CPTC Procedure – Risk Assessment Process: Managing Risks and Vulnerabilities

Overview

Policies and procedures from the Technical College System of Georgia (TCSG) Information Technology (IT) department are the primary foundation for information technology security for Coastal Pines Technical College (CPTC). These are based on industry best practices and National Institute of Standards and Technology (NIST) Special Publication (SP) 800 controls. The NIST SP 800 series is comprised of guidelines, recommendations, technical specifications, and annual reports of NIST's cybersecurity activities. These guides and specifications are of great interest to the computer security community. They are designed and intended to optimize the functionality, security, and interoperability of the College's IT assets and systems. This procedure covers all CPTC IT assets and systems – regardless of location or who is managing the service. This procedure also applies to all contractors and outside users that use and support the CPTC IT assets and systems.

The NIST SP 800 part 53 covers the steps in the Risk Management Framework that address security controls. This includes applying a set of security controls based on determining worst-case impact analysis. The security controls cover 18 areas including access control, incident response, business continuity, and disaster recoverability.

This procedure outlines the risk assessment framework as outlined in the NIST SP 800 part 53 (NIST SP 800-53) controls document that will guide the College in conducting an annual risk assessment on all information system assets and systems. Due to the sensitive information housed in the student information system, an emphasis is placed on it as well as the assets and systems that support it. This is not limited to computer, network, and digital systems.

Risk assessments help to identify threats and vulnerabilities as well as gaps in procedures and protocols that may threaten availability, confidentiality and integrity for CPTC information systems infrastructure.

Role Definition

Everyone at the college from leadership to faculty to staff to contractors have a part to play in the security of our information systems and data.

- ***CPTC Leadership -*** The CPTC leadership is composed of the president, vice presidents, executive directors, and Campus Police Chief. This group is referred to as the CPTC Cabinet. These employees are responsible for the sponsorship and support of the Risk Assessment process and report. This leadership group is responsible for the the review and approval of risk assessments and control recommendations and reporting for each of their respective divisions. They should also report mitigation actions that have been taken to address risks, vulnerabilities and gaps in procedures and protocols.
- ***Information Security Administrator (ISA) -*** The ISA is appointed by TCSG IT leadership. The ISA is responsible for: (1) ensuring the security of information systems and data at the College; (2) the continued development, implementation, and maintenance of the risk assessment study; and (3) delegating responsibilities and gathering input from CPTC Leadership for each of their respective divisions.

- ***System Owner / Administrator -*** System owners are staff who are responsible for a given system. They are expected to participate in the risk assessment process, report results, address identified weaknesses, and report the progress of remediation of previously identified weaknesses to the ISA.
- ***All CPTC Staff –*** Any and all CPTC employees may be asked to participate in meetings or discussions as part of the risk assessment as well as remediation to address areas of need. Employees are expected to follow the "see something say something" maxim to report any areas of concern or potential issues.

Procedure (RA-1)

All College information system assets and media must meet the security controls defined in this procedure. The controls that make up this procedure are based on the NIST SP 800-53, Security and Privacy Controls. The College will engage in appropriate risk management by operating in compliance with these controls. Risk management includes the identification, analysis, and management of risks associated with the College's business, information technology infrastructure, data, and physical security to protect its IT assets and critical business functions:

a. Each division of the College must participate in the CPTC Risk Assessment.
b. The risk assessment process must identify and classify risks to IT systems and data as well as implementing risk mitigation as appropriate.
c. The process will include the identification, classification, prioritization and mitigation processes necessary to ensure the stability and continuity of mission critical IT systems and resources.

In order to ensure systems that are more secure and reliable, TCSG requires each TCSG entity to complete an annual risk and security assessment of critical systems and infrastructure in compliance with GTA mandates. The College must complete a risk and security assessment annually. Particular focus is placed on the student information system and all systems that "touch" or interface with it at any level.

The College will annually submit the completed risk assessment document to TCSG with all results. The results of the risk assessment will be used to create and maintain remediation plans for any deficiencies noted during a risk assessment, including vulnerability scans. Divisional leaders will create plans to address residual risks for those controls that cannot be remediated.

This procedure uses the terminology and framework established in NIST SP 800-53. The "RA" designator (such as RA-1, RA-2, etc) identified in section headings represents the NIST-specified identifier for the Risk Assessment control family. The sections below outline the controls that the College must satisfy in each annual review.

Risk Management Program Activities:

The CPTC Risk Assessment concentrates on four stages of activities:

1. A continual Identification of Risks that may affect business continuity and security of the College and its assets. This also includes documenting the characteristics of the risks.
2. The College will create an analysis of the risks identified in the first step. This will include an estimation of the probability and impact that stem from the risk. This will be followed by prioritizing the risk and developing a timeline for remediation.

3. System owners of the threatened systems will work with other involved parties to develop a plan to mitigate each of the identified risks. That plan should limit the probability of the risk occurring as well as reducing the impact if it does.
4. Tracking and Controlling Risks involves the collection and reporting of status information about risks and their mitigation plans, response to changes in risks over time, and management oversight of corrective measures taken in accordance with the mitigation plan. The system owners will track the implementation of the mitigation plans and document progress and completion. System owners will report security issues relating to information system assets and data to the College ISA. The College ISA will follow the CPTC Cybersecurity Incident Response Plan to determine if the issue should be escalated to the TCSG ISO.

Business Continuity Risk Management Processes

For business continuity, the focus of the CPTC Risk Assessment and associated activities is an analysis of the impact of risks that may disrupt the continuity of business for the College. System owners will identify risks that may negatively affect business continuity and develop strategies needed to provide an appropriate level of remediation. The College should conduct business continuity risk impact analysis (BIA) activities that include the following:

a. Define the College's critical functions and services.
b. Define the system owners of these critical functions and services.
c. Define the resources that support each critical function or service. This includes the information systems, staff, and facilities components needed to sustain each function or service.
d. Identify key relationships and interdependencies among the mission critical infrastructure, functions, staff, and services for the College.
e. Assess and estimate the negative effect over time for each critical function or service
f. Estimate the time that a critical function or service can fail before resulting in a serious or catastrophic impact on the College's function.
g. Estimate the maximum acceptable amount of data, digital or non-digital, that can be lost without a serious or catastrophic impact on the College's function.
h. Estimate financial losses associated with system or service loss over time for each critical function or service.
i. Estimate impacts over time to the College's ability to carry out critical function or service
j. Identify any services that require a higher than normal priority such as payroll, ability to login, or utilities such as electricity or water.
k. Identify critical non-digital media such as paper files or documents that are required to support the College's critical functions or services.
l. Identify or develop interim or workaround procedures that mitigate loss of critical functions or services.
m. Ensure that outside service providers who provide critical services to the College have the capacity and expertise to ensure that they meet the recovery time objective (RTO) and recovery point objective (RPO) requirements of the College. Reliance on third parties should be reviewed to identify and mitigate risk. RTO refers to how long the College or its divisions can survive following a disaster before operations are restored to normal. RPO is a measurement of the maximum amount of data that the College or its divisions can lose; is that point one minute in the past, one day, one week, or a different amount?
n. Takes steps to ensure that the progress and outcomes of any manual work data and the automated processes are available to all involved parties during a recovery period.

Security Risk Process

The focus of CPTC's annual risk assessment is to identify security risks that may jeopardize the College's information assets and mission critical functions or services. The College should identify and analyze the impacts of security risks in order to develop strategies, remediations, and work-arounds that can and will provide the appropriate level of prevention and response. Activities involved in security risk impact analysis activities for the risk assessment include:

a. Identification of all regulatory or legal requirements applicable to the College that address the security, confidentiality, and privacy requirements for College functions or services.
b. Identification of sensitive or confidential information that is stored in the College's information systems as well as the potential for fraud, snooping or other illegal or unwanted activities.
c. Identification of current and needed access control procedures used for requests, authorization, and access approval needed to protect the confidentiality, integrity, and availability of the College's systems and data.
d. Identification and implementation of processes to monitor and report on the health and security of mission critical systems and data. These may include security logs, event logs, access logs, login logs, credential usage, or other relevant processes.
e. Documentation of the College's Change Management and Risk Assessment processes.
f. Identification of security methods used to protect the College's data including web encryption, encryption on disk, and other related technologies.
g. Creation of a Business Impact Analysis (BIA) by each divisional leader based on the findings in the security risk impact analysis activities for the College.

Security Categorization (RA-2)

The College must address the following requirements:

a. All information system assets, both digital and non-digital, as well as the facilities that house them, must be categorized into security categories. These categories should be based on the potential impact on the College should certain events occur that jeopardize the confidentiality, integrity, and availability of the information and information systems. Impact on all processes and personnel internal and external to the College should be considered in the security categorization of the system. System owners are encouraged to consult the NIST SP 800-60 Volume 1 and Volume 2 for guidance during the categorization process.
b. System Owners should be involved in the security categorization of any information system or information system assets for which they are responsible. They should also be involved in the categorizing of systems and assets that depend on the systems they own.
c. Security categorization shall be performed early in the initiation stage of planning and implementation of any new systems or assets.
d. System Owners, members of the President's Cabinet, and the College ISA must assist with the development of the security categorization.
e. All security categorizations must be reviewed and approved by the system owner and divisional leader of the College.
f. All security categorizations must be periodically reviewed and updated as needed.
g. All security categorizations must be reviewed when information system assets, environments, or procedures change.

All data and information, digital or non-digital, that is received, created, or stored by the College is within the scope of this procedure. All data must be classified and handled in a way that protects the data from any unauthorized or accidental disclosure, modification or loss.

Risk Assessment (RA-3)

Risk assessments will take into account risks posed to the College's operations and assets. The risk assessment will also consider threats from employees or external parties. This includes cloud services providers, contractors, employees of other technical colleges, building contractors, or anyone handling data or accessing facilities with sensitive data.

The College will conduct risk assessments to evaluate the security posture, the level of risk, the likelihood of damage, and the magnitude of damage that will result from the unauthorized access, use, disclosure, disruption, modification or destruction of the information system and/or the information it processes, stores, or transmits.

The College will conduct annual risk assessments in order to ensure an acceptable security posture of its systems, assets, and data as well as to populate the risk assessment document assigned by TCSG. If there are significant changes to the critical information systems, environments, procedures, staff, or other changes or conditions that change the security posture of the College's systems, assets, and data, the system owner or system owners responsible for these systems should conduct additional risk assessment activities to assess the risk posed to those systems.

a. The risk assessment must take into account risks posed to the College's operations, assets, employees, students, alumni, and from external parties, including but not limited to the following:
    i. Contractors operating information systems on behalf of the College.
    ii. Contractors working on facilities, infrastructure, and utilities for the College.
    iii. Individuals accessing the College's information systems.
    iv. Outsourcing entities.
    v. Visitors.
b. When planning and budgeting for security/risk assessments, the College must follow these requirements:
    i. System owners are strongly encouraged to coordinate with other internal and external entities that also use the same systems, have control over common systems, or will be impacted by changes in that system.
    ii. The College shall conduct an assessment using the NIST SP 800-53 controls to evaluate their critical systems at a minimum.
    iii. If the College stores, processes or transmits sensitive data, then system owners are encouraged to consult TCSG staff with expertise on those systems.
c. Potential weaknesses in information systems, processes, procedures, environment or any other variable in the system will be added to the risk register of the risk assessment. This will include the level of risk, controls already in place, plan for corrective action, milestones along the way, and date of completion in the risk register of the risk assessment spreadsheet or subsequent document(s).

Risk Assessment/Analysis

Risk assessment or analysis is the act of documenting risks and analyzing their impact in order to determine:

a. The probability or likelihood that the risk will occur.
b. The impact of the risk if it occurs.

Each division will create a BIA for all systems that fall under that division. These BIAs will be included in the risk assessment. They will outline the most significant threats to business continuity as well as information systems and assets as well as the financial impact that may result. Further, each division will identify any work-arounds or mitigations that may be implemented in the event of an interruption of business continuity due to a failure of the College's information systems and information system assets.

Risk Response

System owners must identify a response for each risk identified. The probability and impact of the risk will used to select appropriate actions that should be taken to mitigate the risk.

There are four major ways to address risks identified.

- Avoid the risk – Change the systems, procedures, or users involved to eliminate the threat.
- Transfer the risk – Shift the risk to another division, different employees, or even outside entities who are better able to address it or even outsource the process. Note that this does not eliminate a threat. It only makes another party responsible for addressing the issue(s). Another example of this would be some sort of insurance policy.
- Mitigate the risk – This is when the College makes changes that should reduce the probability and impact of risk threat to a level acceptable to the College, TCSG, or another sanctioning body such as SACSCOC. Contingency plans are a form of mitigation.
- Accept the risk – This should be done when the risk is very low or there is no other way to address the risk.

System owners and ultimately division leadership are responsible for developing strategies and plans for handling the risk.

Risk Level, Risk Description, and Necessary Actions

- High – These are serious issues. It is mandatory to develop and implement corrective actions. Corrective action must be taken as quickly as possible based on resources and funds available. Given the seriousness of the threat, addressing these risks must be given high priority.
- Medium – A plan must be developed to correct or mitigate these threats as soon as possible. System owners should mitigate or correct problems within 3 to 6 months.
- Low – The system owner and divisional leader must decide on remedial actions or to accept the risk.

Vulnerability Scanning (RA-5)

The CPTC Risk Assessment must include the following requirements:

a. All computers and servers must have centrally-managed malware scanning software installed and updated to the most current signatures, rules and updates. The malware scanning software should also generate audit logs of malware events.
b. Real-time scanning software is preferred over scheduled scans. Files downloaded from outside sources and mobile storage devices should be scanned upon access.
c. Vulnerability scans of critical hosts in information systems and hosted applications must be performed at least every 30 days with a vulnerability scanner such as Tenable Nessus with the latest scanning engine and updates. Critical hosts should also be scanned on demand when serious vulnerabilities that may potentially affect them are identified and reported. Scheduled automatic scans are preferred over on-demand scans that are dependent on staff to carry them out.
d. Vulnerability scans should scan specific functions, ports, protocols and services that should not be accessible to users or devices. They should also scan for improperly configured or malfunctioning hosts, protocols, and services.

e. Vulnerability scanning systems should scan files downloaded via Web browsers to protect the College's information systems and data. This may be accomplished via next generation firewalls (NGFWs), intrusion prevention systems (IPSs), web filters, email filters, malware scanning software, or other cybersecurity system. A layered approach is preferred to relying on only one software package or system.
f. All external information systems such as servers or computers that remotely connect to the College's network through the virtual private network (VPN) or any similar remote connection must have College-approved malware scanning software installed, updated, and running.
g. Vulnerability scans should also scan subnets for printers, video cameras, industrial controls, and other subnets that may house vulnerable or misconfigured hosts
h. The college ISA or designee should perform vulnerability scans.

The College will select and implement either regularly-checked manual monitoring tools or automated monitoring tools to monitor and identify vulnerabilities on any hosts connected to the scanned subnets on the College network. Vulnerability scanning tools and techniques will be implemented that:

a. Identify vulnerabilities in different operating system (OS) platforms, software flaws, and improper configurations
b. Automate as much of the vulnerability management process as possible within the constraints of available budget
c. Measure and convey the magnitude of the impact of detected vulnerabilities in easy-to-read reports. The most common way to do this is by assigning a Common Vulnerability Scoring System (CVSS) score or Common Vulnerabilities and Exposures (CVE) score to the vulnerability.
d. Give instructional assistance to IT staff for remediation of vulnerable assets

The College ISA or designee will share vulnerabilities discovered with system owners and staff who support those systems. The system owner or the College ISA will assign the vulnerabilities to responsible employees or partners to ensure that the vulnerabilities are remediated, the vulnerable components or systems replaced, or mitigating procedures are implemented. Examples of ways to remediate systems are to perform upgrades, apply updates, or apply patches. Examples of mitigating procedures are blocking ports or services on a firewall, applying an ACL on the firewall or core switch, or moving the equipment to a secured location if the issue is one of physical security.

Scans should be scheduled or manually run at times when they will cause as little impact on availability or performance as possible.

Vulnerability Risk Ratings

When possible, scanning tools should be selected that assign a Common Vulnerability Scoring System (CVSS) score to assess the severity of vulnerabilities. CVSS scores are based on open standards and are calculated on a scale from 0 (low severity) to 10 (critical severity). They measure the impacts on confidentiality and integrity of data as well as the impact of availability on systems and services.

The CVSS v3.1 risk ratings are listed below with a brief description of each.

a. Critical – CVSS falls between 9.0 and 10.0 – Vulnerabilities with a critical CVSS have the highest possible severity if exploited. In addition, these are frequently easier to exploit. Therefore, these typically have the highest priority for being addressed and should be remediated or mitigated as quickly as possible if not immediately.

b. High – CVSS falls between 7.0 and 8.9 – These vulnerabilities still have high severities if exploited. Urgency is lower than those with critical CVSS scores, so they will typically be addressed after those with critical CVSS scores.

c. Medium – CVSS falls between 4.0 and 6.9 – Urgency for remediating or mitigating this type of vulnerability still exists, but these should be addressed after vulnerabilities with critical and high CVSS scores.

d. Low – CVSS falls between 0.1 and 3.9 – Though system owners should still strive to remediate or mitigate these vulnerabilities, the severity of these is far less than those of higher scores. Therefore, these typically have a lower priority for being addressed.

Note that CVSS scores measure severity, not risk. Severity is a variable that affects the calculation of potential risk, but it is not a direct measurement of risk. For example, a completely isolated system with a CVSS score would be a lower risk than another system with a medium CVSS score that was openly accessible.

Vulnerability Information Review and Analysis

a. System owners should regularly review sources of vulnerability information for all College systems. Sources of this information can be gathered from:

    i. TCSG staff.

    ii. CPTC IT staff and system owners.

    iii. System and software vendors such as Cisco, Microsoft, and Ellucian.

    iv. Other reliable resources such as the Vulnerability Summary of the Week from CISA or advisories from MS-ISAC.

b. Information regarding vulnerabilities discovered shall be shared with and explained to the appropriate College employees, including the ISA.

c. Appropriate College personnel shall be alerted or notified immediately (or as quickly as possible) about warnings or announcements involving vulnerabilities with **Critical** or **High** CVSS scores.

Requirements for Compliance

a. The College will adhere to the TCSG IT System Maintenance Standard in the TCSG Information Security Standards (ISS). Any places where CPTC procedures conflict with TCSG policies and procedures, the TCSG policies and procedures will take precedence.

b. System owners and administrators must plan to ensure resiliency during system maintenance such as upgrades, updates, patches, and reconfigurations in order to ensure high availability of critical systems.

c. System owners and administrators must develop a roll-back plan in the event of a failure in system maintenance.

d. System owners and administrators must employ automated patching mechanisms to schedule and conduct system maintenance where appropriate and when possible.

e. No out of support products shall be utilized if there is a comparable product available with support.

f. Maintenance windows for system or application upgrades, updates, patches, or other maintenance should be scheduled outside normal business hours when possible.

g. The TCSG Chief Information Officer (CIO) or the TCSG Information Security Officer (ISO) or the CPTC Information Security Administrator (ISA) can declare an out-of-band system maintenance window to perform the critical maintenance when a critical Application or Operating System patch is needed.

h. Logs of who, when, what and why a system is being maintained should be kept.

i. The College will ensure system maintainers have a predetermined time window with adequate time to perform necessary system maintenance.
j. If system maintenance can be performed with a high confidence that there will be no interruption in service or performance degradation, system maintenance can be performed during the business day.
k. If maintenance is required outside normal business hours and the system(s) must be up and reliable when business resumes, key staff who use affected systems must be available to test their parts of the system upon completion of system maintenance to ensure all systems work as intended.
l. The system owner is responsible for ensuring that system maintenance and upgrades are applied in a timely manner. The system owner can delegate system maintenance to other staff in their area or may request assistance from staff in other departments or divisions.
m. The College ISA and system owners will monitor vulnerability scans, industry newsletters, vendor emails, TCSG notifications, or any other notification method typically used to gain information regarding system vulnerabilities, and will assign remediation or mitigation to the appropriate system administrators, TCSG contacts, vendors, third-party service providers, or other appropriate contacts to schedule a maintenance window.
n. The system owner or CPTC division leader will communicate any operations that may cause system downtime or performance degradations and coordinate with impacted divisions and departments to schedule a maintenance window. If no downtime or performance degradation will result, no maintenance window may be needed. As a courtesy, system owners should still notify everyone who uses a system of any changes, scheduled or unscheduled, that may have unexpected impacts.

Responsibility

The Executive Director of Information Technology has the overall responsibility for ensuring this procedure is implemented.

Adopted: May 20, 2020
Revised: September 19, 2023