# Procedure III.3010.A.b, Cybersecurity Risk Management

**Associated Policy**
Policy III.3010.A, Information Resources

## 1. Purpose

The College is required to protect its Information Resources and Protected Data from unauthorized disclosure, alteration, or destruction by performing due diligence through the accomplishment of Cybersecurity Risk Assessments. Cybersecurity Security Risk Management assesses potential threats and vulnerabilities to the Confidentiality, Integrity, and Availability of the College's Information Resources and Protected Data, and then develops and implements Risk Mitigation strategies to efficiently and effectively mitigate the Risks identified by such Risk Assessments. Furthermore, such Risk Assessments are required by Texas Administrative Code §202 (TAC 202) for any on-premises or cloud-based computing services (Third-Party Applications) procured or renewed by the College.

## 2. Applicability

This Procedure applies to all College Information Resources and the Users of such Information Resources, in any form, and is intended to be broad enough to include all Users. This Procedure applies to Users that request the procurement or renewal of Third-Party Applications or other Information Resources for use within the College Information Resources environment. Such Third-Party Applications and Information Resources may include software and technologies installed on-premises or within a cloud environment.

## 3. Laws, Regulations, and Standards

The College is required to comply with Federal and State Laws and Regulations. In particular, TAC 202.77 requires that state agencies only enter or renew a contractual agreement to receive cloud-computing services (Third-Party Applications) that comply with the Texas Risk and Authorization Management Program (TX-RAMP). As such, the Texas Department of Information Resources (Texas DIR) established a framework for collecting information about cloud services security posture and assessing responses for compliance with required controls and documentation. Furthermore, the College is required to comply with evaluation standards as set forth by the Family Educational Rights and Privacy Act (FERPA), Gram-Leach-Bliley Act (GLBA), Personal Credit Information (PCI), Health Insurance Portability and Accountability Act (HIPAA), and Children's Online Privacy Protection Act (COPPA), and other regulatory requirements as outlined in the College's Information Security Program Procedure.

## 4. Associated Program Controls

The following Program Controls associated with this Procedure are:

PM Program Management Control Family
- PM-9 Risk Management Strategy

RA Risk Assessment Control Family
- RA-1 Risk Assessment | Policy and Procedures

- RA-2 Security Categorization
- RA-3 Risk Assessment
- RA-3(1) Risk Assessment | Supply Chain Risk Assessment
- RA-5 Vulnerability Monitoring and Scanning
- RA-5(2) Vulnerability Monitoring and Scanning | Update Vulnerabilities To Be
- Scanned
- RA-5(11) Vulnerability Monitoring and Scanning | Public Disclosure Program
- RA-7 Risk Response

SA System and Service Acquisition Control Family

- SA-4 Acquisition Process

## 5. Roles and Responsibilities

The roles and responsibilities as defined by the Information Security Program are described in Procedure III.3010.A.a, Information Security Program. Described below are additional roles and responsibilities that pertain to this Procedure.

a. **The Office of Cybersecurity (OCS)** performs the following duties:

- Schedules, prioritizes, and conducts Cybersecurity Risk Assessments.
- Requests information from College Users related to their collection and use of Protected Data.
- Processes and follows up on requested exceptions to College Policy and Procedures.
- Facilitates Risk reviews of Third-Party vendor via the Software Intake Form (SIF) process to ensure vendors adhere to CIS Benchmarks for applicable products.
- Participates in the Cybersecurity Risk Management program, including identification of assets and services, allocation of resources, risk prioritization, risk acceptance, and implementation of risk treatment plan.

b. **College Users(s)** is an individual, automated application, or process that is authorized by the College to access an Information Resource. Includes, but is not limited to, all College students, faculty, staff, contractors, guests, departments, and any individual, application, or process that accesses and or uses the College's Information Resources.

Specifically, Administrators, Faculty, and Staff that request the procurement or renewal of Third-Party Applications and are, as such, the custodian of the Third-Party Application. Such custodians are required to cooperate with the CISO and the Office of Cybersecurity to:

- Submit a Software Intake Form (SIF).
- Participate in Risk Assessments when applicable. This includes Risk Assessments as part of the SIF process and third-party assessments or audits.
- Submit exceptions to the Cybersecurity Risk Management Procedure through the Office of Cybersecurity and work with the Office of Cybersecurity through the exceptions process.

## 6. Cybersecurity Risk Management Schedule

Two principal components of the Cybersecurity Risk Management process are:

- Risk Assessments, and
- Risk Mitigations

These processes shall be conducted according to the following schedule to ensure the continued adequacy and continuous improvement of the College's Information Security program:

a. **Scheduled Basis**. An overall Risk Assessment of the College's Information System Infrastructure shall be conducted biennially, aligning with the biennial submission of the State Agency Security Plan as required by TAC 202.73. The Risk Assessment process shall be completed in a timely manner to determine Risk Mitigation strategies within the College's annual budgeting process.

b. **Throughout a System's Development Life Cycle.** From the time that a need for a new Third-Party Application or Information Resource is identified through the time it is disposed of, ongoing assessments of the potential threats to the Information Resource and its vulnerabilities will be undertaken as a part of the maintenance of the system. Risk Assessments are conducted:

    - Before the purchase of Third-Party Applications or other Information Resources.
    - Before the integration of new Third-Party Applications or other Information Resources and before changes are made to physical safeguards.
    - While integrating Third-Party Applications or other Information Resources and making physical, technological, or administrative security changes. This includes environmental or operational changes affecting the security of ePHI, Financial NPI, PII, protected cardholder data (PCI-DSS), and student education records.
    - While sustaining and monitoring appropriate security controls. This includes performing periodic technical and non-technical security-rule requirement assessments.

c. **As Needed.** The Chancellor, CTIO, or CISO may call for a full or partial Risk Assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect the College's information systems.

## 7. Submitting a Software Intake Form (SIF)

A key tool in conducting Cybersecurity Assessments is the Software Intake Form (SIF). College Users requesting the procurement or renewal of Third-Party Applications or other Information Resources are required to submit a SIF to the ITS Help Desk. Contact the ITS Help Desk for further instructions on submitting a SIF.

Prior to submitting a SIF, please reference **Procedures 2-13 and 2-14 (Purchasing and Bidding)**. Requestors may also seek guidance from the Office of Cybersecurity (OCS) and Information Technology Services (ITS).

It is the responsibility of the requestor to collect and submit information for the SIF review. If the purchase or renewal is conducted by Request for Proposal (RFP), then the requestor must submit a SIF when a finalist is selected and before a contract is awarded.

Satisfactory completion and approval of the SIF is required for the purchase or renewal of the Third-Party Application or other Information Resource. On approval of the SIF, ITS provides an ITS Approval Number to Purchasing. If the SIF is not approved, then ITS will contact the requestor to discuss the reasons for denying approval and alternative solutions.

Temporary exception requests for SIF approval prior to submission or completion of a SIF must be submitted to the College's Chief Technology Information Officer (CTIO). It is at the CTIO's discretion to approve temporary exception requests. The CTIO will assess the risks associated with the request based on the information provided. If temporary exception approval is granted, then it is subject to the outcome of the SIF review process. Please note the SIF review process may identify critical issues preventing the Third-Party Application or other Information Resource from being installed or implemented. In such cases, such Third-Party application or other Information Resource will be uninstalled and/or removed.

## 8. Conducting Risk Assessments and Analysis

The intent of completing a Risk Assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to manage risks. Prior to this or in conjunction, a Business Impact Analysis, as part of the B-COOP (Business Continuity of Operations Plan) is conducted to determine critical processes and assets.

Risk Analysis is the process of identifying and analyzing potential issues that could negatively impact key business.

## 9. Conducting Risk Mitigation

To mitigate the Risks identified by Risk Assessments, security measures will be implemented that are sufficient to transfer, accept, or reduce risks and vulnerabilities to a reasonable and appropriate level to:

- Ensure the Confidentiality, Integrity, and Availability of all Protected Data the College creates, receives, maintains, and/or transmits,
- Protect against any reasonably anticipated threats or hazards to the security or integrity of Protected Data,
- Protect against any reasonably anticipated uses or disclosures of Protected Data that are not permitted or required, and
- Ensure compliance with Federal and State Laws and Regulations.

## 10. Risk Acceptance Process

Ensuring approval of the security risk acceptance, transference, or mitigation decisions shall be the responsibility of the Information Security Officer (CISO) or CISO designee(s), in coordination with the Information Owner for Information Resources identified with Low or Moderate residual risk as defined by TAC 202.75.

The acceptance of any high-level risks that remain (residual) after other risk controls have been applied requires the approval of the Chancellor. Such approved residual risks will be recorded in the College's Risk Register which is maintained in Texas DIR's Archer system.

## 11. Risk Mitigation and Acceptance Documentation Requirements

All Cybersecurity risk management efforts, including the College's Risk Register with decisions made regarding specific mitigation controls implemented or not implemented shall be documented and documentation maintained for seven (7) years, at which point records will be destroyed in accordance with the College's Records Management program and industry best practices as defined by NIST 800-53.

## 12. Definitions

The terms referenced in this Procedure are outlined in **Procedure III.3010.A.a, Information Security Program**, Section 14. Definitions.

| | |
|---|---|
| Date of SLT Approval | February 15, 2024 |
| Effective Date | February 15, 2024 |
| Associated Policy | Policy III.3010.A, Information Resources |
| Primary Owner of Policy Associated with the Procedure | Chief Technology Innovations Officer |
| Secondary Owner of Policy Associated with the Procedure | Chief Information Security Officer |