Example Vulnerabilities and Protection Measures

Educause Risk Framework

Phase 1, Data Collection

This document lists examples of vulnerabilities and protection measures to consider when surveying management, IT staff and end-users about IT security risks in Phase 1 of the Educause Risk Assessment Framework.

1	**Subject: IT security strategies** Target audience: Management and IT staff Vulnerability: IT security strategies are not adequate. Controls: Are IT security strategies and goals documented and communicated to employees at all levels of the organization? Are IT security strategies communicated to business associates with access to confidential data belonging to the institution? Do strategies take into consideration recent risk assessment results, business strategies and business goals? Are new security products, tools, procedures, and mechanisms routinely reviewed for applicability to security strategies? Do strategies balance security with usability? Do strategies consider cost? Are security strategies periodically reviewed and updated?
2	**Subject: IT security policies** Target audience: Management and IT staff Vulnerability: IT security policies are inadequate. Controls: Is there a documented process for the creation, deployment, implementation, and periodic review and update of information security policies? Do policies address compliance with applicable laws, contracts, and other regulations? Do policies balance security with usability? Do Deans, Directors and Department Chairs uniformly enforce sanctions for non-compliance? Do security policies cover the following topics? - Security strategy and management - Security architecture and design - Roles and responsibilities for security - Staff security training, awareness, practices - Collaborative information security for Associates such as vendors and contractors - System and network management - Access, authentication and authorization - Data classification and protection requirements - Monitoring and auditing - Change management - Incident management - Physical security - Contingency planning and disaster recovery
3	**Subject: IT security risk assessment** Target audience: Management and IT staff Vulnerability: Risk assessment and mitigation strategies are inadequate. Controls: Are procedures documented for managing information security risks? Do Deans, Directors and Department Chairs ensure that risk assessments are performed periodically, in response to incidents, and in response to major changes in technology, threats, systems and operations? Do Deans, Directors and Department Chairs consider risk when before approving projects and purchases? Was a comprehensive risk management assessment performed in the last five years? Were risk mitigation strategies reviewed during the

	last year? Do Deans, Directors and Department chairs demonstrate support by authorizing and providing resources to conduct risk assessment and for risk mitigation strategies? Does the risk assessment process engage Deans, Directors and Department Chairs to determine what level of risk is acceptable? Do mitigation strategies reflect an acceptable level of risk? Is risk assessment used to help select cost-effective security control measures that balance implementation costs against potential losses?
4	**Subject: IT asset classification** Target audience: Management and IT staff Vulnerability: Critical IT assets are not identified and classified. Controls: Are important information assets and related IT resources identified? Are they classified according to their need confidentiality, integrity and availability? Are guidelines for classification of IT assets documented? Is some method used to verify that staff understand how classify IT assets? Do Deans, Directors and Department Chairs provide adequate resources to classify IT assets? Do procedures for installing software, systems, and networks include steps to document the classification of the new IT asset? Is classification documentation periodically audited for accuracy?
5	**Subject: Data identification** Target audience: Management, IT staff and end-users Vulnerability: Systems, media and paper containing confidential data are not labeled with classification and handling instructions. Controls: Are procedures documented for labeling systems, media and paper containing confidential data? Are labels required on all media that is easily lost? Do procedures call for labels to include the data classification, distribution restrictions, and disposal guidelines? Do all employees understand and follow labeling procedures? Is compliance with labeling procedures periodically verified?
6	**Subject: System identification** Target audience: IT staff Vulnerability: System identification does not adequately reflect the security level of the system. Controls: Are procedures documented to ensure that the network address of each network node is appropriate for its security level? Are the purpose and security level of network nodes documented and matched to the documented security level for the network zone? Is compliance with these procedures periodically verified?
7	**Subject: Screening decision makers** Target audience: Management and IT staff Vulnerability: Authority for data is assigned to individuals who lack the expertise to make appropriate decisions about the protection of the data. Controls: Are candidates for positions of authority, such as Deans, Directors and Department Chairs, adequately screened to determine if they have the expertise to make appropriate decisions about the protection of data? Are steps documented in hiring procedures to ensure that candidates for positions with authority for data understand their responsibility protect data? Is some method used to: - Determine that candidates understand how data will be used throughout the institution and how it must be protected. - Ensure that candidates understand their responsibility to authorize and document users and IT staff permitted to use confidential data. - Ensure that candidates understand their responsibility to authorize and document software, systems and networks that can be used with confidential data.

	- Ensure candidates understand their responsibility to inform IT staff and users of security requirements to protect confidential data. - Ensure candidates understand their responsibility to report confidential data exposed to unauthorized individuals. - Ensure candidates understand their responsibility to enforce the institution's data security policy.' - Verify candidates skills.
8	**Subject: Screening IT staff** Target audience: Management and IT staff Vulnerability: Responsibilities for IT resources are assigned to individuals who lack the expertise to perform the duties. Control: Before assigning IT duties or granting privileged access to IT resources, do screening procedures include steps to ensure that candidates have the expertise to implement IT security controls appropriate to the position for which they are being considered? Do supervisors and hiring agents understand how to screen the expertise of candidates for IT Worker positions? Is some criteria such as education, experience or certification used to assess candidate expertise? Is some method used to verify candidates skills? Is some method used to ensure that candidates understand their responsibility to protect IT resources belonging to the institution? Are IT staff duties documented and available to users? Is IT Worker contact information made available to users they support? Do IT staff update their contact information when they are reassigned or leave the institution? As soon as possible after hire, before the probationary period ends, and preferably before privileged access is granted to manage IT resources, do supervisors ensure that IT staff receive IT orientation training? Is this documented in new employee procedures for IT staff?
9	**Subject: Screening Programmers** Target audience: Management and IT staff Vulnerability: Software is written for use with confidential data by programmers who lack appropriate expertise. Controls: Before duties are assign to program software used with confidential data, do screening procedures include steps to ensure that candidates have the expertise to protect the data? Is some method used to verify candidates skills? Do supervisors and hiring agents understand how to screen candidates for programming expertise? Is some criteria such as education, experience or certification used to assess candidate expertise? Is some method used to verify candidates skills? Is some method used to ensure that candidates understand their responsibility to protect confidential data? As soon as possible after hire, before the probationary period ends, and preferably before privileged access is granted to manage IT resources, do supervisors ensure that programmers receive IT orientation training? Is this documented in new employee procedures?
10	**Subject: Screening Users** Target audience: Management and IT staff Vulnerability: Individuals and groups who lack expertise access confidential data. Controls: Before hiring staff, assigning duties or granting access to confidential data, do screening procedures include steps to assess candidates expertise to protect the data? Is some criteria such as education, experience or certification used to evaluate their expertise? Is some method used to verify their skills? Before given access, are new employees instructed about the acceptable use, confidential data protection and sanctions for non-compliance? Do employees sign an agreement to comply? Are the agreements kept on file and periodically audited? Before given access, do Deans, Directors, Department Chairs or their designees ensure that all new employees receive formal training regarding their responsibility to protect confidential data? Does training new employees who access confidential data include the following topics? - Authorization requirements - Authentication requirements - Strong passwords and secure password management - Legal use of software - Recognizing and reporting violations - Mobile device and removable media restrictions - Screen inactivity lock requirements - Secure use of the web - Secure use of email - Secure use of instant messaging - Encryption requirements - File permissions restrictions - Document labeling requirements

	- Malware prevention - Social engineering - Phishing scams - Disposal requirements - Physical location restrictions - Physical access procedures - Secure use of software used to store and transmit confidential information - Sanctions for violating these requirements Is IT security training material readily available to its intended audience? Is some method, such as a quiz, used to assure that employees understand the training and their responsibility to comply? Is employee training periodically reinforced? Are employee training procedures documented? Is compliance with training procedures periodically verified?
11	**Subject: Screening Business Associates** Target audience: Management and IT staff Vulnerability: Business Associates with access to confidential data belonging to the institution are not adequately screened and authorized. Controls: Do purchasing and contracting procedures include steps to ensure that partners, third-party collaborators, vendors, consultants and other Business Associates that will access the institution's confidential data have the expertise to protect the data? Is some method used to verify the expertise of Business Associates? Are Business Associates with access to the institution's confidential data documented? Are the records periodically audited? Are the institution's IT security policies and procedures made available to Business Associates? Is some method used to ensure the Business Associates comply with the institution's IT security policies? Is IT security training provided by Business Associates as needed? Are procedures documented to ensure that Business Associates copies of the institution's data are not the official copies or the only copies? Are incident response procedures communicated to Business Associates? Is some method used to verify that Business Associates understand their responsibility to report to the institution any exposure of the institution's confidential data exposure? Is some method used to periodically verify that Business Associates comply with relevant the institution's policies and procedures?
12	**Subject: Authorization of IT staff to manage software, systems or networks used with confidential data** Target audience: Management and IT staff Vulnerability: IT staff manage IT resources used with confidential data without authorization. Controls: Do Deans, Directors, Department Chairs or their designees authorize individuals and groups permitted to manage IT resources used with confidential data? Are rules for granting, modifying and revoking IT Worker authorization documented? Do they include steps to minimize the number of IT staff that have privileged access to IT resources used with confidential data? Are authorized IT staff documented? Are authorization records periodically audited? Is some methods used to verify that IT staff understand their responsibility to protect confidential data? Is some method use to verify that they have the skills needed to implement data protection requirements?
13	**Subject: Authorization to reset passwords for other users** Target audience: Management and IT staff Vulnerability: Passwords are reset by individuals who are not authorized. Controls: Do Deans, Directors, Department Chairs or their designees authorize individuals and groups permitted to reset passwords for other users? Are rules documented for granting, modifying and revoking authorization to reset passwords for other users? Do they include steps to minimize the number of individuals allowed to reset passwords? Is some method used to verify individuals with password reset authorization understand password reset rules? Is some method used to verify that they understand their responsibility to protect passwords? Are individuals authorized to reset passwords documented? Are authorization records periodically audited?
14	**Subject: Authorization of Users to access confidential data** Target audience: Management and IT staff Vulnerability: Users access confidential data without authorization. Controls: Are policies documented that discourage users from storing confidential data on their workstations, computers not managed by skilled IT staff, portable devices and removable media? Instead, are users instructed to store confidential data only on secure servers belonging to the institution? Do Deans, Directors, Department Chairs or their designees authorize individuals and groups permitted to access confidential data? Are rules for granting, modifying and revoking authorization documented? Do they include steps to minimize the number of individuals

	authorized to access confidential data? Is some method used to verify that users understand data security requirements? Is some method used to verify that they understand their responsibility to protect confidential data? Are authorized users documented? Are authorization records periodically audited?
15	**Subject: Authorization and approval of software, systems and networks used with confidential data** Target audience: Management and IT staff Vulnerability: Confidential data is used on software, systems and networks that are not authorized or approved. Controls: Do Deans, Directors, Department Chairs or their designee authorize software, systems and networks that can be used with confidential data? Do Information Security Managers for each campus unit approve software, systems and networks than can be used with confidential data in their unit? Are rules documented for granting, modifying and revoking authorization of software, systems and networks that can be used with confidential data? Are security requirements documented for software, system and network approval? Are requirements cost-effective? Do requirements balance security with usability? Do Deans, Directors and Department Chairs provide adequate resources to implement workstation security requirements? Are authorized and approved software, systems, and networks documented? Is documentation available to users that need it? Are software, system and network authorization records periodically audited? Are audits periodically performed to ensure that confidential data is not used on software, systems and networks that are not authorized?
16	**Subject: Authorization and approval to store confidential data on workstations** Target audience: Management, IT staff and end-users Vulnerability: Confidential data is stored on workstations without authorization. Controls: Are employees discouraged from storing confidential data on their workstations? Instead, are the encouraged to store confidential data only on approved secure servers belonging to the institution? Do users avoid storing confidential data on their workstations? Where the need outweighs the risk, do Deans, Directors, Department Chairs and supervisors authorize individuals with special permission to store confidential on their workstation? Are rules for granting, modifying, and revoking authorization documented? Do Unit Information Security Managers approve workstations that can be used to store confidential data? Are security requirements documented for workstation approval? Are requirements cost-effective? Do requirements balance security with usability? Do Deans, Directors and Department Chairs provide adequate resources to implement workstation security requirements? Are security requirements available those that need them? Are security requirements periodically reviewed and updated? Are authorized and approved workstations documented? Is documentation available to users that need it? Are workstation authorization and approval records periodically audited? Are audits periodically performed to ensure that confidential data is not stored on workstations that are not authorized?
17	**Subject: Authorization and approval of portable devices and media to use with confidential data** Target audience: Management, IT staff and end-users Vulnerability: Confidential data is stored on portable devices and media without authorization or approval. Controls: Is storing confidential data on laptops, PDAs, smart phones and other portable devices discouraged? Is storing confidential data on CDs, DVDs, USB or thumb drives, and other removable media discouraged? When the need outweighs the risk, do Deans, Directors, Department Chairs or their designees grant individuals special permission to use confidential data on portable devices and removable media? Are rules documented for granting, modifying and revoking authorization? Are authorized users documented? Are authorization records periodically audited? Does the Unit Information Security Manager approve portable computers and removable media that can be used with confidential data? Are security requirements documented for portable devices and removable media? Are security requirements cost-effective? Do security requirements balance usability with security? Are security requirements available to users that need them? Do security requirements prohibit synchronization of portable devices with computers that are not trusted such as home computers and other computers that are not managed by skilled IT staff? Where the need outweighs the risk, Do Deans, Directors, Department Chairs or their designees authorize individuals with special permission to synchronize portable devices with computers that are not trusted? Are rules for granting, modifying, and revoking special permission documented? Are authorized users documented? Are authorization records periodically audited?

	Do security requirements document locations where the portable devices and removable media can be used with confidential data? Do users know that special permission is required to remove portable devices and removable media containing confidential data from secure locations belonging to the institution? Are procedures documented for protecting confidential data removed from secure locations belonging to the institution? Is some method used to verify that users understand procedures to protect confidential data removed from secure locations belonging to the institution? Do procedures include the following? - Encryption - Loss and theft protection - Labeling requirements - Incident response procedures Are authorized users trained about physical security requirements for portable devices and removable media used with confidential data? Is training periodically reinforced? Is some method used to verify that users understand the physical security requirements? Do Deans, Directors and Department Chairs provide resources to implement the physical security requirements for portable devices and removable media? Are security requirements periodically reviewed and updated? Is compliance with the security requirements periodically verified?
18	**Subject: Authorization and approval of computers that are not managed by skilled IT staff** Target audience: Management, IT staff and end-users Vulnerability: Computers used with confidential data are not managed by skilled IT staff. Controls: Are users discouraged from storing confidential data on computers that are not managed by skilled IT staff? Is authorization to store confidential on computers not managed by skilled IT staff rare? When the need outweighs the risk, do Deans, Directors, Department Chairs or their designees authorize individuals with special permission to store confidential data on computers that are not managed by skilled IT staff? Are rules documented for granting, modifying and revoking authorization to store confidential data that are not managed by skilled IT staff? Are authorized individuals documented? Are authorization records periodically audited? Does the Unit Information Security Manager approve computers to use with confidential data that are not managed by skilled IT staff? Are security requirements documented for computers used with confidential data that are not managed by skilled IT staff? Are security requirements cost-effective? Do security requirements balance usability with security? Do Deans, Directors and Department Chairs provide resources to implement the security requirements? Are security requirements available to users that need them? Are computer security requirements periodically reviewed and updated? Is compliance with computer security requirements periodically verified?
19	**Subject: Authorization to use confidential data on the web** Target audience: Management, IT staff and end-users Vulnerability: Confidential data is used on the web without authorization using systems that are not approved. Controls: Do Deans, Directors, Department Chairs or their designees authorize and document individuals and groups allowed to use confidential data on the web? Do they authorize and document individuals and groups authorized to manage confidential web content? Do they authorize and document IT staff to manage web servers? Are rules for granting, modifying and revoking user, content manager and IT Worker access documented? Are authorization records periodically audited? Do Deans, Directors, Department Chairs or their designees provide appropriate resources to protect confidential on the web?
20	**Subject: Authorization to use confidential in data in email** Target audience: Management, IT staff and end-users Vulnerability: Confidential data is used in email without authorization or approval. Controls: Are policies documented to discourage users from sending confidential data in email? When the need outweighs the risk, do Deans, Directors, Department Chairs and supervisors authorize individuals with permission to send confidential data in email? Is special permission required to send confidential data to email addresses that do not belong to the institution? Are rules for determining, modifying and terminating authorization documented? Are the authorization rules periodically reviewed and updated? Are authorized users documented? Are authorization records periodically audited? Do Deans, Directors, Department Chairs or their designees provide resources to implement email security requirements and restrictions?

21	**Subject: Authorization to use confidential data in instant messages** Target audience: Management, IT staff and end-users Vulnerability: Confidential data is sent in instant messages without authorization or approval. Controls: Are policies documented to discourage users from sending confidential data in instant messages? When the need outweighs the risk, do Deans, Directors, Department Chairs and supervisors authorize individuals with permission to send confidential data in instant messages? Is special permission required to send confidential data to addresses that do not belong to the institution? Are rules for determining, modifying and terminating authorization documented? Are the authorization rules periodically reviewed and updated? Are authorized users documented? Are authorization records periodically audited? Do Deans, Directors, Department Chairs or their designees provide resources to implement instant message security requirements and restrictions?
22	**Subject: Authorization to perform backups of confidential data** Target audience: Management, IT staff and end-users Vulnerability: Backups are performed of confidential data without authorization or approval. Controls: Do Deans, Directors, Department Chairs or their designees authorize individuals or groups permitted to perform backups of confidential data? Are rules documented for determining, modifying, and terminating backup authorization? Are those authorized to perform backups of confidential data documented? Are backup authorization records periodically audited? Do Deans, Directors, Department Chairs or their designees provide resources to implement security requirements for systems used to backup confidential data?
23	**Subject: Authorization of networks for transmission of confidential data** Target audience: Management, IT staff and end-users Vulnerability: Confidential data is transmitted over networks that are not trusted. Controls: Are policies documented to discourage transmission of confidential data to or from networks that are not trusted, such as networks that do not belong to the institution or wireless, even those belonging to the institution? Do Deans, Directors, Department Chairs or their designees authorize individuals with special permission to transmit confidential data over networks that are not trusted? Are rules for granting, modifying, and revoking authorization documented? Are authorized networks documented and made available to users? Are network authorization records periodically audited? Do Deans, Directors and Department Chairs provide resources to protect data transmitted over networks that are not trusted?
24	**Subject: Authorization of locations where confidential data can be used** Target audience: Management, IT staff and end-users Vulnerability: Locations where confidential data is used are not adequately protected from unauthorized access. Controls: Do Deans, Directors, Department Chairs and their designees authorize locations where confidential data can be used? Are rules documented for granting, modifying and revoking authorization of locations? Are authorized locations documented and is a list of authorized locations readily available to users? Are authorized locations periodically audited? Is access to authorized locations appropriately secured? Do Deans, Directors, Department Chairs and their designees authorize individuals and groups who are permitted access to locations where confidential data is used? Are rules documented for granting, modifying and revoking authorization of individuals and groups? Do rules include steps to minimize the number of authorized individuals and limit authorization to those who need access in order to perform their job duties? Are authorized individuals and groups documented? Are steps included in new employee procedures, employee exit procedures, and procedures for other staff status changes to update physical access authorization records? Are authorization records periodically audited? Are users discouraged from removing media containing confidential from authorized secure locations belonging to the institution? Where the need outweighs the risk, do Deans, Directors, Department Chairs and their designees authorize individuals with special permission to remove confidential data from secure locations belonging to the institution? Are rules for granting, modifying and revoking special permission documented? Are individuals with special permission documented? Are records periodically audited? Are appropriate loss and theft protections employed for media containing confidential data that are removed from authorized secure locations belonging to the institution? Is media labeled with contact information? Are media labels periodically audited? Is compliance with location restrictions, loss and theft protection, and labeling requirements periodically verified? Do Deans, Directors and Department Chairs provide resources to protect locations where confidential data is used?
25	**Subject: IT Worker expertise to control access to software, systems and networks**

	Target audience: IT staff Vulnerability: IT staff lack expertise to adequately control access to confidential data. Controls: Do IT staff provide facilities to identify and authenticate users that access software, systems and networks used with confidential data? Is unique account identification assigned to each user who accesses confidential data? Where possible, does authentication use official institution systems? Do access controls enforce strong passwords? Where appropriate and possible, is multi-factor authentication implemented to access confidential data? Do IT staff implement software, systems, and network controls to ensure that confidential data is available only to those users who are authorized? Do controls limit user access to the minimum amount of data they need to perform their job duties? Are access procedures documented, readily available and communicated to users? Are failed access attempts logged and tracked. Are access records periodically audited for anomalies? Are accounts expired promptly when the corresponding user terminates their relationship with the university or the account is no longer needed? Are accounts expired immediately when their passwords are discovered to be compromised? Are default accounts and passwords changed or deleted? Is some method used to verify that IT staff have appropriate skills to implement access controls? Is some method used to ensure the authentication is securely implemented? Are access controls monitored to ensure proper function? Is compliance with access requirements periodically verified?
26	**Subject: User understanding of authentication** Target audience: Management, IT staff and end-users Vulnerability: Users lack understanding of access procedures. Controls: Are software, system, network and physical access procedures documented, available and communicated to users who need it? Are access restrictions and requirements documented, available and communicated to users who need it? Is some method used to ensure that all employees understand access procedures? Do users know who to contact for IT support with access procedures? Do users understand that their activity might be monitored? Do users understand that they are responsible for all activity that originates from their account? Do they understand that their access could be disrupted if a security-related event is detected from their account? Is compliance with access procedures periodically verified?
27	**Subject: Guest access** Target audience: IT staff Vulnerability: Software, systems, networks and locations are not adequately protected against access to confidential data from guests and other unauthorized users. Controls: Do IT staff implement software, system, network and physical security controls to restrict guest and other unauthorized access? Are guest access privileges the minimum necessary to preserve the purpose of granting them access? Are controls implemented to prevent guest access to confidential data? Before given access, are guests instructed about the limitations and responsible use of guest accounts? Is some method used to determine if guests understand their access restrictions? Are guest access privileges documented and verified?
28	**Subject: Passwords strength** Target audience: Management, IT staff and end-users Vulnerability: Weak passwords are used to protect accounts that access confidential data. Controls: Are strong passwords required to access confidential data? Are password rules documented and available to users? Do users know who to contact for help creating strong passwords?

	Before given access, is some method used to ensure that all employees understand how to create strong passwords, not to share passwords and to protect their passwords from exposure? Do passwords require some secure combination of the following? - Minimum password length, preferably eight characters - Maximum password age, preferably 180 days or less - Adequate complexity requirements, such as lower and upper case, special characters and numbers - Failed password lockout duration, preferable at least 30 minutes - A small number of failed attempts when it is not possible to require long or complex passwords, preferably three
29	**Subject: Passwords controls** Target audience: IT staff Vulnerability: Password controls are not adequate to secure confidential data. Controls: Are password expiration cycles appropriate to the function and security access level of the accounts they protect? Are users warned in advance when their passwords are about to expire, preferably two weeks? Before resetting their password, do users agree to comply with the institution's acceptable use policy? Are accounts locked after several failed attempts to enter a correct password? Are password reset procedures documented, readily available and communicated to users? Is some method used to verify the identity of users before their password is reset? Is information used to verify user identity something that only they would know, i.e. information that is not readily available to others? To prevent password cycling, must passwords be at least one day old before they can be reset by the user? Are previously used passwords archived for each account so that they cant be reused? Is the number of previous passwords archived larger than the number of times that a user would reasonably reset their password to restore an old one, preferably greater than 10? Are password requirements documented and communicated to the users? Do users know who to contact for IT support with password controls? Are password requirements periodically reviewed and updated? Is some method used to verify compliance with password controls?
30	**Subject: Authentication records** Target audience: IT staff Vulnerability: Access to software, systems and networks is not adequately logged. Controls: Is access to software, systems and networks used with confidential data logged? Do logs include user identification, source address, connection time and disconnection time? Are timestamps accurate? Are logs retained for a sufficient length of time to be available for investigation, usually six months? Are failed access attempts logged? Are access records periodically audited for anomalies? Is a process to audit for unauthorized access documented and implemented? Do Deans, Directors and Department Chairs periodically receive and act upon summarized access reports?
31	**Subject: Software session management** Target audience: IT staff Vulnerability: Software session management is not sufficiently rigorous to protect confidential data. Controls: Is software session management sufficiently rigorous and controlled to protect confidential data? Are IP addresses, cookies, URL encoding and/or hidden HTML form fields used to track client sessions? Is maintaining session state on the server preferred over maintaining session state on the client? Is the session timeout the minimum length of time needed and appropriate for the security level of the data used with software? To prevent session hijacking, are session keys and shared secrets difficult to predict? Are measures taken to prevent session spoofing?

	Are measures taken to prevent session replaying? Are users able to logout to terminate their session? Are session logs maintained for those sessions used to access confidential data and do they include user identification, IP address, accurate connection time and an accurate disconnection time? Are access logs periodically audited for anomalies? Are session management requirements documented? Are session management controls periodically tested to verify compliance?
32	**Subject: Encryption** Target audience: IT staff Vulnerability: Confidential data is stored and transmitted in plain text. Controls: Do IT staff provide facilities such as encryption to protect storage and transmission of confidential data, especially on systems and networks that are difficult to protect, easily lost or stolen, or not trusted? Is some method used to verify that IT staff have the expertise to provide facilities to protect storage and transmission of confidential data? Are procedures documented for facilities that protect storage and transmission of confidential data? Do encryption procedures balance security with usability? Do procedures address systems and networks that difficult to protect or are not trusted? Are procedures readily available and communicated to users? Where encryption is provided, are encryption keys securely managed and protected against loss? Does the Unit Information Security Manager approve procedures for protecting storage and transmission of confidential data? Are transmission procedures periodically reviewed and updated? Are facilities to protect storage and transmission of confidential data periodically tested to verify effective protection of confidential data? Is some method used to verify that storage and transmission methods are effective at protecting confidential data? Do Deans, Directors and Department Chairs provide resources to implement facilities such as encryption to protect storage and transmission of confidential data?
33	**Subject: User understanding of encryption** Target audience: Management, IT staff and end-users Vulnerability: Users lack understanding of encryption and other methods to protect storage and transmission of confidential data. Controls: Are procedures available to users describing methods such as encryption to securely store and transmit confidential data? Do procedures describe when encryption should be used, such as on systems and networks that are difficult to protect, easily lost or stolen, or not trusted Is some method used to verify that users understand when and how to use encryption or other approved methods to protect storage and transmission of confidential data? Do users know who to contact for help with encryption procedures? Is some method used to verify that users employ encryption or other approved methods to protect storage and transmission of confidential data?
34	**Subject: Software, system and network trust** Target audience: IT staff Vulnerability: Software, systems and networks used with confidential data share resources with software, systems, networks and users that are not trusted. Controls: Do software, systems and networks used with confidential data share resources with software, systems, networks and users that are not trusted? Are policies documented that restrict trust relationships beyond what is required for the proper function of the software, system or network? Where needed, are trust relationships based on secure cryptographic methods e.g., SSH public keys or SSL certificates, and not on IP numbers or domain names alone? Are trust relationships documented and is documentation appropriately secured? Is some method used to ensure that IT staff have the expertise to implement trust restrictions? Are trust relationships monitored and verified?

35	**Subject: Access controls of files containing confidential data** Target audience: IT staff Vulnerability: Files containing confidential data are not adequately protected from exposure to unauthorized or unintended audiences. Controls: Do access controls for software, files, media, systems and networks used with confidential data adhere to the principle of least privilege? Do IT staff understand the principle of least privilege? Do they understand how to implement access controls? Is some method used to verify access controls? Are rules documented for granting, modifying, and revoking individual and group ownership of files and directories containing confidential data? Do IT staff understand how to configure file and directory ownership? Is some method used to verify the file ownership is accurately configured? Are rules documented for configuring file and directory access permissions? Do IT staff understand how to implement file and directory access permissions? Is some method used to verify file and directory access permissions?
36	**Subject: User expertise to protect confidential data** Target audience: Management, IT staff and end-users Vulnerability: Users dont understand how to protect confidential data. Controls: Are users instructed to store the minimum amount of confidential data needed to accomplish the purpose of storing it? Is some method used to ensure that users understand to minimize the amount of confidential data they store? Are audits performed periodically to ensure that users minimize the amount of confidential data stored? Are users provided with methods to protect confidential data from exposure to unauthorized or unintended audiences? Is some method used to ensure that they understand methods to protect confidential data from exposure to unauthorized or unintended audiences? Are audits performed periodically to verify that confidential data is not exposed to unauthorized or unintended audiences? Do users know who to contact for IT support with protecting confidential data?
37	**Subject: Programmer expertise to write software used with confidential data** Target audience: Management and IT staff Vulnerability: Programmers lack the expertise to write software used with confidential data. Controls: Does software used with confidential data comply with the institution's policies and industry standards? Is a formal development methodology used to write software used with confidential data? Are software design and function documented and tested thoroughly at every stage of development? Is software code well documented? Is software code subjected to internal review by peers that did not contribute to the code, or is it subjected to a trusted third-party assessment? Are security requirements documented and made available to programmers? Is some method used to ensure the programmers understand software security requirements? Is compliance with programming security requirements periodically verified? Are programmers authorized to write software used with confidential data documented? Are authorized programmer records periodically audited?
38	**Subject: Software input sanitization** Target audience: IT staff Vulnerability: User input to software is not adequately sanitized. Controls: Does software code take reasonable measures to sanitize user input? Are procedures for sanitizing user input documented? Are the following precautions taken to sanitize user input? - Remove unexpected data from input before processing - Prevent users from specifying raw file paths as input instead provide path identifiers - Prevent user input to system commands - Prevent users from formulating cross-site scripting attacks - Prevent users from entering format strings - Prevent users from specifying extra information along with legitimate input - Validate input on the server, regardless of client validation

	- Prefer directory information from official institution systems rather than user input - Where appropriate, block HTML tags from input - Where appropriate, prefer POST over GET in HTML forms Do programmers have the expertise to sanitize user input? Is software tested to verify that it user input is sanitized?
39	**Subject: Secure software file handling** Target audience: IT staff Vulnerability: File handling, ownership and permissions do not adequately restrict access to confidential data. Controls: Does software handle files containing confidential data as securely as possible while maintaining usability of the software? Are file permissions the minimum necessary to perform the task intended for the file by the software? Is data used by software stored in a directory separate from the executable files? Are file permissions of software code the minimum necessary to support proper function of the software? In software code, are full paths used to specify the location of files? Are software temporary files used sparingly, protected from exposure, named so they that are difficult to guess, and deleted when they are no longer useful? Are tests used to ensure that temporary files are not writable by any account or process other than the software for which the temporary file is intended? Is software audited for proper file handling?
40	**Subject: Software memory handling** Target audience: IT staff Vulnerability: Memory handling of software is not secure. Controls: For open-source software and software written by the institution's programmers, are procedures documented to ensure that software handles memory securely? Are variables that index memory within bounds? Does software code check buffer sizes to prevent writing data that is larger than the allocated buffer size? Does software code free allocated memory when it is no longer needed? Is software code tested to verify that memory handling is secure?
41	**Subject: Software testing** Target audience: IT staff Vulnerability: Software is not adequately tested to protect confidential data, data integrity and data availability. Controls: Are procedures documented for testing software used with confidential data? Does testing include attempts to compromise data, compromise the server, impersonate users or servers, perform fraudulent transactions, input junk data, and disrupt service in any way? Is testing performed to ensure that software is robust against unauthorized use or attack? Is vulnerability and penetration testing of software performed?
42	**Subject: IT Worker web management expertise** Target audience: Management and IT staff Vulnerability: IT staff do not understand how to protect confidential data on the web. Controls: Do Unit Information Security Managers approve web servers and workstations that can be used with confidential data? Do they document security requirements for servers, workstations and web browsers? Do they document methods to secure storage and transmission of confidential data on the web? Are other methods to protect confidential data on the web documented? Are security requirements and data protection methods cost-effective? Do they balance security with usability? Do IT staff understand how to implement web server security requirements? Do they understand how to implement security requirements on workstations used to access confidential data on the web? Do they understand how to securely configure browsers used to access confidential data on the web?

	Do web server managers and web content managers avoid storing confidential data directly on web servers? Instead, do they try to store confidential data on back-end servers? Do IT staff minimize access from web servers to back-end databases? When the need to store confidential data directly on a web server outweighs the risk, is the data encrypted? Is the amount of confidential data stored directly on web servers limited to the minimum necessary for accomplishing the purpose of storing it there? Do IT staff understand how to provide facilities such as encryption to protect storage and transmission of confidential data on the web? Are storage and transmission procedures documented? Is some method used to verify that facilities to protect web storage and transmission are implemented? Is some method used to ensure that web storage and transmission procedures are followed? Are security requirements available and communicated to web content managers and users? Are security requirements periodically reviewed and updated? Is some method used to verify that web security requirements are implemented?
43	**Subject: User understanding of web security requirements** Target audience: Management, IT staff and end-users Vulnerability: Users do not understand how to protect confidential data on the web. Controls: Are procedures for securely using confidential data on the web documented and available to users? Do users understand how to protect confidential data on the web? Is some method used to verify user comply with web security procedures? Do security procedures address the following topics? - Using only authorized and approved workstations and web browsers to access confidential data. - Encouraging users to minimize the amount of confidential data used. - Encouraging users to delete confidential when its no longer needed. - How to use facilities such as encryption to protect confidential stored or transmitted on the web. - Discouraging users from cutting and pasting confidential data? - Discouraging users from taking advantage of features to auto-complete or remember their passwords. - Discouraging users from following follow web links in email or instant messages. Do users know who to contact for IT support with web security requirements?
44	**Subject: IT Worker email management expertise** Target audience: Management and IT staff Vulnerability: IT staff do not understand email security requirements. Controls: Do Unit Information Security Managers approve email servers, workstations and email clients that can be used with confidential data? Do they document requirements for approval? Do they document restrictions for using confidential data in email? Are requirements and restrictions periodically reviewed and updated? Are approved servers, workstations and email clients documented? Are approval records periodically audited? v Do email restrictions include the following? - Confining recipients of email containing confidential data to addresses that belong to the institution. - Verifying that recipients are individuals, not lists. - Discouraging use of auto-completion features in email recipient fields. - Minimizing the number of recipients to which confidential data is sent in email. - Minimizing the amount of confidential sent in email. - Identifying in the body of the email that it contains confidential data. - Providing handling instructions in the body of the message such as, Do not forward. Delete this email as soon as possible. - Encrypting confidential data sent in email. Do IT staff understand how to implement email server security requirements? Do they understand how to implement security requirements on workstations used to send confidential data in email? Do they understand how to securely configure email clients used to send confidential data? Is some method used to verify that email security requirements are implemented? Do IT staff understand how to provide facilities such as encryption to protect transmission of confidential data in email? Are transmission procedures documented? Is some method used to verify that facilities to protect email transmission are implemented? Is some method used to ensure that email transmission procedures are followed?
45	**Subject: User understanding email security requirements** Target audience: Management, IT staff and end-users Vulnerability: Users do not understand methods for securely sending confidential data in email. Controls: Do users understand that sending confidential data in email should be rare? Are security requirements and restrictions for sending

	confidential data in email documented and available to users? Do users receive training about security requirements and restrictions for sending confidential data in email? Is some method used to verify that users understand their responsibility to protect confidential data in email? Is compliance with email security requirements and restrictions periodically verified? Do email restrictions include the following? - Confining recipients of email containing confidential data to addresses that belong to the institution. - Verifying that recipients are individuals, not lists. - Discouraging use of auto-completion features in email recipient fields. - Minimizing the number of recipients to which confidential data is sent in email. - Minimizing the amount of confidential sent in email. - Identifying in the body of the email that it contains confidential data. - Providing handling instructions in the body of the message such as, Do not forward. Delete this email as soon as possible. - Encrypting confidential data sent in email. Do users know who to contact for IT support with email security requirements?
46	**Subject: IT staff instant messaging management expertise** Target audience: Management and IT staff Vulnerability: IT staff do not understand instant messaging security requirements. Controls: Do Unit Information Security Managers approve instant messaging servers, workstations and instant messaging clients that can be used with confidential data? Do they document requirements for approval? Do they document restrictions for using confidential data in instant messages? Are requirements and restrictions periodically reviewed and updated? Are approved instant messaging servers, workstations and instant messaging clients documented and available to the users that need them? Are approval records periodically audited? Do instant message restrictions include the following? - Confining recipients of instant messages to addresses that belong to the institution. - Prohibiting transfer of confidential data using commercial instant messaging services such as AOL or MSN. - Verifying that recipients are individuals, not lists. - Discouraging use of auto-completion features in recipient fields. - Minimizing the number of recipients to which confidential data is sent. - Minimizing the amount of confidential sent in instant messages. - Identifying in the body of the message that it contains confidential data. - Providing handling instructions in the body of the message such as, Do not forward. Delete this message as soon as possible. - Encrypting confidential data sent in instant messages. - Prohibiting confidential data from being sent in files attached to instant messages. Do IT staff understand how to implement instant messaging server security requirements? Do they understand how to implement security requirements on workstations used to send confidential data in instant messages? Do they understand how to securely configure instant messaging clients used to send confidential data? Is some method used to verify that instant messaging security requirements are implemented? Do IT staff understand how to provide facilities such as encryption to protect transmission of confidential data in instant messages? Are transmission procedures documented? Is some method used to verify that facilities to protect instant message transmission are implemented? Is some method used to ensure that email transmission procedures are followed?
47	**Subject: User understanding of instant messaging security requirements** Target audience: Management, IT staff and end-users Vulnerability: Users do not understand methods for securely sending confidential data in instant messages. Controls: Do users understand that sending confidential data in instant messages should be rare? Are security requirements and restrictions for sending confidential data in instant messages documented and available to users? Do users receive training about security requirements and restrictions for sending confidential data in instant messages? Is some method used to verify that users understand their responsibility to protect confidential data in instant messages? Is compliance with instant messaging security requirements and restrictions periodically verified? Do instant messaging restrictions include the following? - Confining recipients of instant messages to addresses that belong to the institution. - Verifying that recipients are individuals, not lists. - Discouraging use of auto-completion features in recipient fields. - Minimizing the number of recipients to which confidential data is sent. - Minimizing the amount of confidential sent. - Identifying in the body of the message that it contains confidential data. - Providing handling instructions in the body of the message such as, Do not forward. Delete this message as soon as possible. - Encrypting confidential data sent in instant messages.

	Do users know who to contact for IT support instant messaging security requirements?
48	**Subject: Security requirements for backups of confidential data** Target audience: Management and IT staff Vulnerability: Security requirements for backups of confidential data are not documented. Control: Do Unit Information Security Managers approve systems used to backup confidential data? Are security requirements of backup systems documented? Are requirements periodically reviewed and updated? Are approved backup systems documented? Are backup system approval records periodically audited? Do backup system security requirements include the following? - Retention rules that limit the length of time that backups are retained within the requirements of Florida records retention rules. - Storing backups in physically secure locations. - Encryption of easily portable media. - Encryption of backups transmitted over networks that are not trusted. Is some method used to ensure that individuals that perform backups understand their responsibility to protect confidential data? Is compliance with backup security requirements periodically verified?
49	**Subject: System security requirements** Target audience: Management and IT staff Vulnerability: Computers systems are not adequately protected. Controls: Are servers, workstations, laptops and other computer systems managed by trusted and skilled IT staff? Are systems compliant with the institution's IT security policies? Are system security requirements documented, available and communicated to those that need them? Are system security requirements approved by the Unit Information Security Manager? Do system security requirements specify that system must: - Have a clearly defined institutional purpose and intended user base. - Have an individual or group designated as manager. - Be protected during the installation process. - Be on private IP, unless public IP is required. - Be synchronized with an accurate time server. - Have appropriate access restrictions, including but not limited to: . - Physical . - ACL . - Firewall . - Authentication . - Authorization restrictions . - Screen locks . - Inactivity timeouts - Be operated and secured appropriately for its specified network zone. - Run only the software and services necessary to support its function. - Run only software that complies with licensing agreements. - Comply with the institution's data security standards. Are system security requirements periodically reviewed and updated? Is compliance with server security requirements periodically verified?
50	**Subject: Restrictions for storing confidential data on workstations** Target audience: Management, IT staff and end-users Vulnerability: Confidential data stored on workstations is not adequately protected. Controls: Do users avoid storing confidential data on their workstations? Where the need outweighs the risk, do users understand that special permission is required? Do users understand that the workstation must be approved by the Unit Information Security Manager or their designee? Are security requirements documented, readily available and communicated to users with special permission to store confidential data on their workstation? Are the security requirements approved by the Unit Information Security Manager? Is training periodically reinforced? Do security requirements and methods include the following? - Is confidential data stored on workstations limited to the minimum amount necessary to accomplish the purpose storing it there? - Is confidential data promptly removed from workstations when it is no longer needed? - To minimize so-called shadow systems, is an official copy of confidential data stored on workstations maintained on a secure server belonging to the institution or another comparable system? - Are workstations used with confidential data labeled as such? Are reuse and disposal instructions included on the label?

	- Do employees storing private data on their workstations know to immediately report the exposure is when it is discovered? - Are displays of all computing devices used with confidential data positioned so that they are not viewable by unauthorized individuals? - Are inactivity timeouts to lock workstation displays set for an appropriate minimum time relative to the security level of the data that is used on the workstation? Does re-entry to a locked workstation require a strong password? - Are backups of workstations used to store confidential adequately secured? Is backup retention time minimized? Is backup media rendered unreadable before reuse or disposal? Do users know who to contact for IT support with workstation security requirements? Are security requirements for workstations used to store confidential data periodically reviewed and updated? Is some method used to verify that authorized users understand workstation requirements? Is compliance with workstation security requirements periodically verified?
51	**Subject: Restrictions for storing confidential data on portable devices and removable media** Target audience: Management, IT staff and end-users Vulnerability: Confidential data stored on portable devices and removable media is not adequately protected. Controls: Do users avoid storing confidential data on portable devices such as laptops, PDAs and smart phones, and removable media such as CDs, DVDs, and USB or thumb drives? Where the need outweighs the risk, do users understand that special permission is required? Do users understand the device and media must also be approved by the Unit Information Security Manager or their designee? Are security requirements documented, readily available and communicated to users with special permission to store confidential data on portable devices and removable media? Are the security requirements approved by the Unit Information Security Manager? Is training periodically reinforced? Do security requirements include the following? - Limit the amount of confidential data stored to the minimum necessary for accomplishing the purpose of storing it. - Encrypt the data - Delete confidential data promptly when it is no longer needed. - Prohibit transport outside of authorized secure institution locations without special permission - Prohibit synchronization of portable devices with computers that are not trusted. - Employ appropriate loss and theft protection - Ensure that the copy of the confidential data on the portable device or removable media is not the official copy and not the only copy. - Ensure that any backups are performed of the confidential data are protected from unauthorized access and retained for the least amount of time necessary. - Immediate report a confidential data exposure when it is discovered. Do users know who to contact for IT support with security requirements for portable devices and removable media? Are security requirements for portable devices and removable media periodically reviewed and updated? Is some method used to verify that authorized users understand the security requirements for portable devices and removable media? Is compliance with the security requirements for portable devices and removable media periodically verified?
52	**Subject: Restrictions for storing confidential data on computers that are not managed by trusted and skilled IT staff** Target audience: Management, IT staff and end-users Vulnerability: Confidential data is not adequately protected on computers that are not managed by trusted and skilled IT staff. Controls: Do users avoid storing confidential on computers that are not managed by trusted and skilled IT staff? When the need outweighs the risk, do users understand that special permission is required? Do users understand that the computer must be approved by Unit Information Security Manager or their designee? Are security requirements documented, readily available and communicated to users with special permission to store confidential data on computers that are not managed by trusted and skilled IT staff? Are the security requirements approved by the Unit Information Security Manager? Is training periodically reinforced? Do security requirements include the following? - Strong authentication - Current software updates - Current malware protection - Firewall - Intrusion detection - Encryption - Reuse and disposal - Limiting the amount of confidential data stored to the minimum necessary for accomplishing the purpose of storing it - Promptly removing confidential data when it is no longer needed - Ensuring that the copy stored on the computer that is not managed by IT staff is not the official copy and not the only copy

	- Ensuring that any backups are performed of the confidential data are protected from unauthorized access and retained for the least amount of time necessary - Immediately reporting a confidential data exposure when it is discovered Do users know who to contact in the event of a problem with a computer that is not managed by a trusted and skilled IT staff? Are security requirements periodically reviewed and updated? Is some method used to verify compliance with security requirements?
53	**Subject: Network segregation** Target audience: IT staff Vulnerability: Confidential data is transmitted over networks that are not trusted. Controls: Are similar IT resources logically aggregated to facilitate network zone management? Are network zones used to transmit confidential data segregated from zones that are not trusted? Are network zone restrictions appropriate for the security level of the resources they protect? Is exposure of trusted network zones minimized? Is some method used to verify that IT staff understand how to segregate trusted network traffic from traffic that is not trusted? Are network zone restrictions monitored and periodically verified? To minimize the potential for impact on trusted network zones, is outbound access restricted from network zones that are not trusted? Are outbound access restrictions documented and periodically verified? Is some method used to ensure that untrusted users and systems do not connect to trusted network zones? Is some method used to verify that users understand that they understand not to connect untrusted systems to trusted network zones? Are trusted network zones monitored to verify that all users and systems connected are trusted? Do IT staff have the skills verify that only trusted users and systems connect to trusted network zones?
54	**Subject: User understanding of network security** Target audience: Management, IT staff and end-users Vulnerability: Users lack understanding of trusted network zones. Controls: Do users know which networks are trusted? Is some method used to ensure that users understand that special permission is required to transmit confidential data to or from networks that are not trusted, including networks that do not belong to the institution and all wireless networks, even those that belong to the insitution? Is compliance with network zone restrictions periodically verified? Is some method used to verify that users understand methods to protect confidential data transmitted over networks that are not trusted? Do users know who to contact for IT support with network zones? Is compliance with confidential data transmission requirements periodically verified?
55	**Subject: Physical access restrictions** Target audience: Management, IT staff and end-users Vulnerability: Physical security does not adequately protect confidential data. Controls: Are procedures documented for the physical control of all hardware and media used with confidential data? Are hardware and media used with confidential data organized, labeled, protected from damage and protected from unauthorized access? Are IT resources used with confidential data geographically aggregated to facilitate implementation of access and environmental controls? Do physical access controls ensure that only authorized users are permitted access? Can any individual or group action be accounted for with respect to all physically controlled media? For example, are auditable locks used to protect confidential data locations? Are access controls and procedures documented, available and communicated to those with authorized access? Are access controls periodically verified? Are access records routinely audited for anomalies? Do Deans, Directors and Department Chairs periodically review and act upon reports summarizing physical access anomalies?
56	**Subject: Employee understanding of physical security requirements**

	Target audience: Management, IT staff and end-users Vulnerability: Employees do not understand physical access restrictions. Controls: Is a list available to employees of authorized locations where confidential data can be used? Do employees avoid removing confidential data from authorized secure locations belonging to the institution? Are employees informed about the authorized locations where the portable devices and removable media can be used with confidential data? Is some method used to verify that employees understand that special permission is needed to remove confidential data on any media from authorized secure locations belonging to the institution? Are procedures documented for protecting portable devices and removable media containing confidential data that are removed from secure locations belonging to the institution? Is some method used to verify that users understand the procedures? Is some method used to verify that security requirements are implemented? Do security requirements include the following? - Encryption - Loss and theft protection - Labeling requirements Is some method used to ensure that employees understand to immediately report the incident when they discover that confidential data is exposed to unauthorized or unintended audience? Are employees trained about physical security requirements? Is training periodically reinforced? Is some method used to verify that employees understand physical security requirements? Do employees know who to contact with questions about physical security?
57	**Subject: Physical access restrictions for guests** Target audience: Management, IT staff and end-users Vulnerability: Physical access restrictions for guests do not adequately protect confidential data. Controls: Are policies and procedures documented for managing visitors to locations where confidential data and systems are located? Do procedures include guest sign-in, escort, access log, and reception and hosting requirements? Are guest physical access restrictions communicated to all staff? Is compliance periodically verified?
58	**Subject: Disposal of media that contains confidential data** Target audience: Management, IT staff and end-users Vulnerability: Confidential data stored on media that will be reused for another purpose or disposed is not adequately rendered unreadable. Controls: Are procedures documented for reusing and disposing media that contains confidential data? Do reuse and disposal procedures include steps to render confidential data unreadable? Is media processed for reuse or disposal by trusted and skilled IT staff? Is some method used to ensure that IT staff understand their responsibility to render confidential data unreadable prior to reuse or disposal? Do reuse and disposal procedures include alternatives for certified disposal contractors? If media is stored or transported prior to disposal, is the media and contents inventoried? Is some method used to ensure that users understand media reuse and disposal procedures? Do users know who to contact for IT support with reuse and disposal procedures? Is compliance with reuse and disposal procedures periodically verified?
59	**Subject: Risk-based IT planning** Target audience: Management and IT staff Vulnerability: Security implications are not considered when planning, selecting and installing software, systems and networks. Controls: Are procedures documented for planning, selecting and installing software, systems and networks with consideration for cost and security risks? Is security balanced with usability? Do planning procedures include steps to coordinate the selection and installation of network infrastructure with central IT services? Do IT staff understand how to conduct risk-based planning of software, systems and networks? Prior to the installation, do IT staff plan and select software, systems and network equipment with consideration for the following? - Data protection - IT security incident history - Protections measures against compromise - Risk assessment results

	- Security strategies, policies and procedures Do Deans, Directors, Department Chairs and other positions with authority provide resources for risk-based IT planning.
60	**Subject: Screening for software, systems and networks weaknesses** Target audience: Management and IT staff Vulnerability: Software, systems and networks are not robust against attack. Controls: Are procedures documented to ensure that software, systems and networks are robust against attack? Do procedures document: - Methods to maintain awareness of vulnerabilities - Vulnerability assessment tools - IT resources that will be evaluated - Testing frequency - Secure documentation of vulnerabilities - Vulnerability mitigation procedures Do DNS names of systems that perform security scans clearly identify their purpose? Do Deans, Directors and Department Chairs routinely review and act upon vulnerability reports?
61	**Subject: Patches and security advisories** Target audience: Management and IT staff Vulnerability: Software, systems and networks are not robust against attack. Controls: Are all software, systems and networks up-to-date with respect to revisions, patches, and recommendations in security advisories? Is some method used to verify that IT staff understand patch management procedures? Is some method used to verify that patches are current? Is hardware sufficiently robust to maintain current revisions and patches? Are alternative security controls used to protect systems for which patches are not available or patches cannot be applied in a timely manner? Are equipment replacement schedules sufficient to prevent hardware malfunction and maintain security of aging systems? Are replacements planned with consideration for security risk? Are equipment replacement schedules cost-effective? Do they balance security with usability? Are equipment replacement procedures documented? Is some method used to verify that IT staff understand equipment replacement schedules? Do Deans, Directors and Department Chairs provide resources to adequately maintain current and secure software, systems and networks according to equipment replacement schedules?
62	**Subject: Malware protection** Target audience: Management and IT staff Vulnerability: Software, systems and networks are not adequately protected against malware. Controls: Are software, systems and networks adequately protected from malware including viruses, worms, trojans, bots, scams and others? Are products used to protect against malware updated automatically on a frequent schedule? Where applicable, are products used to protect against malware centrally-managed to ensure consistency? Are malware protection procedures documented? Is some method used to verify that IT staff and users understand malware protection procedures? Are malware protection methods periodically audited for proper function? Do Deans, Directors and Department Chair provide adequate resources for anti-malware protection?
63	**Subject: Change management procedures** Target audience: Management and IT staff Vulnerability: Change management procedures dont adequately consider security implications. Controls: Do change management procedures include the following steps? - Planning - Scheduling - Testing - Notification - Implementation

	Are security implications considered at every stage of change management to protect the confidentiality, integrity and availability of data, for example is confidential data excluded from notifications? Are change management procedures documented and followed? Is some method used to verify that IT staff understand change management procedures? Do Deans, Directors and Department Chairs provide adequate resources for secure change management?
64	**Subject: IT security incident monitoring, logging and alerting** Target audience: Management and IT staff Vulnerability: Software, systems and networks are not adequately monitored confidential data exposure and other security-related events. Controls: Are procedures documented for monitoring, logging and alerting of software, systems and networks for confidential data exposure and other security-related events? Are logs routinely audited for anomalies? Do monitoring procedures include steps to maintain detection of current threats? Is some method used to verify that IT staff understand systems that monitor software, systems and networks for confidential data exposure and other security related events? Are monitoring systems periodically evaluated for their effectiveness to detect events? Are they evaluate for cost-effectiveness? Do Deans, Directors and Department Chairs provide adequate resources to monitor for exposure of confidential data and other security-related events? Do Deans, Directors and Department Chairs periodically review and act upon reports summarizing security-related events?
65	**Subject: Incident notification** Target audience: Management and IT staff Vulnerability: Appropriate parties are not notified of IT security incidents. Controls: In the event of an IT security incident, can someone with responsibility for resolving the event be easily identified and notified? Are records of those with responsibility to resolve security-related events periodically audited and updated? Are procedures documented to ensure that a breach, theft or loss of software, systems, media, networks, or locations used with private data is immediately reported to the proper authorities? Are backups, inventories or other records of confidential data maintained for the purpose of investigation in case of media loss or theft? Are these records periodically audited? Do Deans, Directors and Department Chairs use some method to verify that all employees understand and follow incident notification procedures?
66	**Subject: Incident containment** Target audience: Management and IT staff Vulnerability: IT security incidents are not adequately and timely contained. Controls: Are procedures documented to ensure that all IT security incidents are contained as soon as possible, but no later than the same day in which detection occurs or notification is received? Can network connections be easily terminated to contain IT security incidents? Are the appropriate authorities notified when incidents are contained? If the incident has the potential to involve legal issues, is an first responder or forensic investigator contacted to ensure that containing the incident does not disturb evidence? Do Deans, Directors and Department Chairs use some method to verify that incident containment procedures are understood and followed?
67	**Subject: Incident investigation and forensics** Target audience: Management and IT staff Vulnerability: Evidence from IT security incidents involving confidential data or other legal issues is not adequately preserved. Controls: Do IT security incident response procedures document which incidents require evidence preservation and how evidence must be preserved? Is a forensics investigator contacted to investigate incidents involving exposure of confidential data or legal issues? Is some method used to verify that forensic investigators understand how to preserve evidence?

	Is compliance with evidence preservation procedures periodically verified?
68	**Subject: Incident resolution** Target audience: Management and IT staff Vulnerability: IT security incidents are not adequately resolved. Controls: In order to prevent similar incident recurrence, are risk assessment performed following significant IT security incidents? Do IT staff understand how to conduct a risk assessment following significant IT security incidents? Do Deans, Directors and Department Chairs provide resources for post-incident risk assessment?
69	**Subject: Incident tracking and reporting** Target audience: Management and IT staff Vulnerability: IT security incident records are not adequate. Controls: Do IT staff record and track IT security incidents? Do incident tracking systems record: - Incident type - Incident severity - Detection time - Containment time - Resolution time Are procedures for incident tracking documented? Are reports showing incident number and containment time periodically reviewed and acted upon by Deans, Directors and Department Chairs?
70	**Subject: Hazardous materials** Target audience: Management, IT staff and end-users Vulnerability: IT resources are not adequately protected against hazardous materials. Control: Are safeguards to protect IT resources against hazardous materials commensurate with the availability requirements of the resources? Are safeguards against hazardous materials documented? Is some method used to ensure that relevant staff understand how to protect IT resources from damage by hazardous materials? Where appropriate, is some method used to monitor safeguards against hazardous materials? Are safeguards against hazardous materials safeguards periodically verified?
71	**Subject: Flood protection** Target audience: Management, IT staff and end-users Vulnerability: IT resources are not adequately protected against flood. Control: Are safeguards to protect IT resources against flood commensurate with the availability requirements of the resources? Where appropriate, is some method used to monitor flood safeguards? Are flood safeguards documented? Are flood safeguards periodically verified? Is some method used to ensure that relevant staff understand their responsibilities for flood protection?
72	**Subject: Damaging winds** Target audience: Management, IT staff and end-users Vulnerability: IT resources are not adequately protected against damaging winds. Control: Are structures where IT resources are located adequately resilient against damaging winds? Are structural integrity specifications for wind protection documented? Is some method used to ensure that relevant staff understand their responsibility to ensure wind protection? Is structural integrity for wind protection periodically verified?

73	**Subject: Lightning** Target audience: Management, IT staff and end-users Vulnerability: IT resources are not adequately protected against lightning. Control: Are safeguards to protect IT resources against lightning commensurate with the availability needs of the resources? Are lightning safeguards documented? Is some method used to ensure that relevant staff understand their responsibility to ensure protection against lightning? Are lightning safeguards periodically verified?
74	**Subject: Earthquake** Target audience: Management, IT staff and end-users Vulnerability: IT resources are not adequately protected against earthquakes. Control: Are safeguards to protect IT resources against earthquakes commensurate with the availability needs of the resources? Are earthquake safeguards documented? Is some method used to ensure the relevant staff understand their responsibility to ensure protection against earthquakes? Are earthquake safeguards periodically verified?
75	**Subject: Electromagnetic pulses** Target audience: Management, IT staff and end-users Vulnerability: IT resources are not adequately protected against electro-magnetic pulses. Control: Are safeguards to protect IT resources against electro-magnetic pulses commensurate with the availability requirements of the resources? Are safeguards against electro-magnetic pulses documented? Is some method used to ensure that relevant staff understands how to protect IT resources against electromagnetic pulses? Where appropriate, is some method used to monitor safeguards against electromagnetic pulses? Are safeguards against electromagnetic pulses periodically verified?
76	**Subject: Power surges** Target audience: Management, IT staff and end-users Vulnerability: IT resources are not adequately protected against power surges. Control: Are safeguards to protect IT resources against power surges commensurate with the availability requirements of the resources? Are power surge safeguards documented? Is some method used to ensure that relevant staff understands how to protect IT resources from power surges? Is some method used to monitor power surge safeguards? Are power surge safeguards periodically verified?
77	**Subject: Staff availability** Target audience: Management and IT staff Vulnerability: The availability of essential staff is not adequately ensured. Control: Are safeguards to ensure availability of IT staff commensurate with the need of the IT resources they protect? Are safeguards to ensure availability of essential IT staff documented? Is some method used to ensure that essential IT staff understand the requirements for their availability? Are availability requirements periodically reviewed and updated?
78	**Subject: Integrity** Target audience: Management and IT staff Vulnerability: Data integrity is not adequate? Control: Are data integrity specifications commensurate with the requirements of the data?

	Are integrity requirements documented? Is some method used to ensure that relevant staff understands integrity requirements? Is data integrity monitored? Are methods used to ensure integrity periodically verified?