UNIVERSITY OF CALIFORNIA

Ethics, Compliance and Audit Services

Cybersecurity Reference Guide for UC Leadership

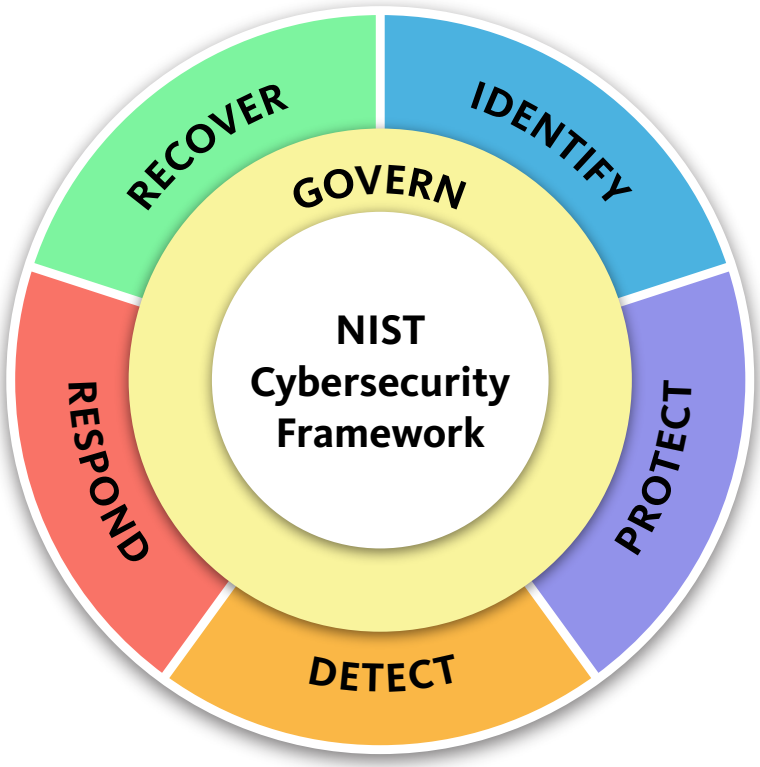
TABLE OF CONTENTS

INTRODUCTION

The *National Institute of Standards and Technology's Cybersecurity Framework* (NIST CSF) is a standard developed by the federal government to help organizations effectively manage cybersecurity risks. Leading organizations across the country, including the University of California (UC), have adopted the NIST CSF to facilitate cybersecurity risk management efforts.

This reference guide is designed to help UC leaders meaningfully engage with information security professionals on cybersecurity risk management issues through the lens of the NIST CSF to facilitate informed decision-making.

AN OVERVIEW OF THE NIST CSF



The first two functions of the NIST CSF — **Identify** and **Protect** — help an organization safeguard its most valuable IT assets and prevent attacks using a risk-based approach.

Recognizing that an organization cannot prevent every attack from occurring, the next three functions — **Detect**, **Respond** and **Recover** — guide an organization through its efforts to identify potential malicious activity, respond to attacks and return to steady state operations after an event.

The overarching NIST CSF function is **Govern**, which addresses how an organization's cybersecurity efforts are established, communicated and monitored.

HOW TO USE THIS DOCUMENT

This document is a quick reference guide to assist UC leaders in their oversight role. It provides an overview of the six functions of the NIST CSF. Each of the functions is divided into categories that address specific cybersecurity outcomes. Each function section within this document reviews selected critical categories indicated in bold below.

Function	Category
GOVERN	Organizational Context **Risk Management Strategy** **Roles, Responsibilities, and Authorities** Policy Oversight **Cybersecurity Supply Chain Risk Management**
IDENTIFY	**Asset Management** **Risk Assessment** **Improvement**
PROTECT	**Identity Management, Authentication, and Access Control** **Awareness and Training** **Data Security** Platform Security Technology Infrastructure Resilience
DETECT	**Continuous Monitoring** **Adverse Event Analysis**
RESPOND	**Incident Management** Incident Analysis **Incident Response Reporting and Communication** Incident Mitigation
RECOVER	**Incident Recovery Plan Execution** **Incident Recovery Communication**

Within each category, you'll find:

- A description of the category and **why it matters** to you
- **Key questions to ask** information security leaders and the answers you should expect
- **Information to request** from them to meaningfully assess the effectiveness of risk management efforts and descriptions of expected deliverables

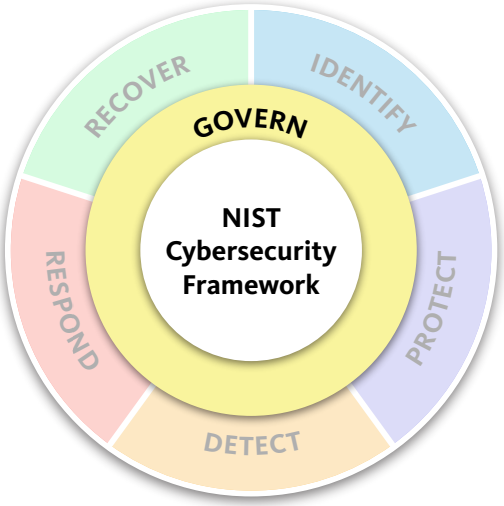
In instances where requested information is not readily available, information security leaders should work with leadership to evaluate the feasibility of producing the requested information with available resources.

The appendices to this document include a glossary of commonly used cybersecurity terms and a list of websites relevant to cybersecurity risk.

Return to table of contents.

GOVERN:

Navigating cybersecurity governance



The "Govern" function is designed for the organization's leadership and sets the foundation for a robust cybersecurity governance structure. This involves establishing strategy, expectations and policies to guide and oversee the organization's cybersecurity risk management activities. Ultimately, the "Govern" function aims to integrate cybersecurity considerations into the organization's broader governance and risk management strategies, fostering a culture of informed, risk-based decision-making across the organization.

This section focuses on three categories within the "Govern" function:

- **Risk management strategy** involves identifying, assessing and prioritizing risks, then implementing appropriate measures to align UC's strategy with its overall risk appetite and enterprise goals. Continuous evaluation and adaptation of the strategy is necessary to address evolving cybersecurity threats. This ensures that UC's defensive measures are in step with its risk management objectives.
- **Cybersecurity supply chain risk management** focuses on identifying and managing risks associated with suppliers and third-party service providers and aligning their security practices with UC's standards. Among other things, it includes conducting risk assessments and establishing security requirements. This reduces the risk of UC's cybersecurity efforts being undermined by its supply chain ecosystem.
- **Roles, responsibilities and authorities** clarifies and formalizes cybersecurity roles, their responsibilities and their authority within UC so that all individuals involved in the cybersecurity program understand what is expected of them. Establishing this clear governance structure promotes accountability and facilitates effective decision-making.

Return to table of contents.

RISK MANAGEMENT STRATEGY: Navigating uncertainty

In the dynamic world of cybersecurity, uncertainty is possibly the only given. UC's success in proactively countering cybersecurity threats hinges on identifying and regularly updating its assessment of where risk exists. Leadership at all levels should actively participate, setting clear priorities, understanding threats, defining our risk tolerance and embedding these principles into systemwide decision-making. An effective cybersecurity risk management strategy helps enable the University to achieve its mission to provide education, research and public service.

GOVERN

Why risk management strategy matters

1. **Appropriate security posture:** By understanding and prioritizing risks, UC can tailor its security practices to effectively safeguard its most *critical assets*. This ensures that UC's cybersecurity measures align with its overall risk appetite, institutional goals and strategic vision.
2. **Proactive risk identification:** Regular *risk assessments* identify potential vulnerabilities and threats before they impact UC's operations. Proactively implementing preventative measures reduces the likelihood of significant security incidents.
3. **Dynamic response to evolving threats:** A well-defined risk management strategy provides a framework for *continuous monitoring*, evaluation and adaptation of security measures. This ensures that UC's defenses evolve with the changing threat landscape.

KEY QUESTIONS TO ASK

Question	You should expect...
How does UC update its cybersecurity risk management objectives for the short and long term?	An explanation that describes regular risk assessments, alignment with business priorities, consideration of emerging threats and periodic reviews to ensure objectives remain relevant.
How does UC ensure that leaders across the enterprise are engaged in defining cybersecurity objectives and standardizing risk and performance management?	A description of regular, structured reporting on cybersecurity to senior leaders. To ensure leadership can provide informed oversight, the reporting should include clear metrics and concise descriptions of how relevant information is gathered, tracked and communicated to leadership at various levels.

Question	You should expect...
How is the risk appetite determined at UC, and how are these levels of acceptable risk communicated across the enterprise?	An explanation of how the risk appetite is established by the board, clearly defined in policy and kept up to date, ideally through an annual review. This policy should be tailored to reflect the specific risk landscapes of different UC locations and be communicated throughout the location. Along with the risk appetite, guidance should be provided on how the appetite should be incorporated into risk management processes, including any specific expectations for cyber risk efforts (e.g., minimum standards for end point protection, timeliness expectations for applying software updates to critical systems). UC locations should determine their risk appetite in accordance with the *Digital Risk Appetite Statement* adopted by the Board of Regents.

GOVERN

INFORMATION TO REQUEST

Metric or report	You should expect...
Risk tolerance statement	A statement adopted by the Board that clearly defines the maximum level of risk UC is willing to accept and the date that the statement was most recently updated. Expect this statement to be reviewed and updated at least annually or in response to significant changes in the cybersecurity landscape or UC's operations.
Risk tolerance guidelines	Written guidance on how to incorporate systemwide risk tolerance into decision-making at various UC locations. These guidelines should translate the overarching risk tolerance statement into actionable strategies for local decision-making.
Risk reporting criteria	A clear set of documented criteria indicating when and how risks should be reported to senior leadership and the Board based on predefined risk tolerance levels, enabling the Board to guide risk-based decision-making effectively.
Outstanding cybersecurity audit findings	A documented summary of outstanding high-risk or significant cybersecurity-related audit findings for each location, including detailed timelines for remediation or justification for accepting certain risks. This description should identify areas requiring additional attention or resources.

Return to table of contents.

ROLES, RESPONSIBILITIES, AND AUTHORITIES: Clarifying the chain of command in cybersecurity

Establishing a clear governance structure for UC that delineates who is responsible for what before, during and after a cybersecurity event helps to provide clarity. In the complex landscape of cybersecurity, this clarity is crucial for keeping the necessary stakeholders from unintentionally working against each other.

GOVERN

Why roles, responsibilities, and authorities matter

1. **Enhanced accountability:** Clearly defining roles and responsibilities ensures that everyone involved in UC's cybersecurity efforts knows their specific duties. This clarity fosters accountability, efficiency and effectiveness.
2. **Streamlined decision-making:** Defining who has the authority to make critical decisions increases the speed and effectiveness of the decision-making process. This reduces delays and increases the likelihood that the actions taken are in line with UC's overall cybersecurity strategy.
3. **Coordinated response:** Clarifying roles and responsibilities increases the likelihood that efforts are aligned, duplication of work is prevented and resources are used optimally. This more efficient use of staff increases the cohesiveness of our response.

KEY QUESTIONS TO ASK

Question	You should expect...
Have we allocated resources (people, processes and technical) commensurate with our cybersecurity risk and our cybersecurity risk management program?	A succinct evaluation of whether the current mix of personnel, technology, and processes aligns with identified cybersecurity risks and objectives. Any gaps should be highlighted and accompanied by actionable adjustments.
Do our human resources practices address cybersecurity?	Practical examples of the integration of cybersecurity in HR practices, from embedding security awareness in onboarding and training to incorporating cybersecurity responsibilities in job roles and evaluations.
Have we memorialized cyber risk management roles and responsibilities in policy?	An explanation of how cyber risk management roles and responsibilities are defined clearly, documented in organizational policies, updated regularly and communicated across the organization.
How do we ensure management roles and responsibilities for cybersecurity are being exercised in accordance with policy?	An explanation of how roles and responsibilities are reinforced through regular training, performance reviews and periodic assessments. This should also include how management is held accountable for setting the right tone at the top for cybersecurity.
How do we ensure that entities we acquire or manage are incorporated into our cybersecurity risk management program, where appropriate?	A description of a structured approach to integrating acquired entities into UC's cybersecurity risk management program. This should include a process for identifying cybersecurity risks specific to the new entity, assessing their existing security posture and aligning the acquired entity's cyber risk management program with UC's overall risk management strategy.

INFORMATION TO REQUEST

Metric or report	You should expect...
Vacant cybersecurity-related roles	Regular reports on the number of open cybersecurity positions, details on the efforts to fill these roles and descriptions of the impact of these vacancies on the organization's cybersecurity posture. This information should include descriptions of how the risks posed by these vacancies are being mitigated in the short term.
Cybersecurity risk management roles	A list of cybersecurity risk management responsibilities defined in policy and the personnel who have been assigned these roles. Relevant policies should exhibit a sufficiently granular level of detail to guide UC through an actual cyber incident and be comprehensive, current and actionable.
Multiple-location roles	A list of the cybersecurity-related roles that are responsible for managing systems and processes that are present at multiple locations. Expect a description of the role and how coordinated cybersecurity efforts are effectively communicated and understood, especially in complex or distributed organizational structure.

Return to table of contents.

GOVERN

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT: Securing the links

In an interconnected world, an organization is only as secure as its supply chain. UC's own cybersecurity depends on its ability to safeguard its ecosystem from vulnerabilities that emanate from third-party vendors and partners.

GOVERN

Why cybersecurity supply chain risk management matters

1. **Enhanced security posture:** By identifying risks presented by suppliers, UC can direct those suppliers to align their practices with its own security standards. This helps to eliminate gaps in UC's defenses that could otherwise lead to breaches that compromise sensitive data.
2. **Strategic management of external risks:** Through *risk assessments* of suppliers, evaluations of their security measures and determinations about their impact on our cybersecurity posture, UC can engage in strategic decision-making about which suppliers to engage with and under what conditions. This can mitigate potential risks at their source.
3. **Identification of emerging threats:** Continuously monitoring the security practices of suppliers provides insight into changes in the threat landscape. This facilitates the identification of emerging risks and the implementation of appropriate countermeasures, ensuring the integrity of the supply chain over time.

KEY QUESTIONS TO ASK

Question	You should expect...
Do we implement a uniform method for onboarding suppliers and is the scrutiny level adjusted for those handling sensitive data or systems?	A description of the onboarding process for suppliers reflecting application of greater scrutiny to suppliers that handle sensitive data or systems. The description should include the minimum cybersecurity requirements that all suppliers being onboarded must meet, and the elevated requirements for suppliers accessing sensitive information. Any challenges or gaps in performing assessments prior to finalizing contracts with suppliers (e.g., insufficient resources to perform assessments) should be noted. Regular monitoring should be established to ensure compliance.
Is there an established, efficient process for limiting access and, if necessary, quickly offboarding suppliers when risks are detected?	Written procedures for terminating suppliers' access to UC systems and data once the term of the agreement ends or if those suppliers have committed a significant violation of contract terms related to cybersecurity risk.
If there is a cybersecurity incident with a supplier, how do we ensure timely and uniform risk communication across all of UC?	A description of a streamlined process for incident reporting. This process should include identifying all affected UC operations and the impact on those operations. The process should also include guidance for escalating the issue to different levels of UC leadership based on the severity of the incident. The incident response process and expectations for reporting to UC leadership should be documented, well publicized and consistently followed.

Question	You should expect...
How do we ensure through our contracts that our suppliers are conducting proper maintenance to protect UC's data?	A description of standard contract terms for cybersecurity that are included in all contracts that are associated with University IT systems or data. The terms should clearly outline obligations for suppliers to maintain and periodically test the security of those systems. The response should also address how they ensure that contracts with both new and long-standing suppliers include these terms. These terms should subject high-risk suppliers' protective measures to increased scrutiny.

GOVERN

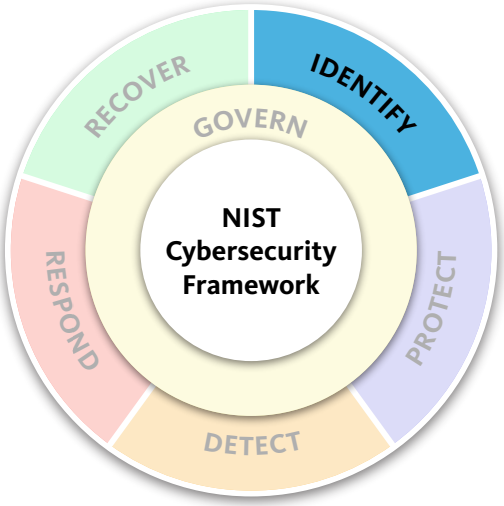
INFORMATION TO REQUEST

Metric or report	You should expect...
Suppliers with UC system and data access	A report listing UC suppliers with access to UC systems and data, including which ones have access to sensitive systems or data.
Supplier onboarding and offboarding compliance	The number of suppliers that are noncompliant with onboarding and offboarding procedures and an action plan detailing how and when these suppliers will be brought into compliance or be offboarded. Offboarding procedures should establish timeliness standards for supplier offboarding after contract termination.
Supplier cybersecurity incidents	Listing of the number of suppliers that have escalated cybersecurity incidents or concerns to UC in the past year. This listing should include a trend analysis of these incidents, an analysis of common vulnerabilities and a description of proactive measures that are being implemented to reduce future incidents from occurring.
Contracts not updated with current security terms	A report on the number of supplier contracts with terms that do not reflect current cybersecurity standards and practices, along with a timeline for renegotiating or updating these contracts.

Return to table of contents.

IDENTIFY:

Understanding UC's cybersecurity landscape



The "Identify" function is the first step in mounting a defense against cyber threats. For UC to proactively protect its assets, it first needs to identify them, determine which are most critical and classify the cyber risks facing them. This section focuses on the three categories of the "Identify" function:

- **Asset management** starts by inventorying digital valuables. It requires the identification of the systems, data and infrastructure that underpin UC's mission — from research labs to student portals. This allows UC to determine what requires protection.
- **Risk assessment** is the process of identifying potential threats and analyzing their severity. This guides UC's allocation of resources to mitigate the most critical risks.
- **Continuous improvement** refers to the process of constantly learning, adapting and refining our "Identify" practices. This allows UC to stay ahead of evolving cyber threats. Cybersecurity is a marathon, not a sprint.

Return to table of contents.

ASSET MANAGEMENT:
Understanding your digital landscape

Asset management is essential to supporting an effective cybersecurity strategy, but it is not a one-time task. It entails continually identifying, documenting and monitoring the systems, devices, software and data crucial to UC's operations. This is a dynamic process that must evolve as UC's digital inventory evolves.

Why asset management matters

1. **Prioritized protection:** Asset management includes identifying UC's most critical assets — those essential to its mission and those containing sensitive information. This prioritization guides resource allocation and cybersecurity efforts.
2. **Enhanced efficiency:** A complete asset inventory facilitates various processes, including:
   - Managing software licenses and updates
   - Tracking hardware maintenance schedules
   - Responding effectively to security incidents
   - Ensuring compliance with regulatory requirements

   A centralized asset management system reduces duplication of effort for each of these processes and the likelihood that one or more processes will overlook an asset.
3. **Reduced risk:** The process of identifying digital assets often uncovers outdated systems, unauthorized devices and misconfigured software. Addressing these vulnerabilities mitigates UC's risks and prevents breaches.

KEY QUESTIONS TO ASK

Question	You should expect...
Do we have a complete and up-to-date inventory of all digital assets within UC?	A description of the inventory, the processes in place to keep it up to date and any gaps or limitations in the list of systems, data and other digital assets.
How is *vulnerability management* risk-based?	An explanation of how vulnerability management efforts are prioritized based on the potential impact and likelihood of exploitation. Vulnerability management involves finding, assessing and addressing security weaknesses in systems and software. With thousands of new vulnerabilities discovered each year and the large number of systems across UC, a risk-based approach helps ensure the most critical vulnerabilities are addressed first.
Have we identified and prioritized our most critical assets based on their sensitivity and importance to our mission?	A clear explanation of the methodology for identifying and prioritizing critical assets that includes the factors considered, such as data sensitivity, operational impact, and alignment with the organization's mission. Expect a description of the criteria used to generate the report, the frequency with which the report is reviewed, the roles involved in the process and a discussion of what changed in the most recent assessment.

IDENTIFY

Question	You should expect...
Do we have established processes for reporting, updating and maintaining asset information?	A detailed description of robust procedures for reporting, updating and maintaining asset information, including a description of how these processes are implemented and managed and assurance that these processes are regularly reviewed for efficacy and compliance with current security standards.
Are we regularly scanning our network to detect new assets and potential vulnerabilities?	A brief description of the frequency and methods used to scan the network for new assets and potential vulnerabilities, and a description of any outstanding findings and how they are being addressed to strengthen the organization's security posture. The description should address coverage of systems that are not centrally managed.

IDENTIFY

INFORMATION TO REQUEST

Metric or report	You should expect...
Up-to-date asset inventory	A current list of all digital assets, specifically highlighting the most valuable and critical.
Unpatched critical security weaknesses	A report on the number or percentage of UC's most important systems that exhibit vulnerabilities (i.e., security weak spots, such as missing *patches* or other weaknesses). Expect a description of the severity of each of these weaknesses based on industry standards, an explanation of the priority level assigned to each of them and a plan and timeline for fixing them.
High-risk legacy systems and their vulnerabilities	A documented inventory of high-risk legacy systems, a *risk assessment* of any critical vulnerabilities in these systems and a timeline for software updates to address critical vulnerabilities. If there are critical vulnerabilities that cannot be resolved through software updates, expect a description of alternative risk mitigation strategies. Any unmitigated vulnerabilities should be tracked on a register and reported to leadership regularly.
Average patch times for critical vulnerabilities	A report outlining the average time taken to patch critical vulnerabilities (i.e., the number of days between when the software patch is released and when it is applied to vulnerable systems). This information should be broken down by administrative, academic, research and clinical environments. This detail will provide an understanding of different sectors' *patch management* efficiency.
Critical asset compliance with applicable laws, regulations and UC policy	A comprehensive report that identifies all units housing critical assets, their compliance status with applicable laws, regulations and UC policies and specific instances of non-compliance. The report should outline the nature and scope of the compliance requirements, detail the impact of any non-compliance and include timelines and plans for remediation. It should also provide a summary of any approved policy exceptions, including the justification for the exceptions and the controls in place to mitigate associated risks.

Return to table of contents.

RISK ASSESSMENT:
Unmasking cybersecurity threats

Risk assessments are the cornerstone of a strong cybersecurity posture and a vital component of the NIST CSF's "Identify" function. Because technology, threats and other factors constantly evolve, UC must regularly reassess risks and align limited resources with the most pressing vulnerabilities.

Why risk assessment matters

1. **Prioritized mitigation:** Risk assessments help to prioritize vulnerabilities based on their severity and potential consequences. This enables leaders to effectively address the most critical issues first, reducing the overall risk to the organization's most valuable assets and data.
2. **Proactive defense:** Identifying vulnerabilities before they are exploited allows UC to implement preventative measures and close security gaps. This reduces the likelihood of data breaches and operational disruptions.
3. **Compliance with regulations:** UC is subject to various regulations that require it to implement appropriate cybersecurity controls. A risk assessment can help UC demonstrate that it is meeting these compliance requirements.

IDENTIFY

KEY QUESTIONS TO ASK

Question	You should expect...
Do we have a defined process for conducting regular risk assessments across all UC locations?	A description of a consistent and repeatable risk assessment process that is applied at all UC locations. The description should describe the frequency of assessments, the standards or frameworks in use and how assessments are adapted to different UC environments while maintaining a unified approach to risk management.
Are our assessments comprehensive and tailored to our specific IT environment, including *critical assets*, data and systems?	A description of how the risk assessments address the full spectrum of UC's IT environment. Expect details on how the assessments account for any specific threats or vulnerabilities inherent to UC's operations and the unique characteristics of its critical assets, data and systems.
Do we have a clear methodology for scoring and prioritizing risks based on their severity and likelihood?	An explanation of the methodology used to evaluate risks, including the criteria for classification, the scoring scale for assessing severity and likelihood and how these scores guide decision-making. The response should outline the process for determining which risks demand immediate action versus those that should be monitored, supported by examples of thresholds or triggers that inform these decisions.
Are risk assessment results effectively communicated to leadership and responsible personnel to inform decision-making and resource allocation?	An overview of how risk assessment findings are documented, the format and frequency of reports to leadership and the protocol for informing and equipping responsible personnel to act on the assessment's findings.

INFORMATION TO REQUEST

Metric or report	You should expect...
Risk assessment status	A summary report describing the current status of cybersecurity risk assessments across the organization. The report should address whether each assessment adheres to the systemwide risk assessment methodology. The report should also describe the scope (the units and systems that were assessed), key findings and any deviations from the standard process.
Mitigation plans for critical risks	A description of the most severe and highest impact risks identified during the assessments and plans to mitigate those risks. The information should be presented in a non-technical fashion and should describe the severity and potential impact of the risks. Any risks that have not been mitigated should be clearly communicated so that leadership can determine whether to accept the risks or allocate resources to mitigate them.
Outstanding risks and material program gaps	A report describing risks or gaps in the cybersecurity program that were identified in the prior risk assessment, but have not yet been addressed. This report should explain why these issues have not been addressed and a timeline for expected resolution.

Return to table of contents.

IDENTIFY

IMPROVEMENT:
Building resilience in cybersecurity

In the world of cybersecurity, threats evolve constantly, and new vulnerabilities emerge. Continuous improvement is a commitment to embrace innovation and proactive strategies that keep our practices effective.

Why improvement matters

1. **Preparedness in the face of change:** *Tabletop exercises* and regular testing of *incident response* plans and disaster recovery procedures help to identify gaps and vulnerabilities. This allows UC to prevent and respond to attacks more effectively.
2. **Collective knowledge for collective defense:** Insights gleaned from security incidents, exercises and industry trends should be shared across all locations. This fosters collaboration and a unified approach to cybersecurity.

IDENTIFY

KEY QUESTIONS TO ASK

Question	You should expect...
How do we stay informed about emerging threats, regulatory developments and technological advancements?	A description of practices for monitoring and analyzing emerging cybersecurity threats, regulatory developments and technological advancements. This could include subscriptions to *threat intelligence* feeds, participation in industry and government cybersecurity forums and collaborations with cybersecurity research institutions. Expect an explanation of how this information is used to improve UC's cybersecurity strategies and defenses.
Is there a system in place for sharing lessons learned and best practices across the organization?	A description of a structured system, process or platform for sharing cybersecurity incidents, lessons learned and best practices across the organization. This system could consist of internal communication channels, regular meetings, collaborative tools or a combination of these elements. Expect details on how information is collected, analyzed and disseminated to all relevant personnel so that they can apply the insights to the cybersecurity functions they manage.
Are we exploring innovative technologies and partnerships to enhance our cybersecurity posture?	An outline of current efforts and future plans to explore and adopt innovative cybersecurity technologies and strategic partnerships. Examples include: • Piloting new security tools • Engaging with cybersecurity startups • Participating in industry consortiums A complete response should provide rationales for how these efforts are expected to improve the organization's cybersecurity posture and the challenges or considerations posed by integrating them into existing systems.

INFORMATION TO REQUEST

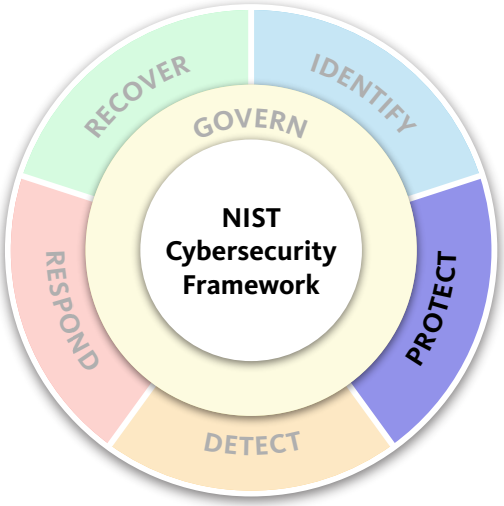
Metric or report	You should expect…
Tabletop exercises conducted	A report detailing the number and types of tabletop exercises performed, the specific scenarios, the departments involved and a summary of the outcomes and any action items.
Number of documented risk acceptances	A count of instances in which the location has decided not to take action to fully mitigate a cyber-related risk and a separate count of those risk acceptances that required Office of the President approval because of the magnitude of the risks involved, as defined by the *Digital Risk Appetite Statement* adopted by the Board of Regents. Decisions to accept cyber-related risks should be informed by the Digital Risk Appetite Statement and the associated guidance.
Impact of investments in cybersecurity	A list of cybersecurity investments (e.g., hiring of additional staff, implementing new cybersecurity tools, additional services provided by cybersecurity firms to help monitor for attacks) and the associated tangible outcomes, such as reduced incident rates, improved response times or improved outcomes from regulatory enforcement and litigation.
UC incidents originating from third parties	A summary of incidents impacting UC during the past year that arose from non-UC entities that house or process UC data. The summary should describe the nature of each incident, the impact to UC and the measures taken to address and prevent future incidents of a similar nature.

Return to table of contents.

IDENTIFY

PROTECT:

Minimizing impact



The "Protect" function focuses on implementing safeguards to maintain the confidentiality, integrity and availability of UC systems and data. UC cannot protect everything equally. For this reason, the "Protect" function takes a risk-based approach, leveraging the *risk assessment* processes of the "Identify" function to allocate resources to areas with the highest potential for loss or disruption.

This section highlights three of the five categories of the "Protect" function:

- **Identity management, authentication, and access control** addresses who has access to UC's systems and data through identity verification and role-based controls. This reduces the risk of unauthorized individuals obtaining access.
- **Awareness and training** educates students, staff and faculty about safe practices (e.g., phishing awareness, the importance of secure passwords) so they can recognize and mitigate cybersecurity threats. This equips stakeholders with the knowledge necessary to help safeguard UC's digital environment.
- **Data security** includes measures to secure data, such as encryption, data minimization and regular security assessments. These measures protect information from unauthorized access, disclosure or theft.

Return to table of contents.

IDENTITY MANAGEMENT, AUTHENTICATION, AND ACCESS CONTROL: Securing access

Identity management, authentication and access control are three key components of the "Protect" function. Collectively, they provide the right individuals access to the appropriate resources at the correct times. By prioritizing these three components, UC safeguards its assets against cybersecurity threats.

Why identity management, authentication, and access control matter

1. **Reduced risk of unauthorized access:** Identity management establishes the known individuals who can access UC systems, authentication uses strong protocols to verify that individuals are who they say, and access controls restrict their access to only the data and resources they need. This reduces the potential for unauthorized individuals to gain access to UC systems and data and cause harm.
2. **Improved data protection:** The amount of data exposed to any one individual is reduced by granting access based on specific needs. This minimizes the potential for accidental or malicious data breaches, protecting sensitive information and ensuring compliance with regulations.
3. **Enhanced security posture:** Strong identity management, authentication and access control practices create a layered defense against cyber threats. They enable faster *incident response* and simplify investigations.

PROTECT

KEY QUESTIONS TO ASK

Question	You should expect...
How do we manage access to our sensitive data for different groups like students and staff, and is this process uniform across all UC locations?	A detailed explanation of the access control mechanisms in place for sensitive data and assets, and specifics about how the protocols align with the risk assessment findings. The explanation should also describe how we monitor whether these measures are consistently applied throughout the organization, providing a standardized level of security.
Can you describe the specific risks that personal and mobile devices pose to our network, and how our policies are protecting sensitive data accessed on these devices?	An explanation of the specific threats posed by mobile and personal devices, such as unauthorized access, data leakage or malware. For each risk, the response should outline the corresponding policy requirements and detail any security measures that are in place such as encryption, multi-factor authentication and monitoring strategies. Additionally, the response should include a description of the process for communicating these policies to users, monitoring for compliance and updating the policies regularly to address emerging threats.

INFORMATION TO REQUEST

Metric or report	You should expect...
Critical system access control reviews	A report on the frequency and nature of evaluations of user access for the highest impact and most sensitive data and systems. This report should detail how often access control reviews are conducted and provide descriptions of the methods used, the scope of the reviews, the nature of the reviews (i.e., whether they are internal, external or both) and how the reviews align with industry best practices.
Material risks identified from audits/reviews	A comprehensive list of significant and consequential risks identified during audits and reviews, categorized by their severity and potential impact to UC. Expect an explanation of the implications of these risks and the proposed or ongoing measures to address them.

Return to table of contents.

PROTECT

AWARENESS AND TRAINING: Empowering our defenders

Strong cybersecurity isn't just about technology; it's about empowering people to be active participants in defending our digital world. UC's people are at the core of its success, but when they are handling critical data, they are also its biggest cybersecurity vulnerability. By investing in ongoing security awareness training, UC creates a community of empowered defenders. This proactive approach fosters a culture of security, minimizes risk and safeguards the critical data entrusted to UC.

Why awareness and training matters

1. **Building a culture of security:** Fostering a culture of awareness and shared responsibility starts with recognizing that everyone plays a role in cybersecurity. This recognition empowers UC's community to proactively protect valuable data.
2. **Compliance with regulations:** A comprehensive awareness training program can improve the UC community's understanding of and adherence to legal and regulatory requirements. This improves compliance with standards for handling sensitive information and can help prevent legal penalties.
3. **From awareness to action:** Effective training teaches users to identify cyberattacks, recognize and avoid phishing scams and adopt secure practices like setting strong passwords and enabling multi-factor authentication. This goes beyond basic awareness and empowers users to make informed decisions and minimize user error — a leading cause of breaches.

PROTECT

KEY QUESTIONS TO ASK

Question	You should expect...
How are we training our community members about cybersecurity, and what is their part in protecting UC?	A summary of the cybersecurity education curriculum, including a description of the frequency of training sessions and the methods used to deliver these trainings. The curriculum should detail how the content is tailored to different groups within the UC community and how it addresses the current cyber risk landscape.
What measures do we take to ensure our cybersecurity training is effective, especially for those with specific security roles?	An explanation of the metrics or feedback mechanisms used to evaluate the effectiveness of cybersecurity training programs, including specific training considerations for positions with designated roles and responsibilities for cybersecurity risk management in policy (e.g., *incident response* responsibilities). The explanation should describe follow-up actions taken to address gaps in knowledge, changes in behavior observed or improvements in security protocol adherence. Expect a description of how the effectiveness of the training is tracked over time and its impact on reducing cybersecurity incidents.

INFORMATION TO REQUEST

Metric or report	You should expect...
Cybersecurity training compliance rates	A report detailing the percentage of users who have completed cybersecurity training at each location, categorized by role (student, faculty, staff and those roles with specific cybersecurity responsibilities). These statistics should be compared against a target completion rate and identify any gaps.
Number, nature and results of cyber awareness programs	A report detailing the number and types of cyber awareness initiatives (e.g., phishing tests) performed at each location. The report should include the participation rates and the pass/fail outcomes, categorized by role (student, faculty, staff and those roles with specific cybersecurity responsibilities). Expect an analysis of trends and improvements over time.
Number and results of *tabletop exercises*	A report on the frequency, scenario types and key takeaways from tabletop exercises, categorized by location. A summary of actionable insights should describe how they have been or will be integrated into current security practices.
IT professionals who maintain a cybersecurity certification	A report on the proportion of IT staff holding current cybersecurity certifications, categorized by location. Higher percentages indicate the organization's commitment to professional development and expertise in cybersecurity.

Return to table of contents.

PROTECT

DATA SECURITY:
Safeguarding the digital vault

In today's world, data is the lifeblood of any organization. UC houses a vast repository of sensitive information from research data to student records. Protecting this information is paramount. The data security category of the "Protect" function includes data security practices such as encryption, data minimization and data backups. These measures protect data from unauthorized access, ensure its integrity and confidentiality and safely manage its storage and deletion.

Why data security matters

1. **Cyber threat mitigation:** Malicious actors constantly seek to exploit vulnerabilities in data storage and access. Strong data security measures, like encryption and secure *access controls*, minimize these risks. This safeguards UC's information from unauthorized access and potential breaches.
2. **Regulatory compliance:** Numerous regulations mandate specific data security practices and robust data security measures can help ensure compliance with these regulations. This prevents legal, financial and reputational ramifications.
3. **Building trust and confidence:** By prioritizing data security, UC demonstrates its commitment to safeguarding data. This builds trust within our community and strengthens our reputation as a responsible steward of sensitive information.

PROTECT

KEY QUESTIONS TO ASK

Question	You should expect...
How are our data security plans at each location shaped by our *risk assessments*?	A detailed explanation of the specific risks at each UC location identified through risk assessments and how those risks inform the data security strategies, including how the risk-based approach is integrated into security planning and operations.
What's our approach to external expert reviews of our IT systems and security measures at different locations?	Information about the process and frequency of independent third-party assessments of IT systems and infrastructure, including details on how these assessments are conducted, how often they are performed, which entities conduct them and how the findings are used to improve cybersecurity across UC locations.

INFORMATION TO REQUEST

Metric or report	You should expect...
Material gaps in data security	A list of identified security gaps (identified during the risk assessment process or elsewhere), the potential risks associated with each and how they were discovered. A clear explanation will describe the implications of these gaps on UC's operations.

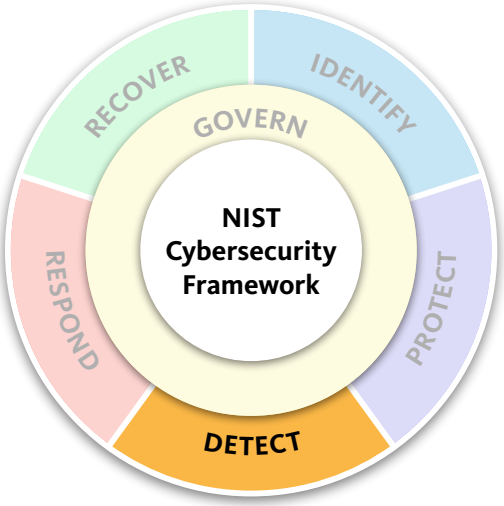
Metric or report	You should expect...
Current status of material gaps identified	An update on how each security gap is being addressed, whether through active mitigation efforts or informed risk acceptance, including any timelines for resolution or reasons for acceptance. The level of leadership accepting a risk should be aligned with the significance of the potential impact to the organization.
Noncompliance with policies	A list of any instances of material noncompliance with UC's established cyber-related policies at each location and a documented assessment of the justifications for these deviations.
Risk reports	Regular reports on identified cyber risks produced through a systematic process that include, at a minimum, an updated *risk register* for each location. This report should call out any changes since the prior report to keep leadership informed about the current risk landscape.

Return to table of contents.

PROTECT

DETECT:

Unveiling threats



The “Detect” function describes measures to identify potential cyber threats and provide early warnings. This allows UC to respond effectively and minimize potential damage.

This section examines two of the “Detect” function categories:

- **Continuous monitoring** involves deploying various tools and techniques to constantly scan UC’s systems, networks and applications for suspicious activity, potential vulnerabilities or unauthorized access attempts. This helps to identify potential security threats.
- **Adverse event analysis** investigates and evaluates the nature and potential impact of suspicious or anomalous activity. This allows UC to distinguish between false positives and genuine threats, ensuring an efficient allocation of resources and a targeted response.

Return to table of contents.

CONTINUOUS MONITORING: Vigilance in the digital age

The relentless nature of cyber threats demands constant vigilance. Breaches and attacks can occur at any time, making continuous monitoring a critical component of the "Detect" function within the NIST Cybersecurity Framework.

Why continuous monitoring matters

1. **Early detection:** Traditional point-in-time security checks leave significant gaps in our defenses. Continuous monitoring bridges this gap by constantly analyzing logs, network activity and system behavior for anomalies. This allows us to identify potential threats at their earliest stages, enabling a swift response before they escalate.
2. **Reduced impact:** Early detection of cyberattacks leads to faster mitigation and containment. This minimizes potential damage, such as data loss or operational disruptions.
3. **Improved threat analysis:** Continuous monitoring generates a wealth of data that aids in our understanding of threat patterns and attacker behaviors. This allows us to refine our security strategies and proactively address emerging threats.

DETECT

KEY QUESTIONS TO ASK

Question	You should expect...
What *critical assets* and systems are continuously monitored as part of the "Detect" function?	A concise overview of the scope of continuous monitoring, outlining the specific areas and types of systems prioritized based on their criticality and *risk assessment*. This should not be an exhaustive list, but a high-level description of the areas covered and any areas with critical assets or systems that are not covered.
How are we ensuring the efficiency and effectiveness of our continuous monitoring efforts? What measures are in place to minimize false positives and ensure timely detection of genuine threats?	An explanation of how the need to minimize false positives (unnecessary alerts) is balanced against the need for timely detection of genuine threats. This explanation should demonstrate a clear understanding of the trade-off between monitoring breadth and depth and may include a description of specific tools, techniques and metrics used to analyze and prioritize alerts.
What resources are currently allocated to continuous monitoring, including personnel, technology and budget? Do we have the necessary expertise in place to analyze and interpret the data generated by continuous monitoring?	A description of the resources dedicated to continuous monitoring, both human and technological, and processes for periodically reassessing these resources. The description of human resources should assess whether they have the necessary cybersecurity expertise to interpret data effectively, distinguish between genuine threats and false positives and leverage insights for threat analysis and improved security strategies.

Question	You should expect...
How is continuous monitoring integrated with other security functions like *incident response* and *threat intelligence*? How are potential threats communicated effectively within the organization?	An explanation of how information about potential threats is shared with relevant teams (such as an incident response team) and how timely and effective communication is provided across departments to facilitate a coordinated response. The explanation should demonstrate how continuous monitoring fits into the broader cybersecurity program.
How do we continuously improve our threat detection capabilities? What steps are being taken to adapt to evolving threats and refine our continuous monitoring program?	A report outlining the strategies for adapting monitoring based on emerging threats, learning lessons from past events and incorporating new technologies or techniques as needed. This report should showcase a proactive approach to continuous improvement and demonstrate a commitment to maintaining a strong and evolving detection posture.

INFORMATION TO REQUEST

Metric or report	You should expect...
Critical systems covered by continuous monitoring	A report outlining the number of critical systems and the percentage for which a continuous monitoring solution has been established. Expect a high percentage (ideally close to 100%) and, for any critical systems without a continuous monitoring solution, a description of the justification for the lack of a solution, the associated risks and a list of alternative security controls in place. The risks being accepted for systems without continuous monitoring should align with the *Digital Risk Appetite Statement* adopted by the Board of Regents and the associated guidance.
Mean time to detection (MTTD)	A report detailing the average elapsed time between when an incident started and when it is detected. Expect an MTTD that aligns with the nature of the systems being monitored. For high-risk areas, an appropriate MTTD might be measured in hours, minutes or even seconds. This metric should be accompanied by an explanation of the approach to MTTD for various parts of the organization, the tradeoffs of higher and lower MTTD and any recommendations about whether additional investment to reduce MTTD is warranted. The reasons for any significant increases in MTTD should be explained, and any improvement plans, such as automation or enhanced monitoring processes, should be disclosed.
False positive rate	A report of the percent of cyberattack monitoring system alerts, or detections, that are not true attacks. False positive rates should be minimized to avoid unnecessary alerts and operational disruptions, but doing so generally requires additional investments in detection capabilities. A strong response will describe the reasons for any changes in the rate and ongoing efforts to refine detection algorithms to reduce false positives.

DETECT

Metric or report	You should expect...
Security incident volume	A report on the number of security incidents during a defined period, such as quarterly or annually. Significant increases in this number and the causes of the incidents, such as evolving threats or improved detection capabilities, should be explained.
Detection capability testing frequency	A report detailing the frequency of tests to verify that detection measures are working as designed. Expect regular testing (e.g., quarterly) to support effective detection of evolving threats. The outcomes of such testing should be described, highlighting any identified weaknesses and improvement efforts.

Return to table of contents.

DETECT

ADVERSE EVENT ANALYSIS: Sifting through the noise

Continuous monitoring identifies potential threats; however, determining whether to respond and how to efficiently allocate resources in the future requires distinguishing between genuine dangers and harmless anomalies. Adverse event analysis transforms the raw data generated by continuous monitoring into actionable intelligence.

Why adverse event analysis matters

1. **Differentiate between false positives and genuine threats:** Not all suspicious activity represents a full-blown cyberattack. Analyzing the context and characteristics of an event allows analysts to distinguish between genuine threats requiring immediate action and harmless anomalies that can be disregarded.
2. **Prioritize response efforts:** Determining the severity and potential impact of each event allows for a risk-based allocation of resources. This helps ensure UC can swiftly address critical threats demanding immediate attention and take a more measured approach to investigating lower-risk events.
3. **Guide security improvements:** A thorough analysis of each event detected provides UC with insight into underlying vulnerabilities and systemic issues that may have allowed the event to occur. These insights allow UC to respond more effectively to future incidents and enhance security to prevent them from occurring.

DETECT

KEY QUESTIONS TO ASK

Question	You should expect...
How are potential adverse events identified and prioritized for further analysis?	A clear explanation of the process for detecting and evaluating potential adverse events, including how indicators of suspicious activity are identified and assessed for urgency. This description might outline specific criteria used for flagging suspicious activity, escalation procedures and the resources allocated to the initial analysis.
Does UC have the necessary tools and expertise to effectively analyze adverse events?	A response to this question should demonstrate an understanding of the capabilities required for effective analysis of adverse events. Those capabilities likely involve analytical tools (e.g., *logging*, *threat intelligence* platforms) and the necessary expertise (e.g., security analysts, incident responders) to conduct thorough investigations.
How do you ensure the efficiency and accuracy of adverse event analysis?	A description of how the analysis of adverse events includes steps to filter out false positives and measures to promote timely identification of genuine threats (e.g., threat intelligence integration, behavioral analysis and increased automation).
How is information about potential threats communicated within the organization and how does adverse event analysis inform UC's overall security posture?	A description of how findings from adverse event analyses are communicated to relevant teams (e.g., *incident response*, IT operations) and methods for using these insights to improve UC's overall security posture (e.g., updating security policies, enhancing detection capabilities).

Question	You should expect...
How do you continually improve UC's adverse event analysis capabilities?	An explanation of the approach taken to enhance UC's adverse event analysis capabilities, focusing on proactive measures to stay ahead of emerging threats. This strategy may involve incorporating lessons learned from past events, adopting new technologies or enhancing analyst training to ensure UC remains proficient in handling evolving threats. Regardless of the specific elements, the response should demonstrate a commitment to ongoing improvement.

INFORMATION TO REQUEST

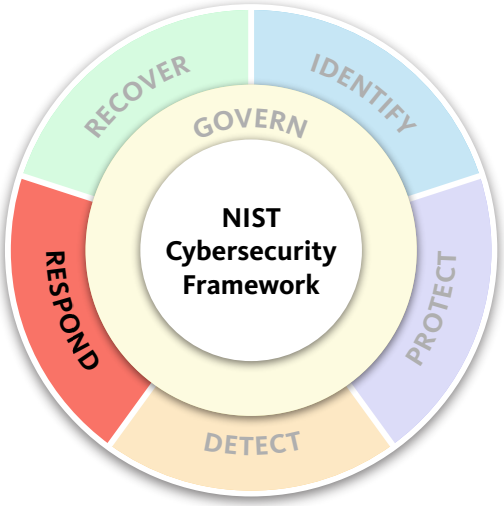
Metric or report	You should expect...
Time to analyze	A report detailing the average time between the detection of an adverse event and a determination about whether the event is a false positive, is low risk or requires further incident response. Time to analyze should be low, demonstrating prompt investigation and evaluation of potential threats. The risks and impacts associated with the current time to analyze should be described as part of the report so that leadership can decide if that time to analyze is adequate given their risk tolerance.
Percentage of events escalated to incident response	A report on the percentage of all detected events that resulted in an incident response. Leaders should monitor this metric because it can provide insight into threat identification effectiveness. Significant increases in this metric may indicate shortcomings in analysis or detection capabilities. The potential causes of any trends, such as evolving threats or changes in analysis criteria, should be described.
Security analyst workload	A report that provides a clear and quantifiable assessment of security analysts' operational load, using metrics such as the number of events handled per analyst, average time spent per event and overall resolution times. Leaders should monitor this metric to ensure security staff are not overwhelmed, which could impact analysis efficiency and effectiveness. The report should explain trends in workload and outline efforts to manage it effectively, such as automation, workload balancing or prioritization strategies.

Return to table of contents.

DETECT

RESPOND:

Reacting with resilience



The "Respond" function guides UC's management of a cyberattack's aftermath. Proactively creating a plan and defining priorities improves the effectiveness of UC's reaction to contain the attack swiftly, minimize damage and restore affected systems. A pre-defined plan should outline roles, responsibilities and communication protocols for a coordinated response.

This section highlights two of the four categories of the "Respond" function:

- **Incident management** focuses on creating and maintaining a comprehensive *incident response* plan that outlines roles, responsibilities, communication protocols and decision-making frameworks aligned with NIST CSF best practices. This facilitates a well-coordinated response with clear ownership and communication.
- **Incident response reporting and communication** describes protocols for timely and transparent communication with stakeholders throughout the incident response process. This includes defining who needs to be informed, what information should be shared and how it should be communicated within UC and, if necessary, to external parties. Efficient and timely communication minimizes confusion and improves appropriate transparency.

Return to table of contents.

INCIDENT MANAGEMENT:
Responding efficiently to cyber threats

Once UC has confirmed through analysis that it is facing a negative cyber event and has declared that the threat meets its response criteria, a pre-defined incident management process provides the following benefits.

Why incident management matters

1. **Faster containment:** Clear procedures for declaring an event, triaging and validating reports and prioritizing incidents will allow UC to minimize potential damage by quickly isolating and containing the threat. This reduces confusion and wasted time.
2. **Improved decision-making:** The plan assigns ownership for key tasks, establishes escalation protocols and outlines communication strategies. This promotes a response that aligns with the nature of the incident.
3. **Enhanced recovery:** The plan facilitates the recovery process by outlining procedures for restoring affected systems and data. This accelerates the return to normalcy and minimizes disruption to UC's operations.
4. **Continuous improvement:** The plan incorporates a process for documenting lessons learned after each event. This allows UC to continuously improve its response capabilities by identifying areas for improvement and incorporating best practices for future incidents.

KEY QUESTIONS TO ASK

Question	You should expect...
Do we have a documented, up-to-date *incident response* plan aligned with NIST CSF for incident management?	An up-to-date plan that outlines roles, responsibilities, communication protocols and decision-making frameworks for incident management. Expect a description of when the plan was last reviewed and the date of the most recent testing exercise.
Can you walk me through the key steps for handling a cyberattack, including how it integrates with our overall cybersecurity program?	An explanation of the plan's structure, including steps for: • Declaring a security incident • Triaging and validating reports • Classifying and prioritizing incidents • Assigning ownership for key tasks • Establishing escalation protocols • Coordinating communication with stakeholders Additionally, expect a description of how the incident management plan interacts with the overall cybersecurity program. For example, how findings from activities in the "Detect" function trigger the incident response plan and how efforts that are part of the "Recover" function are coordinated once the threat is contained.

RESPOND

Question	You should expect...
Who are the key stakeholders notified during an incident, and does the plan include procedures for communicating with the UC community?	An outline of the communication protocols, including which key stakeholders are notified at different stages of the incident (e.g., senior leadership, IT teams and potentially law enforcement). These protocols should include procedures for keeping the organization's community informed, considering the severity of the incident and balancing transparency with confidentiality.
How does the incident response plan incorporate lessons learned to improve future responses?	An explanation of the process for identifying lessons learned after each event and how those areas for improvement are addressed in the plan.
What are the criteria for determining if we have sufficiently mitigated the threat from an incident and can move into the recovery phase? How is that decision made?	A description of key factors used to determine that the active phase of a cyberattack is over and it is safe to begin recovery steps to restore normal operations.

INFORMATION TO REQUEST

Metric or report	You should expect...
Number of incidents escalated and level of escalation	A report on the number of cybersecurity incidents formally reported and the number of incidents reported up to each level of management defined in the incident escalation protocol. The report should break out the number of incidents reported to campus senior leadership and the number reported to the Office of the President. This provides perspective on whether the proper levels of management are being engaged and, when compared to locations across the organization, indicates whether protocols are being followed consistently.
Incident response plan testing frequency	A report detailing the timeframe (e.g., annually, biannually) for reviewing, testing and updating the incident response plan. Regular testing increases the likelihood that the plan will be effective against evolving cyber threats.
Lessons learned incorporated into incident response plan	A demonstration of how insights gained from past incidents were incorporated into the plan. This could involve showcasing specific revisions based on previous events or a process for systematically integrating lessons learned.

RESPOND

Return to table of contents.

INCIDENT RESPONSE REPORTING AND COMMUNICATION: Effective reporting during cyberattacks

A well-defined protocol for keeping stakeholders informed during a cyberattack serves as a roadmap, guiding UC's coordination with internal and external stakeholders throughout the response process. This protocol promotes clear, consistent communication, fostering trust and minimizing confusion during critical moments.

Why incident response reporting and communication matters

1. **Improved decision-making:** The protocol outlines what information needs to be reported, who needs to be informed and the appropriate cadence for updates. Timely and accurate information enables stakeholders to make informed decisions.
2. **Reduced confusion and panic:** The protocol defines responsibilities for communication, facilitating a "single source of truth" and preventing the spread of misinformation. Clear and consistent communication minimizes confusion and panic within UC and among external stakeholders.
3. **Enhanced collaboration:** The protocol outlines channels for collaboration and information exchange, ensuring a unified response effort. Effective communication fosters collaboration between internal teams and external partners, such as law enforcement.
4. **Transparency and trust:** The protocol establishes clear guidelines for what information can be shared publicly, balancing transparency with the need to protect sensitive details. Transparent communication builds stakeholders' trust in UC's ability to handle cyber threats effectively.

RESPOND

KEY QUESTIONS TO ASK

Question	You should expect...
Do we have a documented incident response reporting and communication protocol? How does it ensure timely and accurate information reaches the right stakeholders throughout the response process?	Confirmation that a documented protocol exists, outlining who needs to be informed (based on incident severity), what information needs to be reported (balancing transparency and confidentiality) and the appropriate cadence for updates. Expect an explanation of how the protocol ensures timely communication through designated channels and is publicized across the University to individuals responsible for following the protocol.
How does the protocol define responsibilities for communication during an incident?	An explanation of who has ownership for communication with different stakeholders (e.g., internal teams, the legal department, external partners).
Does the protocol address communication with external stakeholders in case of a major cyberattack?	An explanation outlining criteria, processes and tools for engaging external parties, such as law enforcement, regulatory bodies or the public, during a major cyberattack. This should include pre-approved messaging templates, guidelines for determining when and how to communicate, and identification of designated spokespersons to ensure clear and consistent public communication.

Question	You should expect...
How is the incident response reporting and communication protocol tested and reviewed? Have key personnel received training on the protocol?	An explanation of how the protocol is regularly assessed through simulations or exercises to validate its effectiveness and identify areas for improvement. Expect a confirmation that key personnel involved in incident response have received training on the protocol, ensuring everyone understands their communication roles and responsibilities.

INFORMATION TO REQUEST

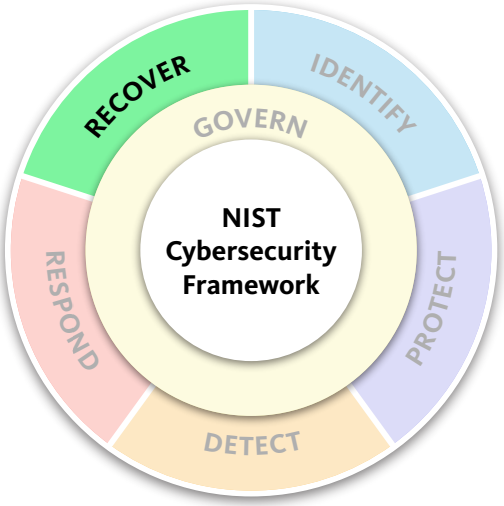
Metric or report	You should expect...
Timeliness of initial reports to key stakeholders	A report on the average time it takes to notify key stakeholders (e.g., senior leadership, IT teams) after an incident is declared. Prompt notification allows for faster decision-making. Leadership should determine if the timeliness of past performance is within its expectations.
Number of communication protocol deviations	A report on the number of times the established communication protocol was not followed during an incident response. A low number indicates consistent adherence to a protocol intended to facilitate clear and consistent messaging.
Communication training completion rate	A report outlining the percentage of key personnel who have completed training on the incident response reporting and communication protocol. A high completion rate increases the likelihood that everyone involved understands their communication roles and responsibilities.
Stakeholder satisfaction with communication during incidents	Reporting on stakeholder feedback, such as the results of surveys or feedback sessions to gauge stakeholder satisfaction with communication during incidents. Positive feedback indicates the communication protocol is effective in keeping stakeholders informed and managing expectations.

Return to table of contents.

RESPOND

RECOVER:

Resuming normal operations



The “Recover” function is the roadmap for rebuilding affected assets and operations after a cyberattack. A well-defined plan leverages people, processes and technology to efficiently restore systems, data and operations. Effective recovery plans are cross-functional, involving collaboration between IT, legal and communication teams.

This section focuses on the two categories within the “Recover” function:

- **Incident recovery plan execution** focuses on documenting and testing a plan for restoring affected systems and data, minimizing downtime and ensuring a smooth return to normal operations. Effective execution of this plan requires the establishment of clear roles, responsibilities and communication protocols for all teams involved.
- **Incident recovery communication** addresses establishing protocols for informing stakeholders about the incident’s impact, recovery progress and expected timelines. Such protocols encourage timely and effective communication that minimizes confusion and fosters trust.

Return to table of contents.

INCIDENT RECOVERY PLAN EXECUTION: Restoring operations

The aftermath of a cyberattack can be chaotic. However, a well-defined and tested incident recovery plan can help UC act swiftly and efficiently.

Why incident recovery plan execution matters

1. **Reduced downtime:** The plan outlines the steps for restoring affected systems and data. This reduces downtime and increases the speed with which UC returns to normal operations, reducing disruption to its essential functions.
2. **Efficient resource allocation:** The plan assigns clear roles and responsibilities for each team involved in the recovery process, defining each individual's tasks. This allows for more efficient resource allocation and a coordinated response.
3. **Improved decision-making:** The plan provides a framework for making informed decisions throughout the recovery process, including defined escalation protocols and clear communication channels. This provides everyone involved with the necessary information to act effectively.

KEY QUESTIONS TO ASK

Question	You should expect...
How comprehensive is our incident recovery plan?	A detailed plan for each location that identifies and addresses all *critical assets* and functions.
How frequently is our incident recovery plan updated?	The plan should be updated at least annually — or after significant changes to the IT environment or business structure — to reflect changes in the threat landscape, technology and business processes.
What is our process for testing the incident recovery plan?	A description of a structured process for regular testing, such as *tabletop exercises*, simulations or live drills, and the various scenarios these tests have addressed, including ransomware attacks, data breaches and system failures. The frequency of these tests and the lessons learned from them should be documented and used to refine the recovery plan.
What metrics do we use to evaluate the effectiveness of our incident recovery efforts?	A list of specific metrics like recovery time objective (RTO), recovery point objective (RPO), system downtime during incidents and the time to return to normal operations. Expect a description of how these metrics are used to assess improvement or degradation in recovery capabilities.

RECOVER

Question	You should expect...
How are incident recovery roles and responsibilities defined and communicated across the organization?	An explanation of how the incident recovery plan clearly defines roles and responsibilities for all personnel involved in recovery efforts, specifying tasks and decision-making authority. The explanation should also describe how this information is communicated to relevant stakeholders, such as through training and awareness programs, to help ensure personnel understand their roles and responsibilities during an incident.
In the event of a significant cyber incident, how do we ensure business continuity?	A detailed description of specific strategies and solutions in place to maintain critical operations during a cyber incident, such as redundant systems, data backups, alternative processing sites and communication to affected stakeholders. This should include a description of how we have coordinated — and how we will coordinate — with external partners, such as cloud service providers and cybersecurity firms.
How do we incorporate lessons learned from past incidents or industry developments into our recovery planning?	A description of how lessons from internal incidents and external threats are captured, analyzed and integrated into the recovery plan. New information and insights about external threats might come from industry forums, cybersecurity *threat intelligence* sharing and recent cyber incidents.
What are the challenges or gaps in our current incident recovery capabilities, and what plans are in place to address them?	A candid description of known weaknesses or areas in the recovery plan that can be improved, and a strategy for addressing these issues. These strategies may involve investing in new technologies, deploying additional training or enhancing collaboration with external partners.

INFORMATION TO REQUEST

Metric or report	You should expect...
Testing of backups and other restoration assets	A report on the total number of backups and restoration assets and when they were most recently tested for integrity and reliability. This report should address, at a minimum, all systems that were designated as critical through the *risk assessment* process.
Recovery plan status	Detailed reports on the completeness and currency of recovery plans for each location, specifically focusing on how these plans cover critical assets identified during the risk assessment process. Reports should include any gaps in coverage of critical assets and propose actionable steps to address them.
Recovery expectations for critical shared and/or external assets	A list of critical shared or external assets (e.g., services provided by third parties), whether the associated contract includes clear expectations about the amount of time it will take to restore systems and whether that amount of time poses an unacceptable disruption to operations. A strong response will assess the risks posed by this issue and describe alternative mitigation strategies or the steps being taken to amend the contract to include such terms.

RECOVER

Return to table of contents.

INCIDENT RECOVERY COMMUNICATION:
Keeping everyone informed after the attack

In the aftermath of a cyberattack, communicating effectively with stakeholders fosters trust and minimizes confusion. Establishing clear protocols for information sharing in advance emphasizes the importance of, and facilitates, clear and timely communication.

Why incident recovery communication matters

1. **Reduced panic and confusion:** Timely and accurate updates from a central source prevent the spread of misinformation and rumors. This reduces uncertainty about when operations will resume, allowing stakeholders to focus on the recovery effort.
2. **Improved decision-making:** Stakeholders with clear information are able to make informed decisions about their own recovery actions, minimizing further disruption. These recovery actions may include transitioning from manual business processes back to IT systems once back online or temporarily implementing more stringent security measures during the recovery process.
3. **Maintaining trust and transparency:** Consistent communication fosters trust with stakeholders, both internal and external. By exhibiting transparency, UC builds confidence in its ability to handle cyber threats effectively.

KEY QUESTIONS TO ASK

Question	You should expect...
How do we communicate with internal stakeholders during and after a cybersecurity incident?	A detailed communication plan that specifies the channels, templates and protocols for communicating with internal stakeholders, including employees, management and the Board. The plan should also establish the frequency of updates and how information should be tailored for different audiences.
What is our strategy for external communication with customers, partners and the public?	A documented strategy that includes pre-defined templates for external communication, identifies spokespersons and outlines how the organization facilitates consistent and accurate messaging. It should also address compliance with legal and regulatory reporting obligations.
How do we ensure that our communication plan is up to date and reflects our current operational and business environment?	A description of a regular review process that involves key stakeholders from across the organization, including public relations, legal and operations teams. This description should address how often the communication plan is updated and pre-defined triggers for an ad-hoc review, such as significant changes in the business or the threat landscape.
Can you provide examples of how our incident communication plan has been put into practice?	A description of anonymized examples of past incidents that illustrate how the communication plan was executed, what worked well and what lessons were learned. This description should also address improvements made to the communication strategy based on these experiences.

RECOVER

INFORMATION TO REQUEST

Metric or report	You should expect...
Most recent communication plan test	A report on the date that each location most recently tested its communication plan. Plans should be tested regularly — no less than annually or following significant changes to the organization or its operational environment.
Time to notify internal stakeholders	A report detailing the average time between detecting a security incident and notifying internal stakeholders. The report should describe efforts to minimize this time.
Frequency of communication training sessions and their efficacy	A report detailing the number of instances of incident communication training sessions conducted for spokespersons and communication teams over a defined period of time. The report should also include an assessment of the training's effectiveness, such as feedback from post-incident reviews on whether the training effectively prepared participants, and suggestions for improvement.

Return to table of contents.

RECOVER

APPENDIX A:
Glossary of cybersecurity terms

A

Access control list (ACL): A list that specifies which users or groups are authorized to access a particular resource.

Access control: The security measures that define who can access a system and what they can do once they have access.

Access management: A security practice that limits resources to authorized users.

Account harvesting: The process of illegally collecting usernames and passwords, often through automated means.

Advanced Encryption Standard (AES): A widely used symmetric encryption algorithm for securing electronic data.

Advanced persistent threat (APT): A sophisticated, sustained cyber operation where an intruder establishes an undetected presence on a network to acquire sensitive data over a prolonged period of time.

Air gap: An isolation technique where two systems are physically separated to prevent unauthorized access between their networks.

Alert: A notification indicating a potential security incident.

Antivirus software: A program that scans for and neutralizes malicious software (malware).

Asset: Any data, device, system or component within an organization that has value and needs protection. This includes hardware, software, information, personnel, facilities and any other resources that support critical business functions and processes.

Asymmetric cryptography: A cryptographic system that uses a pair of mathematically linked keys: a public key for encryption and a private key for decryption.

Attack surface: The total sum of all potential entry points or vulnerabilities through which an unauthorized user could gain access to a system, a network or data. It includes all hardware, software and network components that can be exploited in a cyberattack.

Authentication: The process of verifying a user's claimed identity.

Authorization: The process of granting a user access to specific resources based on their identity and permissions.

Availability: The measure of a system's uptime and accessibility, ensuring that IT services, applications and data are accessible to authorized users whenever needed. It involves preventing and swiftly recovering from disruptions like hardware failures, software issues and cyberattacks.

B

Backdoor: A hidden method of bypassing normal authentication or security controls to gain unauthorized access to a system or network. It is often used by attackers to maintain persistent access without being detected.

Biometrics: The use of unique biological characteristics for identification and access control, such as fingerprints or iris scans.

Blacklist: A list of known malicious actors, websites or email addresses that should be blocked.

Blue team: The security professionals responsible for defending an organization's systems from cyberattacks.

Botnet: A network of compromised computers, often called "bots" or "zombies," that are controlled by a malicious actor, known as a "botmaster" or "bot herder." These infected devices can be used collectively to perform various malicious activities, such as launching distributed denial-of-service (DDoS) attacks, sending spam or stealing data.

APPENDIX

Return to Previous Location

Botnet attack: When a network of compromised devices (bots) controlled by a single attacker launches a large-scale distributed denial-of-service (DDoS) attack aimed at overwhelming websites or online services with traffic, making them inaccessible to legitimate users.

Bring-your-own-device (BYOD): A policy that allows students, faculty, employees and third parties to use personally owned devices for access purposes. Common examples include phones, laptops and tablets.

C

CIA triad: Represents the three pillars of information security where C = confidentiality assurance, I = integrity assurance and A = availability assurance.

Cipher: An algorithm for encrypting or decrypting data.

Cloud computing: Online access to a shared pool of configurable resources such as servers, storage, applications and services.

Cloud security: The practices and technologies used to secure data, applications and infrastructure in the cloud computing environment.

Confidentiality: Preserving authorized restrictions on information access and disclosure.

Continuous monitoring: A cybersecurity approach where an organization constantly monitors its digital information systems and networks to detect security threats, performance issues or noncompliance issues in an automated manner.

Critical asset: An asset whose incapacitation or destruction would have a very serious, debilitating effect on UC's ability to fulfill its mission or an asset that stores or transmits large amounts of sensitive data such as protected health information or personally identifiable information.

Critical infrastructure: Systems and assets, whether physical or virtual, so vital that their incapacitation or destruction would have a debilitating effect on security, economic security, public health or safety or any combination thereof.

Cryptocurrency: A digital or virtual currency secured by cryptography.

Cyber hygiene: The practices and steps that users and organizations take to maintain the health and security of their digital systems and devices. This includes regularly updating software, using strong passwords, backing up data and being vigilant against phishing and other cyber threats to protect against cyberattacks and ensure the integrity and safety of information.

Cyberattack: The attempt by malicious nation state actors, cybercriminals or other digital adversaries to access a network or system, usually for the purpose of altering, exfiltrating, destroying or exposing information.

Cybersecurity incident: An event that compromises the confidentiality, integrity or availability of an information system or data. This can include unauthorized access, data breaches, malware infections, denial-of-service attacks or any other activity that threatens an organization's digital assets and security.

Cybersecurity: The actions taken to defend digital assets, including networks, systems, hardware and data, from cyberattacks, breaches, insider threats and categories of non-malicious but potentially harmful activity.

D

Data breach: An incident where unauthorized individuals gain access to confidential, sensitive or protected information, often leading to the exposure or theft of personal, financial or proprietary data.

Data encryption: The process of converting plaintext information into an unreadable format called ciphertext using an algorithm and an encryption key. This ensures that only authorized parties with the decryption key can access and read the original data.

Data security: The practice of protecting digital information from unauthorized access, use or disclosure in a manner consistent with an organization's risk strategy.

APPENDIX

Return to Previous Location

Deep web: Parts of the internet that are not indexed by standard search engines and are therefore not easily accessible to the general public. It includes private databases, membership sites and other content that requires specific credentials or permissions to access.

Dark web: The dark web is a subset of the deep web that is intentionally hidden and accessible only through specialized software like Tor. It is often associated with illegal activities, such as the sale of illicit goods and services, but also hosts anonymous communication and privacy-focused resources.

Defense in depth: A security tactic using a layered approach to protect an ecosystem from cyberattacks and breaches.

Digital signature: A mathematical scheme used to verify the authenticity and integrity of a message or document.

Denial-of-service attack (DoS): A malicious attempt to disrupt the normal functioning of a targeted server, service or network by overwhelming it with a flood of internet traffic. This makes the resources unavailable to legitimate users.

Distributed denial-of-service (DDoS) attack: A type of cyberattack where multiple compromised devices, often part of a botnet, are used to flood a target with excessive traffic, overwhelming its resources and making it unavailable to legitimate users.

Drive-by download: An unintentional download of malicious software onto a user's device when they visit a compromised or malicious website. The download occurs without the user's knowledge or consent, often exploiting vulnerabilities in the web browser or its plugins.

E

Encryption: The process of transforming data into a scrambled form that only authorized users can access.

Endpoint: Any device that can be connected to a network.

Endpoint detection and response (EDR): A cybersecurity approach focused on continuously monitoring and responding to threats on endpoints, such as computers and mobile devices. It involves real-time data collection, analysis and automated responses to detect, investigate and mitigate suspicious activities and cyber threats.

Ethical hacking (penetration testing): The authorized practice of simulating an attacker's methods to identify vulnerabilities in a system.

Exploit: An exploit is a piece of code or a technique that takes advantage of a vulnerability or flaw in a software or system to perform unauthorized actions, such as gaining control, stealing data or causing harm. Exploits are often used by attackers to breach security defenses and compromise systems.

F

Fileless malware: A modern malware variant that doesn't rely on traditional files, but leverages legitimate system tools and processes to execute malicious code within memory, making it harder to detect by traditional antivirus software.

Firewall: A security device or program that controls the flow of traffic between networks or hosts.

Firmware: A type of specialized software programmed into a hardware device to provide low-level control and functionality. It operates as the intermediary between the hardware and higher-level software, enabling the device to perform its intended tasks.

Footprinting: The process of gathering information about a target system or network to identify its vulnerabilities and potential entry points. It involves techniques such as scanning, social engineering and open-source intelligence to create a comprehensive map of the target's infrastructure and security posture.

Fraud: The intentional deception for personal gain, often involving financial transactions.

H

Hardware: The physical components of a system.

APPENDIX

Return to Previous Location

Hashing: The process of converting data into a fixed-length string of characters using a mathematical algorithm. The resulting hash value uniquely represents the original data, enabling secure verification of data integrity without revealing the original information.

Honeynet: A network of decoy systems designed to attract and monitor cyberattackers. It mimics a real network environment to gather intelligence on attack methods and strategies, helping security professionals understand and mitigate potential threats.

Honeypot: A decoy system or network designed to attract and monitor cyberattackers. It serves as a trap to gather information on attack techniques and behavior, helping to enhance security defenses.

I

Incident response (IR): The approach to addressing and managing the aftermath of a cybersecurity breach or attack.

Information security: The protection of information assets from unauthorized access, use, disclosure, disruption, modification or destruction.

Institutional information proprietor: Assumes overall responsibility for establishing the Protection Level classification, access to and release of a defined set of institutional information.

Integrity: The assurance that information is accurate, is complete and has not been altered or tampered with. It ensures that data remains consistent and trustworthy from its origin to its destination.

Internet: A global network of interconnected computers and servers that communicate using standardized protocols, enabling the exchange of data, access to information and a wide range of online services. It supports various functions such as web browsing, email, file sharing and social networking.

Internet of things (IOT): A network of physical devices, vehicles, appliances and other objects embedded with sensors, software and connectivity capabilities. These devices collect and exchange data over the internet, enabling them to be monitored and controlled remotely.

K

Keylogger: A specific type of spyware that records every keystroke made on an infected device, allowing attackers to capture passwords and other sensitive information.

L

Logging: The recording of security events and activities for analysis and auditing purposes.

Logic bomb: A piece of malicious code intentionally inserted into a software system that is designed to execute a harmful action when specific conditions are met. It lies dormant until triggered by an event such as a particular date or the deletion of a specific file.

M

Malicious software (malware): Any software designed to intentionally cause damage to a computer, server, client or network. It includes viruses, worms, trojans, ransomware, spyware, adware and other harmful programs that can disrupt operations, steal data or gain unauthorized access to systems.

Malvertising: Malicious advertisements displayed on legitimate websites. Clicking on such ads can unknowingly download malware onto the user's device.

Man-in-the-middle (MitM) attack: A cyberattack where an attacker intercepts and potentially alters the communication between two parties without their knowledge. The attacker can eavesdrop, steal information or inject malicious data, compromising the confidentiality and integrity of the communication.

Metadata: Information that describes the characteristics of data viewed in the aggregate.

Multi-factor authentication (MFA): A security process that requires users to provide two or more verification factors to gain access to a system, application or data. These factors typically include something the user knows (password), something the user has (security token or smartphone) and something the user is (biometric verification such as a fingerprint or facial recognition).

APPENDIX

Return to Previous Location

N

Network: Comprises two or more computers that are connected either by cables (wired) or wireless (Wi-Fi) for the purpose of transmitting, exchanging or sharing data and resources.

Network security: The protection of a computer network from unauthorized access, intrusion, misuse, modification or destruction.

NIST Cybersecurity Framework (NIST CSF): A framework developed by the National Institute of Standards and Technology to help organizations manage their cybersecurity risk.

O

Open-source security: The practices and tools used to protect and ensure the integrity, confidentiality and availability of software whose source code is openly available. It involves community-driven efforts to identify, report and patch vulnerabilities, as well as the use of security best practices and tools to enhance the security of open-source projects.

Operational technology (OT): The hardware and software systems used to monitor, control and automate industrial processes and infrastructure. This includes systems for managing manufacturing equipment, power plants, transportation networks and other critical services, focusing on physical device operations and performance.

P

Patch: A software update that fixes a security vulnerability.

Patch management: The process of identifying and deploying software updates, or "patches," to a variety of endpoints, including mobile devices and servers.

Penetration testing ("pen testing"): A simulated cyberattack conducted by security professionals to identify and exploit vulnerabilities in a system, network or application. The goal is to evaluate the security posture and uncover weaknesses that could be exploited by malicious actors.

Personally identifiable information (PII): Information that can be used to distinguish or trace an individual's specific identity.

Phishing: An email scam that impersonates a reputable person or organization with the intent to steal credentials or obtain access to unauthorized and/or sensitive information.

Physical security: The measures taken to protect physical assets, such as data centers and servers, from unauthorized access.

Port: A virtual connection on a computer used for communication between applications.

Public key infrastructure (PKI): A framework for managing digital certificates and public key cryptography.

R

Ransomware: A type of malicious software that encrypts a victim's data or locks them out of their systems, demanding a ransom payment to restore access. It disrupts operations and poses significant financial and reputational risks to individuals and organizations.

Red team: A team that simulates attackers to test an organization's security posture.

Risk: The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

Risk assessment: The process of identifying risks to organizational operations (including mission, functions, image and reputation), organizational assets, individuals and other organizations, arising through the operation of an information system.

Risk management: The process of identifying, assessing and controlling risks arising from operational factors and making decisions that balance risk costs with mission benefits.

Risk register: A documented tool used to identify, assess and manage risks to an organization's information systems and data, detailing potential threats, their impacts and the mitigation strategies in place. It helps prioritize risks and track the effectiveness of risk management efforts.

APPENDIX

Return to Previous Location

Rootkit: A type of malicious software designed to gain unauthorized root-level access to a computer system and hide its presence from the system's users and security software. It allows attackers to maintain persistent control over the system while concealing their activities and any other malicious processes.

S

Sandbox: A secure environment used to safely execute untrusted code.

SCADA (supervisory control and data acquisition): A system used to control and monitor industrial processes.

Security awareness training: Education programs to teach employees about cybersecurity best practices.

Security policy: A document that outlines an organization's security rules and procedures.

Server: A software or hardware device that accepts and responds to requests made over a network.

Social engineering: Describes a variety of cyberattacks that use psychological tactics to manipulate people into taking a desired action, such as unwittingly giving password information.

Software: A collection of programs, data and instructions that enable a computer or device to perform specific tasks or functions. Examples of software include applications, operating systems and utilities that control hardware, execute processes and provide various services to users.

Spam: Unsolicited bulk email messages, often used for advertising or phishing attacks.

Spoofing: A cyberattack technique where an attacker disguises their identity or the origin of their communication to deceive systems or individuals. This can involve falsifying IP addresses, email addresses, caller IDs or websites to gain unauthorized access to information or trick victims into taking harmful actions.

Spyware: Malware designed to steal sensitive information from a victim's device, such as login credentials, financial data or browsing history.

SQL injection: A type of cyberattack where an attacker exploits vulnerabilities in an application's software by inserting malicious SQL code into an input field. This allows the attacker to manipulate the database, potentially gaining unauthorized access to sensitive data, modifying or deleting records and executing administrative operations.

SSH (Secure Shell): A secure protocol for remote login and command execution.

Supply chain attack: A type of cyberattack that targets a third-party vendor.

Supply chain risk: The potential for harm or compromise that arises as a result of security risks from suppliers, their supply chains and their products or services.

Symmetric cryptography: A cryptographic system that uses a single shared secret key for encryption and decryption.

System life cycle: The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

T

Tabletop exercise: A discussion-based, simulated scenario in which participants, typically key stakeholders and cybersecurity team members, walk through the hypothetical cybersecurity-related scenarios such as cybersecurity investment decisions and responses to cyber incidents. This exercise helps organizations evaluate their incident response plans, identify gaps and improve their readiness for actual cyber threats.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

Threat actor: An individual or group that poses a cybersecurity threat.

APPENDIX

Return to Previous Location

Threat intelligence: The collection, analysis and dissemination of information about cyber threats.

Trojan horse: A malicious program disguised as legitimate software.

Two-factor authentication (2FA): A security method that requires two verification factors for user access (often synonymous with MFA).

U

Unit head: A generic term for dean, vice chancellor or a person in a similarly senior role who has the authority to allocate budget and is responsible for unit performance. At a particular location or in a specific situation, the following senior roles may also be unit heads: department chairs, assistant/associate vice chancellor (AVC), principal investigators, directors or senior managers. Unit heads have important responsibilities to ensure effective management of cyber risks.

Unit information security lead (UISL): A term for the workforce member(s) assigned responsibility for tactical execution of information security activities including, but not limited to, implementing security controls; reviewing and updating risk assessment and risk treatment plans; devising procedures for the proper handling, storage and disposal of electronic media within the unit; and reviewing access rights.

V

Virtual private network (VPN): A technology that creates a secure, encrypted connection over a less secure network, such as the internet. It allows users to send and receive data as if their devices were directly connected to a private network, ensuring privacy and security.

Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability management: The systematic process of identifying, evaluating, prioritizing and addressing security vulnerabilities in an organization's IT systems and software. This proactive approach aims to reduce the risk of exploitation by continuously monitoring for weaknesses, applying patches and implementing mitigation strategies.

W

War driving: The act of searching for unsecured Wi-Fi networks.

Watering hole attack: Targeting a specific group of users by infecting a website they are known to frequent. Once a user visits the compromised site, their device becomes vulnerable to malware infection.

White hat hacker: A security professional who uses their skills for ethical purposes.

Worm: A type of malicious software that replicates itself and spreads across networks without the need for user intervention. Unlike viruses, worms can propagate independently, exploiting vulnerabilities to infect as many systems as possible, often causing widespread damage and disruption.

Z

Zero-day: A software vulnerability that is unknown to the software's vendor or developer and has not yet been patched or fixed. It is called "zero-day" because the developer has had zero days to address and mitigate the vulnerability, making it highly valuable for attackers who can exploit it before a fix is released.

Zero-day attack: A cyberattack that exploits a previously unknown vulnerability in software or hardware before the vendor has had a chance to develop and release a patch or fix. This type of attack is particularly dangerous because there are no defenses or remedies available at the time of the exploit.

Zero trust: A security strategy that requires all users to be authenticated and authorized before being granted access to applications and data.

APPENDIX

Return to Previous Location

APPENDIX B:
Relevant website links

Website	Description
Systemwide Information Security	A website that provides information on UC information security services, policies and resources.
BFB-IS-3: Electronic Information Security	A UC policy that establishes guidelines for achieving appropriate protection of University electronic information resources and to identify roles and responsibilities at all levels in the UC system.
BFB IS-3 Frequently Asked Questions	Two sets of Frequently Asked Questions to guide users interested in better understanding UC's information security policy.
IS-12: IT Recovery	A UC policy that establishes guidelines to prepare the ability to recover Institutional Information and IT Resources in the event of an unavoidable or unforeseen disaster, whether natural or human-made.
Electronic Communications Policy	UC's policy on privacy, confidentiality and security in electronic communications.
UC Information Security Incident Response Standard	A UC Standard regarding electronic information security incident response planning.
UC Breach Decision Tree	A document that guides UC locations through decisions on notification requirements for cyber incidents.
NIST Cybersecurity Framework	A standard developed by the federal government to help organizations effectively manage cybersecurity risks.
NIST Special Publication 800-53	A publication that catalogs security and privacy controls to protect systems, organizations, individuals and the U.S. from a diverse set of threats and risks.
ISO/IEC 27001:2022	An international standard to manage information security developed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
UC's Digital Risk Appetite Statement	A statement approved by the Board of Regents establishing UC's appetite for digital risk.
Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Sponsored Research and Development	Guidance on implementing NSPM-33 which established national security policy for U.S. Government-supported research and development. See pages 18-21 for cybersecurity-related guidance.
About U.S. Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) Program	CMMC is a program created by the DoD to enforce the protection of sensitive unclassified information.

APPENDIX