University Cyber-security Program
Critical Asset Mapping

Larry Wilson
Version 1.0
November, 2013

Part 3 - Cyber-Security Controls Mapping

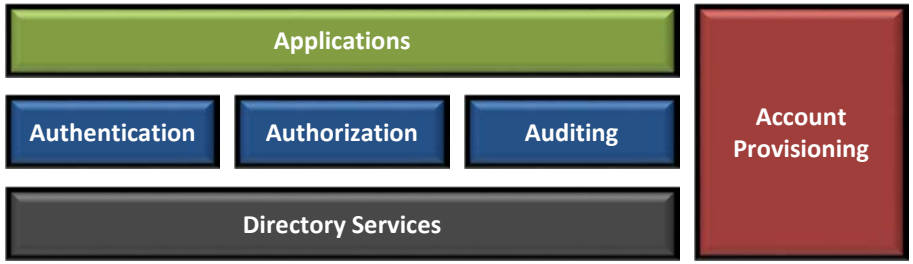
Cyber-security Controls mapped to Critical Asset Groups

CSC Control	Control Description	CAG-01	CAG-02	CAG-03	CAG-04	CAG-05	CAG-06	CAG-07
		People, Identities & Entitlements	Endpoint Devices	Business Applications	University Networks	Data Center Systems	Databases	University Data
CSC-01	Device Inventory		✓		✓	✓	✓	
CSC-02	Software Inventory		✓			✓	✓	
CSC-03	System Configuration (servers, endpoints)		✓			✓	✓	
CSC-04	Vulnerability Management		✓		✓	✓	✓	
CSC-05	Malware Defenses		✓			✓	✓	
CSC-06	Application Security			✓				
CSC-07	Wireless Devices				✓			
CSC-08	Data Backup & Recovery		✓		✓	✓	✓	✓
CSC-09	Skills Assessment	✓		✓				
CSC-10	Network Configuration				✓			
CSC-11	Control of Ports, Protocols, Services					✓	✓	
CSC-12	Administrative Privileges	✓	✓	✓	✓	✓	✓	✓
CSC-13	Boundary Defense			✓	✓			
CSC-14	Audit Logs	✓	✓	✓	✓	✓	✓	✓
CSC-15	Controlled Access based on Need to Know	✓		✓				✓
CSC-16	User & Service Account Monitoring	✓	✓	✓				✓
CSC-17	Data Loss Prevention		✓	✓				✓
CSC-18	Incident Response	✓						✓
CSC-19	Secure Network Engineering				✓			
CSC-20	Penetration Testing & Red Team Exercises	✓		✓	✓			

CAG-01: People, Identities, Entitlements

Best Practices for securing People, Identities, Entitlements

Framework for Security Administration



Security Administration Architecture

Account Provisioning

The process of creating, managing and deleting a digital identity :

- Account provisioning (on-boarding) – the creation of electronic identity and access rights; creating accounts, setting access privileges and controlling policy across a diverse collection of systems
- Account management (recertification) – tracks changes in user status and modifying entitlements including password management
- Account deletion (off-boarding) – removal of the electronic identity, generally when the employee has left the organization

Access Management [Authentication, Authorization, Auditing]

Includes verifying users are who they claim to be (Authentication), granting user access to resources based on role (Authorization), and recording who did what and when (Auditing).

- Authentication (AuthN) - Act of proving a digital identity of a user or object to a network, application, or resource
- Authorization (AuthZ) - Uses attributes associated with the digital identity to derive entitlements. Includes defining which resources the digital identity can access and which actions the digital identity can perform.
- Auditing – logging of identities as they are used within University applications and IT systems.

Directory Services

- Strategically important source of digital identity.

CAG-01 Security Controls

CSC-09 Skills Assessment Control Requirements: *Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.*

CSC-12 Administrative Privileges Control Requirements: *Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.*

CSC-14 Audit Logs Control Requirements: *Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.*

CSC-15 Controlled Access Based on Need to Know Control Requirements: *Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.*

CSC-16 Account Monitoring Control Requirements: *Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees and contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.*

CSC-18 Incident Response Control Requirements: *Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of network and systems.*

CSC-20 Penetration Testing Control Requirements: *Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises – all-out attempts to gain access to critical data and systems to test existing defenses and response capabilities.*

CAG-02: Endpoint Devices

Best Practices for securing Endpoints

Framework for Endpoint Security

EVERY SOLUTION HAS AN AGENT	EVERY AGENT HAS A CONSOLE	EVERY CONSOLE REQUIRES A SERVER	EVERY SERVER REQUIRES AN OS/DB	EVERY OS/DB REQUIRES PEOPLE, MAINTENANCE, PATCHING	WHERE DOES IT END?

Endpoint Security Architecture

- Every solution has an agent (inventory, auditing, DLP, NAC, encryption, etc.)
- Every solution requires a console to manage that agent
- Every console ends up requires a server
- Every server connects to data storage an OS database
- Need people to patch and manage each server OS and database.
- Where does it end?

CAG-02 Security Controls

CSC-01 Device Inventory Control Requirements: *Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the organization network, including servers, workstations, laptops, and remote devices.*

CSC-02 Software Inventory Control Requirements: *Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.*

CSC-03 Secure Configuration of Endpoints Control Requirements: *Establish a secure configuration standard (based on industry best practices such as DISA STIGs, CIS Benchmarks, etc.) ensures the secure configurations are deployed on pre-configured hardened systems, the configurations are updated on a regular basis, and are tracked in a configuration management system*

CSC-04 Vulnerability Management Control Requirements: *Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities.*

CSC-05 Malware Defenses Control Requirements: *Use automated ant-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.*

CSC-08 Backup and Recovery Control Requirements: *Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often.*

CSC-12 Administrative Privileges Control Requirements: *Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine.*

CSC-14 Audit Logs Control Requirements: *Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.*

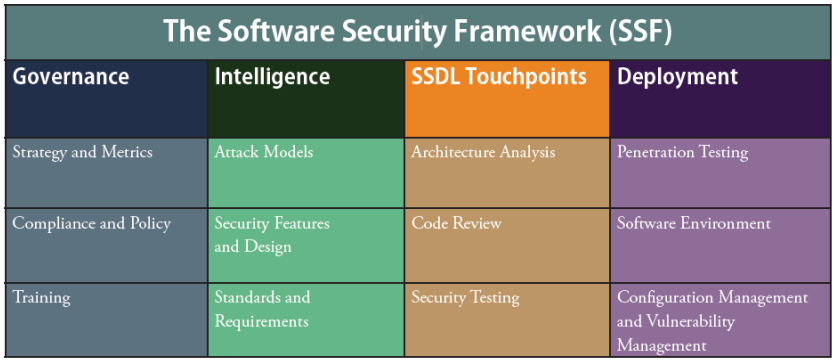
CSC-16 Account Monitoring Control Requirements: *Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees and contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards*

CSC-17 DLP Control Requirements: *Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.*

CAG-03: Business Applications

Best Practices for securing Business Applications

Building Security In Maturity Model - BSIMM-V (October, 2013)



Application (Software) Security Architecture
There are twelve *practices* organized into four *domains*.

The domains are:

1. **Governance**: Practices that help organize, manage, and measure a software security initiative. Staff development is also a central governance practice.

2. **Intelligence**: Practices that result in collections of corporate knowledge used in carrying out software security activities throughout the organization. Collections include both proactive security guidance and organizational threat modeling.

3. **SSDL Touchpoints**: Practices associated with analysis and assurance of particular software development artifacts and processes. All software security methodologies include these practices.

4. **Deployment**: Practices that interface with traditional network security and software maintenance organizations. Software configuration, maintenance, and other environment issues have direct impact on software security.

CAG-03 Security Controls

CSC-06 Control Requirements: *Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect traffic, and explicitly check for errors in all user input (including by size and data type).*

CSC-09 Skills Assessment Control Requirements: *Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.*

CSC-12 Administrative Privileges Control Requirements: *Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.*

CSC-13 Boundary Defenses Control Requirements: *Establish multi-layer boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks (extranets).*

CSC-14 Audit Logs Control Requirements: *Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.*

CSC-15 Controlled Access Based on Need to Know Control Requirements: *Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.*

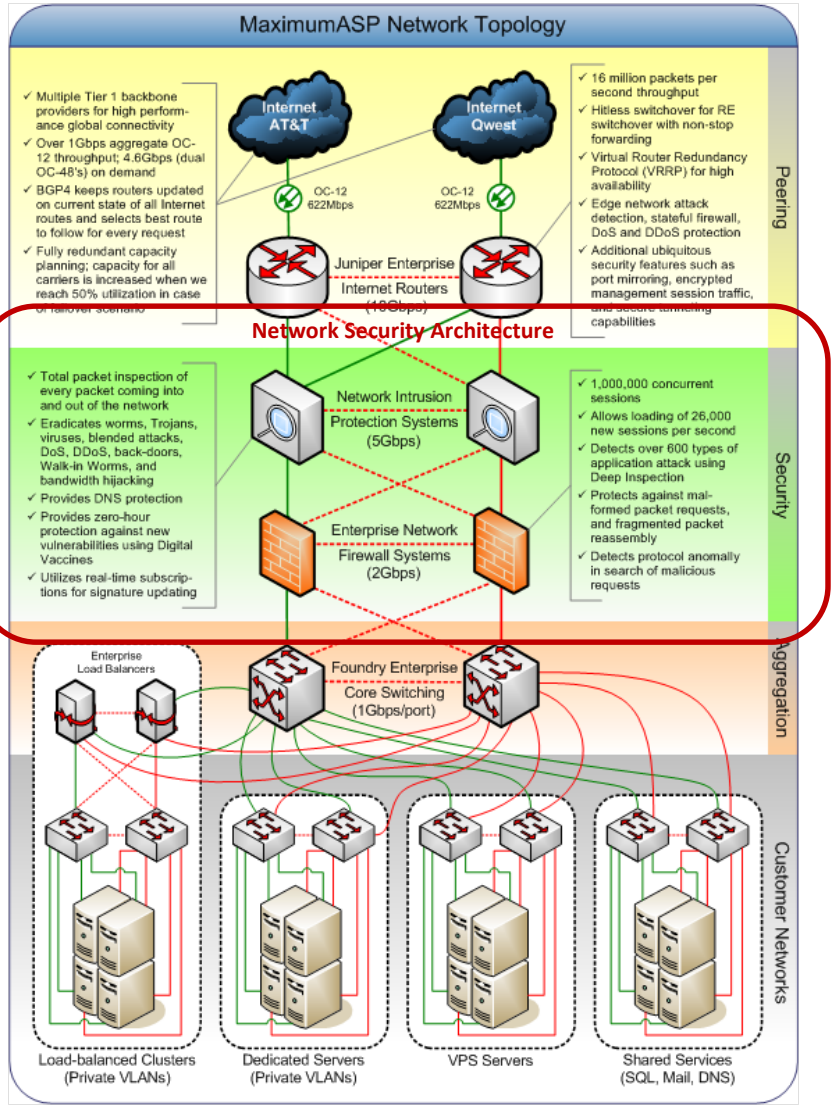
CSC-16 Account Monitoring Control Requirements: *Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees and contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.*

CSC-17 DLP Control Requirements: *Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.*

CSC-20 Penetration Testing Control Requirements: *Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises – all-out attempts to gain access to critical data and systems to test existing defenses and response capabilities.*

CAG-04: University Networks

Best Practices for securing University Networks



CAG-04 Security Controls

CSC-01 Device Inventory Control Requirements: *Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the organization network, including servers, workstations, laptops, and remote devices.*

CSC-04 Vulnerability Management Control Requirements: *Regularly run automated vulnerability scanning tools against all systems and remediate vulnerabilities, critical problems within 48 hours.*

CSC-07 Wireless Devices Control Requirements: *Allow wireless devices to connect to the network only if they match an authorized configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.*

CSC-08 Backup and Recovery Control Requirements: *Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test restoration process.*

CSC-10 Secure Network Configuration Control Requirements: *Compare firewall, router, switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates*

CSC-12 Administrative Privileges Control Requirements: *Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine.*

CSC-13 Boundary Defenses Control Requirements: *Establish multi-layer boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including business partner networks (extranets).*

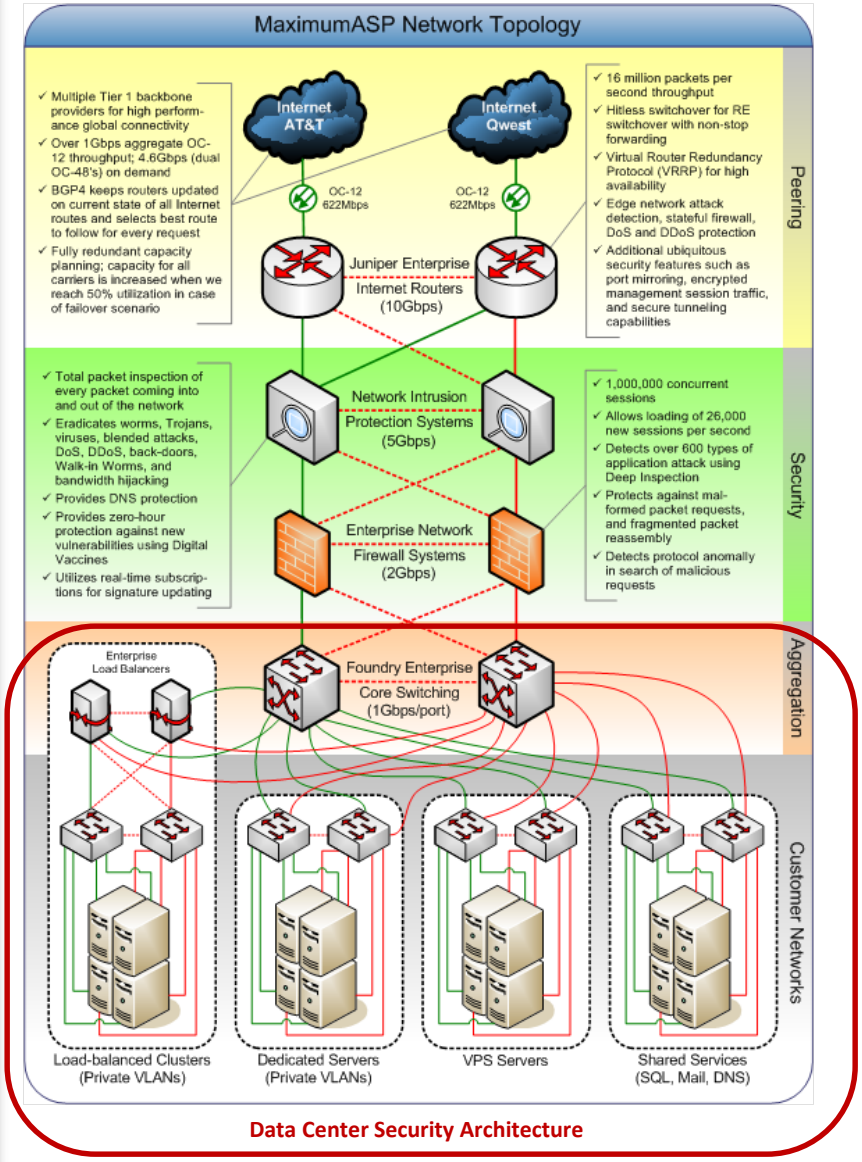
CSC-14 Audit Logs Control Requirements: *Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.*

CSC-19 Secure Network Control Requirements: *Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers; DMZ, middleware, private network. Allow rapid deployment of new access controls.*

CSC-20 Penetration Testing Control Requirements: *Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises –to test existing defenses and response capabilities.*

CAG-05: Data Center Systems

Best Practices for securing Data Center Systems



Data Center Security Architecture

CAG-05 Security Controls

CSC-01 Device Inventory Control Requirements: *Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the organization network, including servers, workstations, laptops, and remote devices.*

CSC-02 Software Inventory Control Requirements: *Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.*

CSC-03 Secure Configuration of Servers Control Requirements: *Establishing a secure configuration standard (based on industry best practices such as DISA STIGs, CIS Benchmarks, etc.) ensures secure configurations are deployed on pre-configured hardened systems, updated on a regular basis, and tracked in a configuration management system*

CSC-04 Vulnerability Management Control Requirements: *Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.*

CSC-05 Malware Defenses Control Requirements: *Use automated ant-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.*

CSC-08 Backups Control Requirements: *Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test restoration process.*

CSC-11 Ports, Protocols, Services Control Requirement: *Apply host-based firewalls and port-filtering and scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file servers, print servers and domain name servers (DNS) to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.*

CSC-12 Administrative Privileges Control Requirements: *Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.*

CSC-14 Audit Logs Control Requirements: *Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.*

CAG-06: Database Security

Best Practices for securing Databases

Defense-in-Depth for Maximum Security

PREVENTIVE	DETECTIVE	ADMINISTRATIVE
Encryption	Activity Monitoring	Privilege Analysis
Masking	Database Firewall	Sensitive Data Discovery
Privileged User Controls	Auditing and Reporting	Configuration Management

Preventive Controls

- **Advanced Security** - Encryption prevents database by-pass and provides the foundation on which to build security controls
- **Data Masking (for non-production) -** Replace sensitive application data stored in the Oracle database
- **Privileged User Controls** - Multi-factor authorization within database to enforce enterprise data governance and least privilege policies
- **Label Based Access Control -** Database enforced row level access control transparent to applications

Detective Controls

- **Activity Monitoring -** Monitor database traffic, detect and block unauthorized activity.
- **Audit Vault -** Consolidate diverse audit trails and logs into secure centralized repository.
- **Database Firewall -** Monitor database traffic, detect and block unauthorized activity
- **Auditing and Reporting** - Detect and alert on suspicious activities, including privileged users.

Administrative Controls

- **Asset Management -** Discover / classify databases into security & compliance policy groups
- **Sensitive Data Discovery -** Scan Oracle databases for sensitive data using built-in/custom definitions
- **Configuration Management -** Detect unauthorized database configuration changes, trouble ticket tracking

CAG-06 Security Controls

CSC-01 Device Inventory Control Requirements: *Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the organization network, including servers, workstations, laptops, and remote devices.*

CSC-02 Software Inventory Control Requirements: *Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.*

CSC-03 Secure Configuration of Servers Control Requirements: *Establishing a secure configuration standard (based on industry best practices such as DISA STIGs, CIS Benchmarks, etc.) ensures secure configurations are deployed on pre-configured hardened systems, updated on a regular basis, and tracked in a configuration management system*

CSC-04 Vulnerability Management Control Requirements: *Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.*

CSC-05 Malware Defenses Control Requirements: *Use automated ant-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.*

CSC-08 Backup and Recovery Control Requirements: *Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often.*

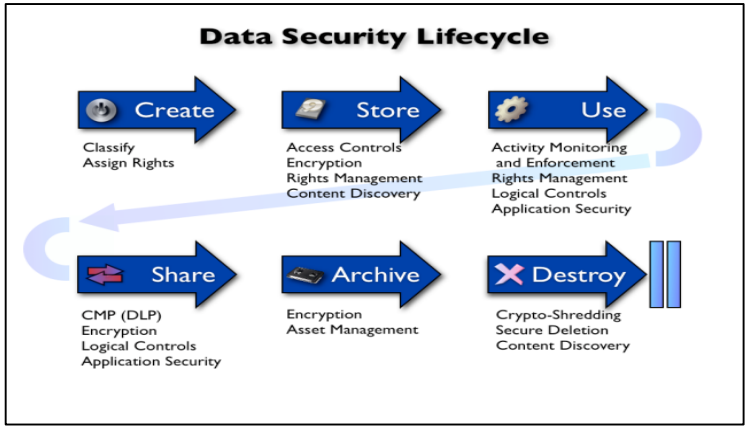
CSC-11 Ports, Protocols, Services Control Requirement: *Apply host-based firewalls and port-filtering and scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file servers, print servers and domain name servers (DNS) to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.*

CSC-12 Administrative Privileges Control Requirements: *Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.*

CSC-14 Audit Logs Control Requirements: *Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.*

CAG-07: University Data Security

Best Practices for securing University Data



Data Security Lifecycle

Create
- Content is classified as it's created based on labeling of data elements.
- Rights are assigned, based on central policies (mandatory and discretionary policies)

Store
- Access controls, encryption, and rights management to protect data in storage.
- Content Discovery helps find unprotected sensitive data that slipped through the gaps.

Use
- Monitor and protect information during use.
- Includes business applications and productivity applications.
- Heavy use of content-aware technologies.

Share
- Securely exchange information, inside and outside of the university
- A mixture of content-aware technologies and encryption for secure exchange.

Archive
- Protect information in archival storage.
- Encryption and asset management.

Destroy
- Ensure data is not recoverable at end of life
- Content discovery to ensure dangerous data isn't hiding where it shouldn't be.

CAG-07 Security Controls

CSC-08 Backup and Recovery Control Requirements: *Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.*

CSC-12 Administrative Privileges Control Requirements: *Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.*

CSC-14 Audit Logs Control Requirements: *Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.*

CSC-15 Controlled Access Based on Need to Know Control Requirements: *Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.*

CSC-16 Account Monitoring Control Requirements: *Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees and contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.*

CSC-17 DLP Control Requirements: *Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.*

CSC-18 Incident Response Control Requirements: *Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of network and systems.*