use, the impact of a realized risk will also be reduced.
- Use the most severe but still likely impact. This system favors identifying risks that are realized often, if even the impact is minor, over more impactful events that are less likely to occur.

IMPACT	Minor	Moderate	Major

Monetary	IT-related losses or unanticipated expenses below $20,000, excluding internal staffing costs. Small cost increases due to limited system outages, minor cybersecurity fixes, or additional IT staffing needs.	IT-related costs are between $20,000 and $200,000, excluding internal staffing costs. Moderate losses due to data recovery efforts, compliance fines, or software/service disruptions requiring significant remediation.	IT-related financial impacts exceeding $200,000, excluding internal staffing costs. Large-scale costs due to ransomware attacks, prolonged outages, or breaches exposing highly sensitive data, resulting in lawsuits, fines, or settlement payouts.

Process	Brief, localized IT disruptions affecting a small number of users or a small department. Minimal downtime for crit-1 or crit-2 system.	Temporary loss of key IT systems or platforms affecting a larger population or application. Downtime lasting a day or more for a crit-1 or crit-2 system. May also include a smaller outage that impacts business process at a critical time (admissions, e.g.)	Widespread IT outages, such as campus-wide network failures or prolonged unavailability of crit-1 or crit-2 system. Extended recovery times significantly disrupting academic or administrative operations. May also include a smaller outage that impacts business process at a critical time (admissions, e.g.)

Reputational	Negative attention limited to a minor IT mishap (e.g., an isolated data leak or service outage) with minimal media coverage. No long-term damage to trust among students, faculty, or donors.	Broader reputational damage due to significant IT failures, such as delayed grades or financial aid processing, or a phishing attack targeting the institution. Negative coverage in regional or national media, causing temporary loss of trust from students, parents, or partners.	Widespread reputational harm from large-scale IT failures or breaches, such as the exposure of sensitive student or employee data, misuse of research data, or a ransomware attack. Loss of research sponsorship, loss of donor trust, reduced student applications, or diminished competitiveness in the higher education market.

Strategic	Delays in IT projects or implementations without affecting long-term goals. Minor setbacks to planned improvements in IT capabilities.	Significant delays or failures in IT modernization projects or system upgrades that impede strategic goals, such as enrollment growth or digital transformation. Reduced efficiency or competitiveness compared to peer institutions.	Catastrophic failure to meet strategic goals due to IT issues, such as failure to secure a digital transformation or loss of accreditation tied to inadequate IT systems. Compromised ability to attract top students, faculty, or funding due to IT system vulnerabilities or inadequacies.
Legal, Audit, Compliance	Minor IT compliance violations, such as delayed software updates, with no external penalties or low-cost remediation. Internal audit findings that are resolved easily.	IT non-compliance leading to regulatory investigations or moderate fines (e.g., FERPA, HIPAA, or GDPR violations due to data breaches). Litigation risks tied to IT failures or unauthorized data access affecting moderate numbers of users.	Significant legal or compliance failures, such as massive data breaches or IT security lapses exposing sensitive student, research, or financial data. Regulatory fines exceeding $10 million, lawsuits, or loss of federal funding tied to IT system deficiencies.

Likelihood Assessment

After establishing the impact to be considered, review the following table to determine how likely the impact is to be realized in the next 3 years.

LIKELIHOOD	Rare	Possible	Almost Certain
Detailed Description	The risk event is not expected to occur but could occur at some time under most conditions. It may be possible under a specific set of conditions, such as under multiple and simultaneous failures.	The risk event may occur at some time under specific conditions. It has happened to other higher education institutes under specific circumstances. External factors may cause the risk event to occur.	The risk event is expected to occur or is occurring. BU and/or other higher education institutes have experienced the risk event in the recent past. External and internal conditions are or will become favorable for the risk event to occur.
% of Chance Annually	< 20 % Chance of occurring in 1 – 3 Years	20 – 60 % Chance of occurring in 1 – 3 Years	> 60 % Chance of occurring in 1 – 3 Years
Event	Not likely to occur	May or may not occur	Almost certain to occur

Risk Severity Levels

Having identified the impact and likelihood, the risk level is determined using the table below.

		Likelihood

	Rare	Possible	Almost Certain		
Impact	Major	Moderate Risk	High Risk	Critical R
	Moderate	Moderate Risk	Moderate Risk	High Ris
	Minor	Low Risk	Moderate Risk	High Ris

Risk Registration

After risks are identified and evaluated, risks are grouped into Risk Assessment documents based on the Risk Owner. Multiple related risks may be recorded in a single Risk Assessment.

All completed Risk Assessments will be recorded in Information Security's Cyber Risk Register.

Documentation must minimally include:

- Identification of the Risk Owner and Assessor
- Description of the asset, system, service, or process under assessment.
- The quantity and types of sensitive data stored, processed, or transmitted by the asset, system, service, or process under assessment that may be impacted.
- Description of identified risks.
- Assessment of likelihood and impact of each risk and resulting risk level. Rank risks by risk level to focus on addressing the most critical threats.
- Recommendation of mitigations and allowable timeframes based on risk level

Exceptions

Information Security is authorized to grant exceptions to the requirements set forth in this document. Any exception granted will require a thorough review of the situation and the implementation of appropriate compensating controls.

In addition, Information Security may publish directives aimed at clarifying the intent of a standard to aid in the interpretation of this standard.

Important

Failure to comply with the Data Protection Standards may result in harm to individuals, organizations or Boston University. The unauthorized or unacceptable use of University Data, including the failure to comply with these standards, constitutes a violation of University policy and may subject the User to revocation of the privilege to use University Data or Information Technology or disciplinary action, up to and including termination of employment.

Version History

Notes	Approver	D
Initial Publication of Cyber Risk Assessment Standard	IS&T Policy and Standards Review Committee	M

Appendix A: NIST Cyber Security Framework and SP 800.171 Mapping

The following table maps the National Institute of Science and Technology (NIST, nist.gov) Cyber Security Framework (CSF) and Special Publication (SP) 800-171 controls to standards expressed in this document. Fully implementing this standard with associated procedures and evidence of adherence to those procedures would likely indicate that all the controls listed here are met. However, compliance must always be evaluated for the scope of the information system in question, and having a standard by itself does not guarantee compliance. This document references CSF version 1 and 800-171 revision 2.

CSF Control	800.171 Control	Control
	3.11.1	Periodically assess the risk to organizational operations (i functions, image, or reputation), organizational assets, an resulting from the operation of organizational systems and processing, storage, or transmission of CUI
GV.RM-06		A standardized method for calculating, documenting, cate prioritizing cybersecurity risks is established and commun
ID.RA-01		Vulnerabilities in assets are identified, validated, and reco
ID.RA-04		Potential impacts and likelihoods of threats exploiting vuln identified and recorded
ID.RA-05		Threats, vulnerabilities, likelihoods, and impacts are used inherent risk and inform risk response prioritization
ID.RA-07		Changes and exceptions are managed, assessed for risk and tracked

Appendix B: Risk Categories

The following table aligns risks with control families from cybersecurity frameworks (e.g., NIST Cybersecurity Framework, ISO 27001) as well additional risk categories not covered by these frameworks:

Risk Category	Example Risks	Evaluation Factors	CORRECTIVE ACTION EXAMPLES

Access Control	Unauthorized access to sensitive data	Type of data affected; impact of unauthorized access	Enforce MFA; restrict access based on roles
Asset Management	Untracked or unmanaged devices	Visibility of assets; risk from unknown vulnerabilities	Conduct regular asset inventories
Audit and Accountability	Lack of logging or monitoring	Ability to detect and respond to incidents; regulatory compliance	Implement centralized logging; regular reviews
Configuration Management	Default or weak configurations	Scope of affected systems; ease of remediation	Apply secure configurations; automate checks
Incident Response	Lack of incident response plan	Time to detect and respond; organizational impact	Develop and test response plans
Data Protection	Unencrypted sensitive data	Sensitivity and volume of data; potential for data loss	Implement encryption; secure backups
System Maintenance	Missing patches or updates, Obsolete hardware or software	Likelihood of exploitation; exposure of critical systems	Accelerate patching cycles; temporary isolation

Training and Awareness	User susceptibility to phishing	Frequency of incidents; impact of successful attacks	Conduct regular training; simulate phishing tests
Physical Security	Unsecured data centers or devices	Accessibility of critical assets; potential for theft or sabotage	Enhance physical security; restrict access
Vendor Management	Third-party security weaknesses	Vendor compliance with security standards; impact of vendor compromise	Conduct risk assessments; require SLAs
Disaster Recovery / business continuity	Lack of disaster recovery plans	Impact on critical operations; time to recovery	Develop and test recovery plans
Documentation	Lack of system documentation	Ability to manage, maintain, operate, or recover solution	Develop documentation

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related BU Policies, Procedures, and Standards

- Data Protection Standards Overview
  - Data Classification Standard
  - Data Access Management Standard
  - Identity and Access Management Standards [this webpage]
  - Data Lifecycle Management Standard
  - Minimum Security Standards
  - Cybersecurity Training, Compliance, and Remediation Standards
  - Cyber Risk Assessment Standard
  - Cyber Risk Management Standard
  - Data Center Security Standards
  - Vulnerability Management Standard
  - Log Collection, Analysis, and Retention Standard

BU Websites

- Information Services & Technology

BU Resources

- Additional Guidance on Data Protection Standards
  - 1.2.D.1 – Destruction of Paper Records and Non-Erasable Media -CD-ROMs, DVDs (Data Protection Standards Guidance)
  - 1.2.D.2 – Destruction of Individual Files on Reusable Media (Data Protection Standards Guidance)
  - 1.2.D.3 – Securely Erasing Entire Reusable Storage Devices (Data Protection Standards Guidance)
  - 1.2.D.4 – Physically Destroying Reusable Storage Devices (Data Protection Standards Guidance)

History

This Cyber Risk Assessment Standard was enacted May 2026.

Categories: Data Protection Standards, Data Protection Standards, Employment, Information Management, Information Technology Use, Access, and Security, Privacy and Security
Keywords: cyber, Cyber Risk Assessment, Cyber Risk Assessment Standard, risk assessment