# 3.6 ASSIGNMENT 3: GAP ANALYSIS AND CIS CONTROLS CASE STUDY

Joan V. Rodriguez Collazo
CYB469-O Section 01
Term C202306

## ASSIGNMENT

We will use a case study that will allow you to demonstrate what you have learned this week. Read the case study first and then see the assignment details and questions at the bottom of this assignment.

**Case Study:** https://online.fullsail.edu/class_sections/146149/modules/602745/activities/3503210

A Luigi's Inc. employee brought a personal laptop into the facility infected (albeit unknowingly) with PSL and connected it to the corporate network via a wireless access point (AP). The system obtained an IP Address using Dynamic Host Configuration Protocol (DHCP) addressing provided by the core corporate network services. Upon connection, the infected system is connected to the command-and-control server.

Once connected, the threat actor provided the command for the system to scan the local network for available services. While the user noticed the machine was running slowly, it was late on Friday before a three-day weekend. The user left the machine powered on with plans to look at it again on Tuesday. The scan identified an open File Transfer Protocol (FTP) service on the internal network that allowed anonymous access. Still using the compromised machine, the threat actor logged into the FTP server, compressed the contents, and then transferred the data to the control server (over the internet) using an encrypted outbound VPN connection.

Over the weekend, the Network Operations Center (NOC) tracked much data over an encrypted channel. While they could identify both the source and destination, without the encryption keys, they could not decrypt the traffic to identify the content. The destination was not on the current list of known malicious sites (the list was out of date by four months). The help desk technician opened a work ticket for the local desktop services to investigate.

The user noticed the machine still acting erratically early Tuesday morning, even after a reboot. The user then called the help desk to open a ticket. The help desk technician could tie the IP address of this machine to the traffic identified over the weekend. When the desktop technician arrived, it was determined that the machine was not corporate-issued and had no standard protection software. A quick scan using a boot time tool found the PSL signature. At this point, the technician confiscated the machine for forensic investigation and closed the ticket.

The forensics team determined that a known malware tool named PSL compromised the machine. They also found a temporary file left over by the scanning that included the directory listing of the FTP site. Many of the folders within the directory were named after previous high-value programs. These files included parts lists, price quotes, and even proprietary drawings. Included in the information were patents from the current Chief Executive Officer (Ms. J. Rabbit) and legal documents describing the purchasing and legal aspects of these programs.

**Assumptions:**

Luigi's falls somewhere between IG1 and IG2; hence, all the IG1 Safeguards apply, but so do some of the IG2 Safeguards. The facts of the case study should determine this.

**Instructions:**

Utilize the information from this week to determine which of the CIS Controls could have helped to prevent the attack detailed in the case study. Answer each question or section of a question separately.

## ISSUES AT LUIGIS

1. Clearly state all the issues that need to be addressed at Luigi's. (How did the attack occur?) (Please use bullets or numbers.)

   - **Lack of user awareness and education:**
     - The employee unknowingly brought an infected personal laptop to Luigi's and connected it to the corporate network. This highlights the need for user training on cybersecurity best practices to prevent the introduction of malware into the network.

     - The employee left the laptop powered on for three days. Leaving a computer powered on and unattended for three days can lead to an attack because it allows threat actors to exploit the device and gain unauthorized access to the corporate network. In this case, the employee's infected personal laptop connected to Luigi's corporate network, allowing the malware (PSL) to spread and communicate with a command-and-control server.
   - **Insufficient network access controls:**
     - The infected laptop could wirelessly connect to the corporate network without proper authentication or authorization. Implementing robust network access controls, such as strong authentication mechanisms and network segmentation, could have prevented unauthorized devices from connecting to the network.
   - **Inadequate malware defenses:**
     - The infected system made an internet connection to a command-and-control server, indicating a lack of effective malware detection and prevention mechanisms. Deploying and maintaining up-to-date anti-malware solutions across all endpoints could have helped identify and block the malware communication.
   - **Open FTP service with anonymous access:**
     - The scan identified an open File Transfer Protocol (FTP) service on the internal network that allowed anonymous access. This configuration allowed the threat actor to log into the FTP server and transfer sensitive data to the control server. Implementing access controls, such as requiring authentication and restricting anonymous access, would have mitigated this risk.
   - **Outdated list of known malicious sites:**
     - The destination server for the transferred data was not on the current list of known malicious sites. Maintaining an up-to-date list of known malicious sites is crucial for effective threat detection and prevention. Regularly updating the list would have increased the chances of detecting the communication to the control server.
   - **Lack of standard protection software:**
     - The compromised machine was not a corporate machine and did not have all the standard protection software. Implementing a standardized set of security software, including anti-malware, host-based firewalls, and intrusion detection/prevention systems, would have provided a baseline level of protection against common threats.
   - **Inadequate incident response procedures:**
     - It took several days before the user reported the machine's erratic behavior to the help desk, leading to delayed detection and response. Having well-defined incident response procedures, including clear escalation paths and response timelines, is crucial for the timely identification and containment of security incidents.
   - **Lack of forensics readiness:**
     - Although the compromised machine was confiscated for forensic investigation, it is unclear if the organization had well-established forensic readiness procedures and tools. Being prepared with forensic capabilities enables effective post-incident analysis and aids in identifying the extent of the compromise and potential data exfiltration.

## CIS CONTROLS V8

2. Which CIS Controls v8 could have helped prevent the attack detailed in the case study? (Please use bullets or numbers.) Why is each control important? 25-word min. Be thorough in your response.

   For this response, IG1/2 controls will be in blue, and those only related to IG2 are in green.

   - **CIS Control 01 - Inventory and Control of Enterprise Assets**: IG1/2
     - Luigi’s cannot defend hardware effectively if they do not know what is connected to their network. Maintaining an inventory of all devices connected to the corporate network would have allowed Luigi's to identify and control unauthorized devices like the infected personal laptop, preventing its connection and subsequent attack.
   - **CIS Control 02 - Inventory and Control of Software Assets:** IG1/2
     - An inventory of authorized software would have enabled Luigi's to identify any unauthorized or unpatched software on devices, ensuring that only approved and secure software is used, reducing the risk of malware infections. In this case, the PSL Malware could have been detected as soon as the connection was made.
   - **CIS Control 03 - Data Protection**: IG1/2
     - Implementing data protection measures would have safeguarded sensitive information stored on Luigi's systems, making it difficult for threat actors to access and steal data.
   - **CIS Control 04 - Secure Configuration of Enterprise Assets and Software:**
     - This control could have minimized vulnerabilities exploitable by the PSL Malware. This could have disabled anonymous FTP access, thereby reducing the attack surface.
   - **CIS Control 05 - Account Management:** IG1/2
     - Implementing solid passwords, MFA, and regular account reviews, would have prevented unauthorized access to the system and could prevent a threat actor from using compromised credentials to access unauthorized areas of the network.
   - **CIS Control 06 - Access Control Management:** IG1/2
     - Enforcing access controls based on the principle of least privilege would limit user access to other parts of the network, preventing the threat actor from freely moving within the network and accessing sensitive data and information.
   - **CIS Control 07 - Continuous Vulnerability Management:** IG1/2
     - Regularly scanning for weaknesses and promptly applying patches and updates would have closed security gaps, reducing the likelihood of the attack at Luigi’s from exploiting vulnerabilities like the ones PSL used to compromise the laptop and sensitive data.
   - **CIS Control 08 - Audit Log Management:** IG1/2
     - Implementing effective logging and monitoring mechanisms would have allowed Luigi's to detect and investigate suspicious activities, providing visibility into the network and helping identify the compromised laptop's activities during the attack.
   - **CIS Control 09 - Email and Web Browser Protections:** IG1/2
     - Implementing email and web browser protections, such as spam filters, web content filtering, and email attachment scanning, would have reduced the chances of employees unintentionally downloading malware or accessing malicious websites.
   - **CIS Control 10 - Malware Defenses:** IG1/2
     - Installing and regularly updating anti-malware software on devices would have detected and blocked the PSL malware, preventing the infected personal laptop from spreading it through the network.
   - **CIS Control 11 - Data Recovery:** IG1/2
     - Having proper data backup and recovery processes in place would have allowed Luigi's to restore systems and data to a known good state after an incident, minimizing the impact of the attack and reducing downtime.
   - **CIS Control 12 - Network Infrastructure Management:** IG1/2
     - Properly managing network infrastructure would ensure that access to the network is secure, preventing unauthorized devices and malicious traffic from entering the network.
   - **CIS Control 13 - Network Monitoring and Defense:** IG2
     - Implementing network monitoring tools and intrusion detection systems would have enabled Luigi's to detect and respond to suspicious network activities, allowing them to identify the malware infection and act sooner.

- **CIS Control 14 - Security Awareness and Skills Training:** IG1/2
  - Providing security awareness training to employees would have educated them about the risks, best practices, and potential signs of a cyberattack while empowering them to identify and report suspicious activities before it’s too late, which could have avoided the 3-day attack by the infected laptop.
- **CIS Control 15 - Service Provider Management:** IG1/2
  - Implementing proper vendor management processes and ensuring third-party service providers meet security requirements would have reduced the risk of an attack through compromised service providers or insecure connections.
- **CIS Control 16 - Application Software Security:** IG2
  - Implementing secure coding practices, regularly updating and patching applications, and conducting security testing would have reduced the likelihood of vulnerabilities in the software that attackers could exploit.
- **CIS Control 17 - Incident Response Management:** IG1/2
  - This control would have allowed Luigi's to respond promptly and effectively to the attack, minimizing the impact and helping the forensic team identify the source of the compromise.
- **CIS Control 18 - Penetration Testing:** IG2
  - Regularly conducting penetration testing would have identified vulnerabilities and weaknesses in Luigi's systems and network, allowing them to address the issues before attackers could exploit them.

## SAFEGUARDS

3. List the Safeguards for each Control in question 2 that should have been implemented to prevent the attack. Why are the Safeguards important? 25-word min. Be thorough in your response.

   IG1 safeguards listed in blue, and IG2 safeguards in green.  Everything is bulleted as follows:

- **Control (bold)**
  - *Safeguard (italicized)*
    - Why important (normal font)

- **CIS Control 01 - Inventory and Control of Enterprise Assets**
  - *Safeguard 01.1: Establish and Maintain Detailed Enterprise Asset Inventory*
    - There is a need for proper inventory management to identify unauthorized devices, such as the infected personal laptop connected to the corporate network.
  - *Safeguard 01.2: Address Unauthorized Assets*
    - A process to detect and handle unauthorized assets could have prevented the infected personal laptop from connecting to the corporate network without authorization.
  - *Safeguard 01.4: Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory*
    - Enabling DHCP logging would have allowed Luigis to track the assignment of IP addresses and identify the unauthorized laptop connected to the network.

- **CIS Control 02 - Inventory and Control of Software Assets:**
  - *Safeguard 02.1: Establish and Maintain a Software Inventory*
    - The absence of standard protection software on the compromised machine demonstrates the importance of keeping track of authorized software installations.
  - *Safeguard 02.2: Ensure Authorized Software is Currently Supported*
    - Designating unsupported software as unauthorized and documenting exceptions can help prevent vulnerabilities and ensure timely updates.
  - *Safeguard 02.3: Address Unauthorized Software*
    - Identifying and removing unauthorized software can help reduce the risk of malware infections and maintain a secure software environment.

- **CIS Control 03 - Data Protection:**
  - *Safeguard 03.1: Establish and Maintain a Data Management Process*
    - A well-defined data management process ensures the proper handling, retention, and disposal of sensitive data to prevent unauthorized access or loss of data.
  - *Safeguard 03.2: Establish and Maintain a Data Inventory*
    - Maintaining an inventory of sensitive data helps track its existence, location, and appropriate security controls, reducing the risk of unauthorized access or data breaches.
  - *Safeguard 03.3: Configure Data Access Control Lists*
    - Applying access controls to data prevents unauthorized access, such as the anonymous access to the FTP server that led to the exfiltration of sensitive information.
  - *Safeguard 03.4: Enforce Data Retention*
    - Proper data retention ensures compliance with legal requirements, preserves valuable information, and facilitates efficient data recovery and incident response.
  - *Safeguard 03.5: Securely Dispose of Data*
    - Secure data-disposal methods, such as secure erasure or destruction, help prevent unauthorized access to sensitive information when no longer needed.
  - *Safeguard 03.6: Encrypt Data on End-User Devices*
    - Encrypting data on devices adds an additional layer of protection, reducing the risk of unauthorized access in case of device loss or theft.
  - *Safeguard 03.10: Encrypt Sensitive Data in Transit*
    - Encrypting data transmitted over the network would have protected the content of the FTP server from being intercepted and accessed by the threat actor.
  - *Safeguard 03.13: Deploy a Data Loss Prevention Solution*
    - Implementing a data loss prevention solution would have detected the unauthorized transfer of sensitive data from the FTP server and prevented it from leaving the network.

- **CIS Control 04 - Secure Configuration of Enterprise Assets and Software:**
  - *Safeguard 04.1: Establish and Maintain a Secure Configuration Process*
    - Following secure configuration practices for end-user devices would have ensured that the personal laptop had the necessary security software and settings to detect and prevent PSL malware.
  - *Safeguard 04.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure*
    - Configuring network devices securely reduces the risk of unauthorized access and helps maintain the integrity and confidentiality of network communications.
  - *Safeguard 04.3: Configure Automatic Session Locking on Enterprise Assets*
    - Enabling automatic session locking enhances security by preventing unauthorized access when users are away from their devices. This could have helped prevent the three-day attack at Luigi Inc. when the employee left the computer running over the long weekend.
  - *Safeguard 04.4: Implement and Manage a Firewall on Servers*
    - A properly configured firewall could have prevented unauthorized access to the FTP service, reducing the risk of data exfiltration.
  - *Safeguard 04.5: Implement and Manage a Firewall on End-User Devices*
    - Using host-based firewalls or port-filtering tools helps control inbound and outbound network traffic, reducing the attack surface and preventing unauthorized access.
  - *Safeguard 04.6: Securely Manage Enterprise Assets and Software*
    - Implementing robust management processes for enterprise assets would have ensured that the personal laptop went through proper security checks and had the required protection software before connecting to the corporate network.
  - *Safeguard 04.7: Manage Default Accounts on Enterprise Assets and Software*
    - Disabling or making default accounts unusable helps prevent unauthorized access through commonly known account credentials or default configurations.
  - *Safeguard 04.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software*
    - Disabling unnecessary services on end-user devices, such as FTP, would have eliminated the potential vulnerability exploited by the threat actor.

- **CIS Control 05 - Account Management:**
  - *Safeguard 05.1: Establish and Maintain an Inventory of Accounts*
    - Maintaining an inventory of user accounts would have made it easier to identify and investigate the unauthorized account used by the threat actor to access the FTP server.
  - *Safeguard 05.2: Use Unique Passwords*
    - Enforcing unique passwords for each user account would have made it more difficult for the threat actor to gain unauthorized access to the FTP server.
  - *Safeguard 05.3: Disable Dormant Accounts*
    - Disabling or removing dormant accounts reduces the risk of unauthorized access through unused accounts, which may be targeted by threat actors or forgotten by users.
  - *Safeguard 05.4: Restrict Administrator Privileges to Dedicated Administrator Accounts*
    - Limiting admin privileges and separating general computing activities helps minimize the risk of unauthorized system changes or malware infections through user accounts.

- **CIS Control 06 - Access Control Management:**
  - *Safeguard 06.1: Establish an Access Granting Process*
    - Implementing a process for granting access to systems and resources would have ensured that only authorized individuals could access the FTP server.
  - *Safeguard 06.2: Establish an Access Revoking Process*
    - A process for revoking access ensures that terminated or role-changed individuals no longer have privileges to enterprise assets, reducing the risk of unauthorized access.
  - *Safeguard 06.3: Require MFA for Externally Exposed Applications*
    - Enforcing MFA for externally accessible applications adds an additional layer of security to protect against unauthorized access, such as in the case of remote network access.
  - *Safeguard 06.4: Require MFA for Remote Network Access*
    - *Requiring MFA for remote network access enhances authentication security, reducing the risk of unauthorized access to enterprise networks from external locations.*
  - *Safeguard 06.5: Require MFA for Administrative Access*
    - Requiring MFA for administrative access helps protect critical systems and accounts from unauthorized access, enhancing overall security posture.
  - *Safeguard 06.6: Establish/Maintain an Inventory of Authentication & Authorization Systems*
    - Maintaining an inventory of authentication and authorization systems would have helped identify any unauthorized systems the threat actor could exploit.

- **CIS Control 07 - Continuous Vulnerability Management:**
  - *Safeguard 07.1: Establish and Maintain a Vulnerability Management Process*
    - Implementing a vulnerability management process would have allowed Luigi's to identify and patch vulnerabilities in the FTP server, preventing unauthorized access.
  - *Safeguard 07.2: Establish and Maintain a Remediation Process*
    - A risk-based remediation strategy guides the prioritization and timely resolution of vulnerabilities, reducing the window of opportunity for potential attacks.
  - *Safeguard 07.3: Perform Automated Operating System Patch Management*
    - Regular OS updates through automated patch management help address known vulnerabilities, reducing the risk of exploitation by malware or attackers.
  - *Safeguard 07.4: Perform Automated Application Patch Management*
    - Applying timely updates to applications addresses vulnerabilities and ensures the use of the latest security patches, reducing the risk of unauthorized access or data breaches.

- **CIS Control 08 - Audit Log Management:**
  - *Safeguard 08.1: Establish and Maintain an Audit Log Management Process*
    - Implementing an audit log management process would have provided the necessary logs to trace the actions of the threat actor and identify the compromise of the FTP server.
  - *Safeguard 08.2: Collect Audit Logs*
    - Collecting audit logs and enabling logging on assets helps provide a record of events, facilitating the detection, investigation, and resolution of security incidents.
  - *Safeguard 08.3: Ensure Adequate Audit Log Storage*
    - Having sufficient storage for audit logs ensures the retention of logs for an appropriate period, allowing for analysis, incident response, and compliance purposes.

- **CIS Control 09 - Email and Web Browser Protections:**
  - *Safeguard 09.1: Ensure Use of Only Fully Supported Browsers and Email Clients*
    - Using supported and updated software reduces the risk of vulnerabilities and ensures the use of the latest security features in web browsers and email clients.
  - *Safeguard 09.2: Use DNS Filtering Services*
    - Employing DNS filtering services would have allowed Luigi's to block access to known malicious domains, preventing the threat actor's command-and-control server from communicating with the compromised laptop.

- **CIS Control 10 - Malware Defenses:**
  - *Safeguard 10.1: Deploy and Maintain Anti-Malware Software*
    - Installing anti-malware software on all end-user devices, including personal laptops, would have helped detect and prevent the PSL malware from infecting the unauthorized laptop.
  - *Safeguard 10.2: Enable Automatic Updates for Anti-Malware Software*
    - Enabling automatic updates for anti-malware software ensures that the software is up to date with the latest threat definitions and security patches, increasing its effectiveness against new malware variants.
  - *Safeguard 10.3: Disable Autorun and Autoplay for Removable Media*
    - Disabling autorun and autoplay functionality reduces the risk of automatic execution of malicious code from removable media, mitigating potential malware infections.

- **CIS Control 11 - Data Recovery:**
  - *Safeguard 11.1: Establish and Maintain Secure Configurations for Network Devices*
    - Following secure configuration practices for network devices, such as firewalls and routers, would have reduced the risk of unauthorized access to the network and mitigated the attack's potential impact.
  - *Safeguard 11.2: Perform Automated Backups*
    - Regular automated backups help protect against data loss and facilitate data recovery in the event of system failures or incidents, such as malware infections.
  - *Safeguard 11.3: Protect Recovery Data*
    - Applying appropriate security controls, such as encryption or data separation, to recovery data ensures its confidentiality and integrity, maintaining its value.
  - *Safeguard 11.4: Establish and Maintain an Isolated Instance of Recovery Data*
    - Isolating recovery data helps protect it from unauthorized access or tampering, ensuring its availability when needed for restoration or incident response purposes.
  - *Safeguard 11.5: Regularly Monitor and Analyze Network Traffic*
    - Implementing network traffic monitoring and analysis tools would have allowed Luigi's to identify suspicious activities and anomalous network behavior, enabling early detection and response to potential threats.

- **CIS Control 12 - Network Infrastructure Management:**
  - *Safeguard 12.1: Establish and Maintain Security Awareness and Training Program*
    - Providing regular security awareness and training sessions to employees would have educated them about the risks associated with unauthorized devices, suspicious emails, and safe internet practices, reducing the likelihood of successful attacks.

- **CIS Control 13 - Network Monitoring and Defense:**
  - *Safeguard 13.2: Implement Multi-Factor Authentication (MFA)*
    - Enforcing multi-factor authentication for accessing critical systems and resources, including the FTP server, would have added an extra layer of security, making it more difficult for the threat actor to gain unauthorized access.

- **CIS Control 14 - Security Awareness and Skills Training:**
  - *Safeguard 14.1: Conduct Regular Security Assessments*
    - Performing regular security assessments, including penetration testing and vulnerability assessments, would have identified weaknesses in Luigi's security posture, allowing them to address vulnerabilities before they could be exploited proactively

  - *Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks*
    - Educating employees about social engineering attacks, like phishing, helps prevent incidents where employees unknowingly compromise security, as in the case study.
  - *Safeguard 14.3: Train Workforce Members on Authentication Best Practices*
    - Educating employees on authentication best practices, such as using strong passwords and multi-factor authentication, helps protect against unauthorized access.
  - *Safeguard 14.4: Train Workforce on Data Handling Best Practices*
    - Training employees on how to handle, store, and dispose of data properly reduces the risk of data breaches and unauthorized access to sensitive information.
  - *Safeguard 14.5: Train Workforce Members on Causes of Unintentional Data Exposure*
    - Educating employees about potential risks and mistakes that can lead to unintentional data exposure helps mitigate the chances of data leaks or accidental data disclosures.
  - *Safeguard 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents*
    - Training employees to identify and report security incidents promptly helps facilitate a rapid response and minimize the impact of security breaches.
  - *Safeguard 14.7: Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates*
    - Encouraging employees to report software patching issues and tool failures helps ensure that vulnerabilities are addressed promptly and critical systems remain protected.
  - *Safeguard 14.8: Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks*
    - Educating employees on the dangers of insecure network connections helps them make informed decisions to secure their connections, both within and outside the organization.

- **CIS Control 15 - Service Provider Management:**
  - *Safeguard 15.1: Establish an Incident Response Plan*
    - Having a well-defined incident response plan in place would have enabled Luigi's to respond promptly and effectively to the security incident, minimizing the impact and facilitating a coordinated response to mitigate the breach.

- **CIS Control 16 - Application Software Security:**
  - *Safeguard 16.1: Regularly Back Up Data*
    - Implementing regular data backups, both locally and offsite, would have allowed Luigi's to restore the compromised data in case of a breach, reducing the potential impact on business operations.

- **CIS Control 17 - Incident Response Management:**
  - *Safeguard 17.1: Establish and Maintain Security Monitoring and Incident Detection Systems*
    - Deploying security monitoring and incident detection systems would have provided real-time visibility into suspicious activities, helping detect and mitigate incidents quickly.
  - *Safeguard 17.2: Establish and Maintain Contact Information for Reporting Security Incidents*
    - Having up-to-date contact information for relevant stakeholders helps streamline communication during security incidents, enabling a timely and coordinated response.
  - *Safeguard 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents*
    - Establishing a clear process for reporting security incidents encourages employees to promptly report any suspicious activities or potential security breaches they encounter.

- **CIS Control 18 - Penetration Testing:**
  - *Safeguard 18.1: Encrypt Sensitive Data*
    - Implementing data encryption for sensitive information at rest and in transit would have added an extra layer of protection. Encryption would make it significantly harder for unauthorized individuals to access and exploit the data even if they managed to gain unauthorized access.

## SOURCES

CIS. (n.d.). *CIS Critical Security Controls FAQ*. Retrieved from Center for Internet Security: https://www.cisecurity.org/controls/cis-controls-faq

CIS. (n.d.). *CIS Critical Security Controls Navigator* . Retrieved from CIS: https://www.cisecurity.org/controls/cis-controls-navigator

Controls-Assessment-Specification. (2022). *CIS Control 1: Inventory and Control of Enterprise Assets*ℑ . Retrieved from Controls-Assessment-Specification: https://controls-assessment-specification.readthedocs.io/en/stable/control-1/index.html#:~:text=Why%20is%20this%20CIS%20Control,%2C%20system%20backup%2C%20and%20recovery.

Landoll, D. (2016). *The Security Risk Assessment Handbook, 2nd Edition* . CRC Press.

Landoll, D. J. (2017). *Information Security Policies, Procedures, and Standards* . Auerbach Publications.

Tunggal, A. T. (2023, 04 20). *What are the CIS Controls for Effective Cyber Defense?* . Retrieved from UpGuard: https://www.upguard.com/blog/cis-controls#:~:text=agencies%20and%20defense.-,Why%20are%20the%20CIS%20Controls%20Important%3F,service%20and%20other%20cyber%20threats.