BITS 3523 COMPUTER AUDIT & RISK MANAGEMENT
LAB 4 (EXERCISE)

Common Security Control

Introduction:

Asset management is intended to first identify all hardware, software, systems, and data that support a facility's information systems. Once that baseline is completed, regular audits and assessments should be conducted periodically (e.g., on an annual or biannual basis). This is to ensure that the system is operating as designed and approved.

There are many ways to perform an asset inventory and tracking, such as using automated tools or manual inspections. Most facilities will benefit from a combination of these two approaches. Once a baseline inventory is completed, the effort required to maintain and update the asset inventory is greatly reduced.

Instructions:

1. You are provided with common security control inspection manual from Table 1 to Table 4. Fill up the empty place (rationale) why we need to do such security control for each attribute.
2. Submit the softcopy which may contain your answers via the ULearn portal.

Table 1: Access Control Security Control

Attribute	Activity/Security Control	Rationale
Access Control	Review all system accounts and disable any account that cannot be associated with a business process and owner.	To remove unwanted account from accessing system
	Ensure that all accounts have an expiration date associated with the account.	To remove traces of activities from being stolen
	Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.	To determine any misuse of access privileges or data policies from malicious intent
	Minimize the use of administrative privileges and only use privileged accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behaviour.	Administrative privilege poses a serious risk to security as compromised admin account can give access to malicious users
	Before granting users access to network resources, ensure that they are authenticated and authorized using their own individual (i.e., non-shared) credentials.	To lessen fraud from pretending to be someone else

Table 2: Baseline Configuration Security Control

Attribute	Activity/Security Control	Rationale
	Establish and ensure the use of standard secure configurations for operating systems. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system.	To lessen the area of vulnerability on systems
	Configure laptops, workstations, and servers so that they will not auto-run content from removable media, such as universal serial bus (USB) tokens (i.e., “thumb drives”), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares.	To avoid malware injection from removable media

Baseline Configuration	Implement automated patching tools and processes for both applications and for operating system software. When outdated systems can no longer be patched, update to the latest version of the application software.	To patch vulnerabilities on outdated softwares
	Employ anti-malware software that offers a remote, cloud-based centralized infrastructure that compiles information on file reputations. Alternatively, administrators can manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.	Prevents latest pervasive and dangerous attacks
	For all acquired application software, check that the version being used is still supported by the vendor. Update to the most current version and install all relevant patches and vendor security recommendations.	To stay up to date with latest security patches

Table 3: Communication Security Control

Attribute	Activity/Security Control	Rationale
Communication	Carry out all remote administration of servers, workstation, network devices, and similar equipment over secure channels.	To avoid from man-in-the-middle attacks or communication sniffer
	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	To allow only trusted services and ports to communicate
	Deny communications with (or limit data flow to) known malicious IP addresses (black lists) or limit access only to trusted sites (whitelists).	To avoid communication from untrustworthy ip addresses
	Configure operating systems so that passwords cannot be reused within a time, frame of six months.	Reduces the risk of password exposure
	Configure screen locks on systems to limit access to unattended workstations.	To reduce the risk of unauthorized use of workstation

Table 4: Cryptography Security Control

Attribute	Activity/Security Control	Rationale
Cryptography	Ensure all communication of sensitive information over less trusted networks are encrypted.	To prevent packet sniffers from getting sensitive data
	Use proven encryption techniques	To create strong encryption of data
	Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.	To protect from data theft
	Manage network devices using two-factor authentication and encrypted sessions.	Neutralize the risk when passwords were compromised
	Verify that cryptographic devices and software are configured to use publicly vetted algorithms.	To make sure that the encryption used are accepted as secured by many

-END-