**Risk Management Plan for DHAEI: New Branch Office in Brampton**

By James Kuzhilaparambil

# TABLE OF CONTENTS

EXECUTIVE SUMMARY…………………………………………………………………………………...3

RISK ASSESSMENT AND RISK TREATMENT METHODOLOGY………………………………...…3

RISK ASSESSMENT…………………………………………………………………………….….3

RISK ASSESSMENT PROCESS……………………………………………………….….3

ASSETS, VULNERABILITIES, AND THREATS………………………………………....5

DETERMINING THE RISK OWNERS…………………………………………………..…7

IMPACT AND LIKELIHOOD…………………………………………………………….…11

RISK ACCEPTANCE CRITERIA……………………………………………………..…...14

RISK TREATMENT………………………………………………………………………….………14

REFERENCES……………………………………………………………………………………………….21

APPENDIX…………………………………………………………………………………………………….25

**EXECUTIVE SUMMARY**

The purpose of this document is to define the methodology for assessment and treatment of information risks in DHA Enterprise Incorporated’s (DHAEI) plan to open a new branch office in Brampton, and to define the acceptable level of risk according to the ISO/IEC 27001 standard.

Risk Assessment and Risk Treatment are applied to all assets used within the organization that are involved or will be involved in the creation of the Brampton branch office or which could have an impact on information security within the ISMS related to the branch creation.

Users of this document are all employees of DHAEI who take part in Risk Assessment and Risk Treatment.

**RISK ASSESSMENT AND RISK TREATMENT METHODOLOGY**

**RISK ASSESSMENT**

**RISK ASSESSMENT PROCESS**

We will divide the methodology in two: we first do **Risk Assessment**, then **Risk Treatment** or Management. This method is easy to frame mentally and logically.

A Cyber Security **Risk Assessment** identifies risks to an organization’s IT infrastructure, including information, systems, and networks. As a result of identifying these risks, the organization can take required action to mitigate or reduce these risks. Most importantly, a Risk Assessment helps an organization work on a plan to respond and recover from a cyber attack.

A Cyber Security Risk Assessment has three key phases: **Risk Identification**, **Risk Analysis**, and **Risk Evaluation**.

**Risk Identification**: This is the first stage of the risk assessment process; at this stage, we identify assets (people, process, and technology), threats, existing controls, and vulnerabilities.

**Risk Analysis**: In this stage, we assess impact and likelihood of risk and then calculate risk levels (based on impact and likelihood) by control.

**Risk Evaluation**: In the last and the final stage of Risk Assessment, we use the calculated risk levels to compare against risk evaluation criteria and risk acceptance criteria, and then draft recommendations to mitigate risks for those controls failing to meet acceptance criteria.

The case study says the creation of the Brampton branch office will include the following technical, security, and user requirements:

**Technical Requirements**

Ensure that all company-issued computers receive all updates that have been approved for release by the technology department.

Minimize Internet bandwidth by providing internal computers with Microsoft updates via internal servers.

Minimize traffic across the VPN for remote users.

Provide central monitoring of all servers.

Generate an email whenever a hardware event occurs on any of the servers in the company.

The support technicians located in the branch office must have the rights to perform all local maintenance on the branch office servers in their respective branches.

The installation of the new Read-Only Domain Controller in the Brampton office must minimize active directory replication across the WAN link between Columbus, and the main office storage space to store user data must be minimized.

All company-issued computers must be configured with Office 365.

**Security Requirements**

The branch office technicians should not have any rights to servers not located in their respective branch offices.

The installation of the new RODC in the Brampton office must not require any passwords or cached secrets to be stored outside of company servers.

Files stored on the company file servers must be protected in the event that a file server or the drives from any file server are stolen.

**User Requirements**

Users in the new branch office must access their data using mapped drives.

User drives should not need to be remapped when the data is moved from the main office file server to the branch office server.

In order to satisfy these three groups of requirements, we need to involve in the Risk Assessment and Risk Treatment phase executives, managers, and support staff who are or will be in the best position to list the risks, the threats and the controls that affect all information assets involved or will be involved in the creation of the Brampton branch office. We consider the following persons as needed for the analysis and review:

Amanda Wilson, CIO

Paul Alexander, CISO

William Freund, Manager, Systems

Scotty Doohan, Manager, Applications

Harold Fry, Security Technician

Jonathan Jasper, Senior Systems Administrator

Tina Mann, Senior Network Administrator

Vincent DiSalvo, Network Architect

Robert Briscoe, Manager, Corporate Security

Risk Assessment is implemented through the **Risk Assessment Table**. The Risk Assessment process is coordinated by Mr. Harold Fry, Security Technician, reporting to Mr. Paul Alexander, CISO. The identification of threats and vulnerabilities is performed by **asset owners**, and assessment of consequences and likelihood is performed by **risk owners**. There may be instances where the asset owner and the risk owner are the same person.

**ASSETS, VULNERABILITIES, AND THREATS**

We identify the following five (5) threats to DHAEI with respect to the new Brampton office.

**The Brampton File Server - Hardware Sabotage**

It is possible for the Brampton File Server to be physically attacked, damaged or some of its components stolen if the physical security at the branch is inadequate. Key cards may not be properly configured or installed, the sign-in/sign-out procedures are not strictly enforced, or the file server itself is situated in an area that isn’t properly secured.

**The Windows 10 personal computers - Bypass Windows Lock Screen**

CVE-2019-9510 (*NVD - CVE-2019-9510*, n.d.) details an interesting Windows 10 vulnerability wherein a user who initially connects remotely can gain access to user sessions without needing to interact with the Windows lock screen. Should a network anomaly trigger a temporary Remote Desktop Protocol (RDP) disconnect, if Automatic Reconnection of the RDP session is enabled (the default) the session will be restored to an unlocked state. By interrupting network connectivity of a system, an attacker with access to a system being used as a Windows RDP client can gain access to a connected remote system, regardless of whether or not the remote system was locked.

**The Read-Only Domain Controller - Stolen Credentials**

The Read-Only Domain Controller holds all Active Directory accounts of all objects needed by the Brampton branch to fully function as a satellite office of DHAEI. Among others, these include user accounts, service accounts, printers, computer objects, and shared folders. A Windows domain controller can be compromised via a Tactic called Defense Evasion (*Defense Evasion, Tactic TA0005 - Enterprise*, 2018), and a Technique called Modify Authentication Process (*Modify Authentication Process, Technique T1556 - Enterprise*, n.d.). Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts. Compromised credentials or access may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. The attacker, though, has to be able to gain entry into the network first to be able to modify the authentication process. Using simple-to-crack passwords makes the exploit possible and easier.

**The Brampton Office Routers - DDoS Attack**

The WAN link to the brampton office will be expected to carry many kinds of data. These include application software updates from the WSUS server, Active Directory updates (unidirectionally), file and data access from the (eventual) Brampton File Server by remote users, and branch office Internet access. The routers controlling network traffic for this site can be compromised by a Tactic called Resource Development (*Resource Development, Tactic TA0042 - Enterprise*, 2020) and a Technique called Acquire Infrastructure (*Acquire Infrastructure: Botnet, Sub-Technique T1583.005 - Enterprise*, 2020). With enough botnets, an attacker can start a Distributed Denial of Service (DDoS) attack on the routers, crippling response of the routers and utilizing all the bandwidth to stop all network traffic. MITRE acknowledges that this type of attack cannot be easily mitigated.

**The Brampton File Server - Impersonation**

The Brampton File Server needs to have the file sharing protocol SMB (Server Message Block) enabled so that the branch office users can define shares on their individual computers that point to the actual locations on the file server, without the need to refer to the actual locations. This introduces flexibility in accessing the files, especially since the data will initially reside not on the Brampton file server but on the main office file server (prior to being moved to the Brampton FS). SMB can be compromised via a Tactic called Lateral Movement (*Lateral Movement, Tactic TA0008 - Enterprise*, 2018) and a Technique called Remote Services (*Remote Services, Technique T1021 - Enterprise*, n.d.). Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to interact with a remote network share using SMB. The adversary may then perform actions as the logged-on user. Again, eschewing strong password rules contributes to this.

The asset owner of the Read-Only Domain Controller is Mr. Jonathan Jasper, Senior Systems Administrator.

The asset owner of the Brampton Office Routers is Ms. Tina Mann, Senior Network Administrator.

The asset owner of the Brampton File Server is also Mr. Jonathan Jasper, Senior Systems Administrator.

The asset owner of the Windows 10 personal computer is the End User, or User, the individual who uses the computer for everyday work. We can say now that the End User or User will not be the asset risk owner, as the risk owner is the person tasked with managing the risk.

Based on the information given, we are to choose three (3) main threats we expect DHAEI to face and the challenges we expect them to face while managing these threats. Critical to the choice is the need for the previously listed technical, security, and user requirements to be satisfied. We conclude that the following three (3) assets pose the most critical risks when creating the Brampton branch office:

The Read-Only Domain Controller can be compromised to steal user credentials.

The Brampton Office Routers can be compromised to start a DDoS attack.

The Brampton File Server can be compromised to impersonate end users.

Secondarily, the Brampton File Server can also be compromised through hardware sabotage. Lastly, the Windows 10 computers can be compromised by bypassing the Windows Lock Screen.

**DETERMINING THE RISK OWNERS**

For each risk, a risk owner has to be identified: the person or organizational unit responsible for each risk. We can simplify the process and just assign the asset owner to be also the risk owner, except for the Windows 10 computers. In this case study we will assign the role of Windows 10 PC risk owner to the Senior System Administrator, who will be tasked with managing the attendant risk.

However, the asset owner, if also the risk owner, may not stay as the risk owner for the entire life cycle of the asset. If the identified risk to the asset grows beyond the capacity, capability, or control of the initial owner, it may be escalated to a higher authority, one better able to manage the risk. This could involve transferring the responsibility to another level of management or department with more resources or expertise. A “chain of ownerships of risks” is created. The **chain of ownership of risks** refers to the process of identifying who is responsible for managing and mitigating specific risks at various stages of a project or organizational process. This concept is crucial for ensuring that risks are actively managed by the right individuals or teams. The "ownership" indicates accountability for tracking, addressing, and controlling the risk to minimize its impact.

Consider the following examples.

**Example 1: Consider the Brampton Read-Only Domain Controller**

The Senior Systems Administrator, Jonathan, is responsible for maintaining the security and performance of this server.

#### **Initial Risk Identification**

Jonathan identifies a security vulnerability in the DC software. Let’s assume that it is the vulnerability that allows the threat actor to steal user credentials. Jonathan patches the software and monitors the situation closely, minimizing the risk.

**Risk Ownership Assignment**

As the Senior Systems Administrator, Jonathan owns the risk of this specific vulnerability. He is responsible for implementing patches, monitoring for suspicious activity, and ensuring that the DC is secure.

**Escalation Trigger**

Despite Jonathan’s patching efforts, however, he notices unusual traffic patterns and detects that an attempted breach has occurred. This suggests that a sophisticated attack is underway, potentially from a group targeting the company’s servers. The scale and complexity of the attack are beyond Jonathan’s resources, and it may impact not only the domain controllers but also broader network security and customer trust.

**Risk Escalation**

Recognizing the severity of the situation, Jonathan escalates the risk to the CIO, Ms. Amanda Wilson. This is necessary because the potential breach could affect not only IT infrastructure but also customer data, compliance with regulations (such as GDPR), and the company’s reputation.

**Higher-Level Risk Management**

As the CIO, Amanda takes ownership of the escalated risk. She has the authority to coordinate a company-wide response. Amanda mobilizes the cybersecurity team to perform a full forensic analysis, engages third-party security experts to assist in mitigating the attack, and informs senior leadership about the situation.

**New Controls Implemented**

Amanda decides to temporarily take the domain controller offline to prevent further breaches while the issue is being investigated. She also ensures communication with legal and compliance teams to report the incident to regulatory authorities, if necessary, and begins preparing a customer communication plan in case data was compromised.

In this example, the risk started at the Senior Systems Administrator level but escalated to the CIO when the severity of the situation became apparent. The CIO, with greater authority and resources, can deploy broader security measures, involve legal and compliance teams, and make high-stakes decisions to mitigate damage.

**Example 2: Consider the Brampton Office Routers**

Tina Mann, Senior Network Administrator, is responsible for maintaining the routers and ensuring network reliability.

**Initial Risk Identification**

Tina identifies that one of the core routers in the network is showing signs of intermittent failure. If the router goes down, it could cause connectivity issues for several branches, leading to disruptions in customer transactions and business operations. More importantly, it could lead to clients and customers being unable to access DHAEI’s servers and their own hosted applications, leading to lost revenue, complaints and reputational damage.

**Risk Ownership Assignment**

Tina takes ownership of the risk. She begins troubleshooting the router and schedules a maintenance window to replace it, ensuring minimal disruption to operations. At this stage, the risk is under control and within Tina’s ability to manage.

**Escalation Trigger**

Despite Tina’s efforts, the router experiences a critical failure before the scheduled maintenance. This causes a major outage that affects several branch offices and disrupts real-time financial transactions.The network disruption could also lead to potential regulatory non-compliance and customer dissatisfaction.

The scale of the impact exceeds Tina’s ability to manage alone because it requires more resources to fix the outage quickly and manage external communications, including notifying regulatory bodies and affected customers.

**Risk Escalation**

Realizing the gravity of the situation, Tina escalates the risk to the CIO, Ms. Amanda Wilson. The outage now affects critical business functions, customer trust, and regulatory obligations, requiring higher-level decision-making and resources.

**Higher-Level Risk Management**

As the CIO, Amanda takes ownership of the escalated risk. She immediately assembles a cross-functional team, including the cybersecurity team (to ensure the issue isn’t security-related), legal (for regulatory reporting), and the business continuity team. Amanda also brings in external network specialists to expedite repairs and restore full network functionality as quickly as possible.

#### **New Controls Implemented**

Amanda authorizes the purchase of new, high-reliability routers to prevent future issues, allocates budget for redundant backup systems to minimize the chance of future network failures, and oversees the development of a more robust incident response plan. She also communicates with regulatory agencies and ensures that customers are informed about the outage and the company’s response.

In this example, Tina, the network administrator, initially owned the risk and had plans to manage it, but when the **router failure escalated into a critical outage**, she had to escalate the issue to the CIO. The CIO, with greater authority and resources, could coordinate a comprehensive response involving multiple departments and external partners to mitigate the impact, restore services, and address compliance concerns.

**Example 3: Consider the Brampton File Server**

Jonathan, the Senior Systems Administrator, is responsible for maintaining the Brampton file server operating system, which is Windows Server 2019.

#### **Initial Risk Identification**

Jonathan notices that the Brampton file server is experiencing unusual system behavior, such as frequent crashes and sluggish response times. He also notices the presence of suspicious files and programs. He is concerned that if the server fails completely, the branch office users will not be able to access their data, affecting sales and customer experience.

#### **Risk Ownership Assignment**

Jonathan takes ownership of the risk. He suspects that somehow the server became infected with malware, so he immediately disinfects the server using antivirus software. He also monitors the server closely to ensure it stays operational.

#### **Escalation Trigger**

A short time later, he gets reports from the branch office end users that their other file and application servers are also behaving erratically. The other servers then crash almost simultaneously. The outage causes significant financial losses, disrupts customer transactions, and damages the company’s reputation during a high-traffic period (such as during a flash sale or holiday season, for instance).

Given the scale of the outage and the potential impact on business operations, Jonathan realizes that the issue is beyond his capacity to manage alone. The loss of business and customer dissatisfaction requires immediate high-level intervention and a broader company response.

#### **Risk Escalation**

Jonathan escalates the risk to the CIO, Ms. Amanda Wilson, as the downtime could severely impact the company’s revenue, customer loyalty, and legal obligations (e.g., for online sales guarantees). The situation requires decisions beyond technical fixes, such as managing the financial and reputational impact.

#### **Higher-Level Risk Management**

As the CIO, Amanda takes ownership of the escalated risk. She has the authority to make swift decisions regarding budget and resources. Amanda immediately engages the company cybersecurity team to identify the actual cause of the problem and activate the company’s incident response plan. She calls for the deployment of backup servers and engages the company’s cloud service provider to shift operations temporarily to a cloud-based infrastructure. She coordinates with customer service and legal teams to handle customer complaints, and she initiates an internal investigation to ensure cyber attacks are immediately identified and remediated.

#### **New Controls Implemented**

To prevent future occurrences, Amanda authorizes the purchase of redundant servers and accelerates the company’s move to a hybrid cloud infrastructure for scalability and reliability. She also works with the marketing team to manage public relations and issue statements to customers, explaining the outage and offering discounts to mitigate damage to customer relationships.

In this example, Jonathan, the Senior Systems Administrator, initially owned the risk and attempted to manage it through antivirus, antimalware measures. However, when the branch’s other servers failed during a critical period, the issue escalated beyond technical repairs, impacting the business's overall operations. The CIO took over the risk ownership, enabling a company-wide response to address the financial, technical, and reputational challenges.

**IMPACT AND LIKELIHOOD**

Once risk owners have been identified, it is necessary to assess impacts for each combination of threats and vulnerabilities for an individual asset if such a risk materializes. We are asked to use a rating system where the impact values range from 0 -10:

| **Impact** | **Value** | **Description** |
| --- | --- | --- |
| **No impact** | 0 | No noticeable effect |
| **Insignificant** | 1 | Minor issues, easily managed |
| **Minor** | 2 | Small impact, some effort required to manage |
| **Moderate** | 3 | Noticeable impact, requires management effort |
| **Significant** | 4 | Significant impact, requires substantial management effort |
| **Major** | 5 | Major impact, significant management effort required |
| **Severe** | 6 | Severe impact, major management effort required |
| **Critical** | 7 | Critical impact, severe management effort required |
| **Catastrophic** | 8 | Catastrophic impact, extensive management effort required |
| **Disaster** | 9 | Disaster-level impact, extreme management required |
| **Cataclysmic** | 10 | Cataclysmic impact, potentially unmanageable |

After the assessment of consequences, it is necessary to assess the likelihood of occurrence of such a risk (i.e., the probability that a threat will exploit the vulnerability of the respective asset). We are asked to use a rating system where the likelihood values range from 0 - 5:

| **Likelihood** | **Value** | **Description** |
| --- | --- | --- |
| **Rare** | 0 | Highly unlikely to occur |
| **Unlikely** | 1 | Possible but not expected to happen |
| **Possible** | 2 | Could happen occasionally |
| **Likely** | 3 | Expected to occur in many circumstances |
| **Very Likely** | 4 | Will probably happen in most circumstances |
| **Almost Certain** | 5 | Almost sure to happen |

We can combine both tables into a Risk Assessment Matrix:

|  | | **Likelihood** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Rare** | **Unlikely** | **Possible** | **Likely** | **Very Likely** | **Almost Certain** |
| **0** | **1** | **2** | **3** | **4** | **5** |
| **Severity** | |  |  |  |  |  |  |
| **No Impact** | **0** | 0 | 1 | 2 | 3 | 4 | 5 |
| **Insignificant** | **1** | 1 | 2 | 3 | 4 | 5 | 6 |
| **Minor** | **2** | 2 | 3 | 4 | 5 | 6 | 7 |
| **Moderate** | **3** | 3 | 4 | 5 | 6 | 7 | 8 |
| **Significant** | **4** | 4 | 5 | 6 | 7 | 8 | 9 |
| **Major** | **5** | 5 | 6 | 7 | 8 | 9 | 10 |
| **Severe** | **6** | 6 | 7 | 8 | 9 | 10 | 11 |
| **Critical** | **7** | 7 | 8 | 9 | 10 | 11 | 12 |
| **Catastrophic** | **8** | 8 | 9 | 10 | 11 | 12 | 13 |
| **Disaster** | **9** | 9 | 10 | 11 | 12 | 13 | 14 |
| **Cataclysmic** | **10** | 10 | 11 | 12 | 13 | 14 | 15 |

By entering the values of consequence and likelihood into the Risk Assessment Table, the level of risk is calculated automatically by adding up the two values. This produces a very granular risk assessment matrix. Existing security controls are to be entered in the last column of the Risk Assessment Table. Note that the risk level values range from 0 to a maximum of 15.

For the Read-Only Domain Controller threat of stolen credentials, we can assign a value of 8 for the Impact and 2 for the Likelihood, giving us a risk value of 10.

For the Brampton Office Routers threat of DDoS, we can assign a value of 8 for the Impact and 2 for the Likelihood, giving us a risk value of 10.

For the Brampton File Server threat of Impersonation, we can assign a value of 8 for the Impact and 2 for the Likelihood, giving us a risk value of 10.

For the Windows 10 computers threat of Bypass Windows Lock Screen, we can assign a value of 2 for the Impact and 1 for the Likelihood, giving us a risk value of 3.

For the Brampton File Server threat of Hardware Sabotage, we can assign a value of 8 for the Impact and 1 for the Likelihood, giving us a risk value of 9.

Please refer to **Appendix A: Risk Assessment Table**

**RISK ACCEPTANCE CRITERIA**

Now we have to decide which risk values are acceptable and which are unacceptable. Unacceptable risks must be treated.

The risk values we arrived at are in the range of 0 - 15. Management can make a decision about how to categorize the risks as Acceptable or Unacceptable. We can assume that DHAEI management will decide to only treat risks that significantly impact the asset (“Significant”) while at the same time also having a possible likelihood of happening (“Possible”). Looking at our table, the intersection of Significant on the left and Possible on top gives us a risk value of 6. This means that if a threat has a risk value less than 6, the risk of the threat is acceptable. Otherwise, the risk of the threat is unacceptable and must be looked at. Another way of looking at it is that only if the risk value is greater than or equal to 6 will the risk be addressed.

This is just an example and is based on an impression of how risk-averse DHAEI’s management is. If a company’s decision makers are very risk-averse, then by definition they would prefer to be in an environment where the risk is low. Consequently, their risk value that separates acceptable from unacceptable threats is lower than managers less risk-averse than them. They would want to address a bigger set of risks and consequently manage them. The downside is that doing so devotes more resources to remediate risks that in the end may turn out to be benign.

If we continue with the risk value of 6 as the minimum risk value of a threat to be managed, then from the Appendix A table, we can see that the only threat to an asset that is less than 6 is the Bypass Lock Screen threat to the Windows 10 computers. Management has thus made a decision, a choice, that DHAEI can live with this threat to this asset. The other threats have to be looked at.

**RISK TREATMENT**

To respond to the threats found unacceptable, we will recommend the appropriate controls found in Annex A of ISO 27001 2022 and NIST Controls (NIST SP 800-53 Rev. 5).

For reference we will again list the risks to be addressed:

**The Read-Only Domain Controller can be compromised to steal user credentials.**

In **ISO/IEC 27001:2022**, Annex A, the controls that help prevent login credentials from being stolen are primarily related to **access control**, **user authentication**, and **secure communication**. Some key controls include:

1. **A.9.4.2 - Secure Logon Procedures (Edwards, n.d.)**This control requires organizations to implement secure logon procedures to ensure that authentication is strong and protected. This may involve:
   * Using multi-factor authentication (MFA).
   * Enforcing strong password policies.
   * Preventing password storage in insecure locations.
2. **A.9.4.3 - Password Management System (Edwards, n.d.)**This control mandates secure methods for managing and protecting passwords, ensuring that passwords are encrypted, hashed, or protected in other ways to reduce the risk of theft.
3. **A.13.2.3 - Protection of Confidentiality and Integrity of Information in Transit (Edwards, n.d.)**This control ensures the confidentiality and integrity of sensitive data like login credentials while they are transmitted over networks, reducing the risk of credentials being intercepted (e.g., using encrypted protocols like TLS/SSL).
4. **A.12.6.2 - Technical Vulnerability Management (Edwards, n.d.)**This control ensures that systems are kept up-to-date with security patches, preventing attackers from exploiting known vulnerabilities to steal credentials.

By enforcing these controls, an organization can significantly reduce the risk of login credentials being compromised.

**The Brampton Office Routers can be compromised to start a DDoS attack.**

ISO 27001 Annex A does not directly mention specific technical controls like DDoS (Distributed Denial of Service) prevention. However, several controls in Annex A relate to mitigating the risk of DDoS attacks. The most relevant control is:

### **A.13.1.3 – Segregation in Networks (*ISO 27001 - Annex A.13 - Communications Security*, 2022)**

This control aims to ensure networks are properly segregated to reduce the potential impact of attacks like DDoS. Segmentation of critical services can help prevent a DDoS attack on one part of the network from affecting the entire organization.

In addition, these controls could be relevant for DDoS prevention:

### **A.12.1.2 – Change Management (Edwards, n.d.)**

Ensures proper planning and testing of network changes, which can include measures like configuring firewalls or DDoS mitigation services.

### **A.12.4.1 – Event Logging (Infosavvy, n.d.)**

Ensures the logging of network events to identify unusual traffic patterns, which might indicate a DDoS attack in progress.

### **A.16.1.1 – Responsibilities and Procedures (G, 2023)**

Establishes incident management procedures, including those for handling DDoS incidents.

### **A.13.2.1 – Information Transfer Policies and Procedures (ISODOCS, n.d.)**

Addresses secure information transfer, which can include DDoS prevention mechanisms like secure protocols or traffic filtering.

While ISO 27001 focuses more on processes, a proper DDoS prevention strategy would likely involve additional technical measures, such as firewalls, intrusion prevention systems, and cloud-based DDoS protection services.

**The Brampton File Server can be compromised to impersonate end users.**

Impersonation of end users is a security risk that typically involves attackers pretending to be legitimate users to gain unauthorized access. In ISO 27001 Annex A, there are several controls related to preventing such impersonation, focusing on authentication, identity management, and access control.

The most relevant controls are:

### **A.9.2.2 – User Access Provisioning**

This control ensures that access to information systems is based on formalized procedures and assigned to authorized users only. Proper user identity verification is key to preventing impersonation.

### **A.9.4.2 – Secure Log-on Procedures (G, 2023)**

This control ensures that systems require secure log-on procedures to verify user identity (e.g., using usernames and strong passwords, multi-factor authentication (MFA), etc.), reducing the risk of impersonation.

### **A.9.4.3 – Password Management System (G, 2023)**

Password management systems should ensure the use of strong passwords and prevent weak or easily guessed credentials. This helps prevent unauthorized users from gaining access by impersonating legitimate users.

### **A.9.4.4 – Use of Privileged Utility Programs (G, 2023)**

Privileged utility programs are often used by administrators, but attackers could use them to impersonate users. This control mandates restrictions on the use of such programs to reduce impersonation risks.

### **A.12.5.1 – Installation of Software on Operational Systems (G, 2023)**

This control ensures that unauthorized software, which could be used to perform impersonation attacks, is not installed on operational systems.

### **A.14.1.2 – Securing Application Services on Public Networks (Edwards, n.d.)**

Ensures that communications over public networks are protected, such as using encryption (e.g., SSL/TLS) to prevent attackers from intercepting and using user credentials to impersonate users.

### **A.16.1.4 – Assessment of and Decision on Information Security Events (Edwards, n.d.)**

This control helps detect and respond to security incidents such as impersonation attempts, helping to identify and mitigate such threats in real-time.

By implementing these controls, an organization can reduce the risk of impersonation of end users by ensuring robust authentication and identity verification, alongside monitoring and responding to potential impersonation threats.

**The Brampton File Server can also be compromised through hardware sabotage.**

Preventing hardware sabotage is critical to maintaining the security and integrity of an organization's physical assets. ISO 27001 Annex A includes several controls that indirectly address the risk of hardware sabotage by focusing on physical security, asset management, and incident response. The most relevant controls include:

### **A.11.1.1 – Physical Security Perimeter (Edwards, n.d.)**

This control ensures that physical security measures, such as secure boundaries, are implemented around sensitive areas like data centers or equipment rooms to prevent unauthorized physical access and sabotage.

### **A.11.1.2 – Physical Entry Controls (Edwards, n.d.)**

Access to facilities that house critical hardware should be restricted using physical entry controls (e.g., card readers, biometrics). This control helps to prevent unauthorized personnel from tampering with or sabotaging hardware.

### **A.11.1.4 – Protecting Against External and Environmental Threats (Edwards, n.d.)**

This control ensures that hardware is protected against environmental threats such as fire, floods, or power surges, which could cause damage or sabotage. Proper shielding and protection measures can prevent accidental or malicious damage to hardware.

### **A.11.2.2 – Supporting Utilities (Edwards, n.d.)**

This control ensures that essential utilities (e.g., power, water, cooling) that support hardware operations are protected and maintained. Sabotage to utilities could impact hardware performance and availability.

### **A.11.2.4 – Equipment Maintenance (Edwards, n.d.)**

Regular maintenance of hardware is essential to prevent vulnerabilities that could be exploited for sabotage. This control ensures that equipment is properly maintained and safeguarded against unauthorized modifications.

### **A.11.2.6 – Security of Equipment and Assets Off-Premises (Edwards, n.d.)**

This control ensures that hardware taken off-site (e.g., for remote work or maintenance) is secured and protected against theft or sabotage while it is outside the organization’s controlled environment.

### **A.8.1.1 – Inventory of Assets (Edwards, n.d.)**

Maintaining an accurate and up-to-date inventory of all physical assets, including hardware, ensures that any tampering or sabotage can be quickly detected and addressed.

### **A.14.2.9 – Protection of Test Data (Edwards, n.d.)**

While primarily focused on software, this control ensures that test environments (which could include hardware testing) are secured, preventing sabotage during testing phases.

By implementing these controls, an organization can mitigate the risk of hardware sabotage through physical security measures, proper maintenance, and environmental protections.

**The Windows 10 computers can be compromised by bypassing the Windows Lock Screen.**

In ISO 27001:2022, the prevention of users bypassing the Windows Lock Screen primarily relates to access control and secure system configurations. The relevant controls from Annex A that help address this risk are:

### **A.9.2.1 – User Access Management (G, 2023)**

This control ensures that user access to systems and services is appropriately managed, and users are granted access based on their role and need-to-know basis. Strong access controls can help ensure that unauthorized users cannot bypass the lock screen and gain access to systems.

### **A.9.4.2 – Secure Log-on Procedures (G, 2023)**

This control requires secure log-on processes to be enforced for accessing systems, ensuring that systems (like Windows) lock after a period of inactivity and require proper authentication (e.g., password, biometrics, etc.) to regain access. Configuring Windows policies to enforce lock screen timeouts and password entry helps prevent bypass.

### **A.9.4.3 – Password Management System (G, 2023)**

A strong password management system ensures that users use secure, complex passwords and that password policies (such as lockout after failed attempts) are enforced. These measures help prevent an attacker from bypassing the lock screen by guessing or brute-forcing a password.

### **A.9.2.5 – Review of User Access Rights (G, 2023)**

Regular reviews of user access rights ensure that only authorized users have appropriate access to systems. If users have unnecessary privileges, they may exploit them to bypass security controls, including lock screens. Limiting and auditing these privileges reduces this risk.

### **A.12.6.1 – Technical Vulnerability Management (G, 2023)**

This control ensures that systems are protected against known vulnerabilities, including configuration flaws that might allow users to bypass security mechanisms such as the lock screen. Ensuring Windows systems are patched and correctly configured reduces the risk of vulnerabilities that could be exploited to bypass the lock screen.

By implementing these controls and combining technical measures such as secure log-on procedures, strong password management, and regular access reviews, organizations can minimize the risk of users bypassing the Windows Lock Screen.

Note that **t**his threat is deemed acceptable due to its risk value score being less than the management threshold value of 6. This means that the Annex A controls mentioned above to mitigate and/or remediate this threat will not be implemented in the system.

**NIST Controls (NIST SP 800-53 Rev. 5)**

1. **Cyber Attacks**
   * **Advanced Firewalls**: AC-4 (Information Flow Enforcement), SC-7 (Boundary Protection)
   * **Regular Software Updates**: SI-2 (Flaw Remediation)
   * **Employee Training**: AT-2 (Security Awareness Training)
2. **Insider Threats**
   * **Strict Access Controls**: AC-2 (Account Management), AC-3 (Access Enforcement)
   * **Regular Audits**: AU-2 (Audit Events), AU-6 (Audit Review, Analysis, and Reporting)
   * **Ongoing Employee Training**: AT-3 (Role-Based Training)
3. **Natural Disasters**
   * **Disaster Recovery Plans**: CP-2 (Contingency Plan), CP-4 (Contingency Plan Testing)
   * **Off-Site Backups**: CP-9 (Information System Backup)
   * **Securing Physical Infrastructure**: PE-3 (Physical Access Control), PE-6 (Monitoring Physical Access)

**ISO 27001 Controls (Annex A)**

1. **Cyber Attacks**
   * **Advanced Firewalls**: A.13.1.1 (Network Controls)
   * **Regular Software Updates**: A.12.6.1 (Management of Technical Vulnerabilities)
   * **Employee Training**: A.7.2.2 (Information Security Awareness, Education, and Training)
2. **Insider Threats**
   * **Strict Access Controls**: A.9.1.2 (Access Control Policy), A.9.2.3 (Management of Privileged Access Rights)
   * **Regular Audits**: A.12.4.1 (Event Logging), A.12.4.3 (Administrator and Operator Logs)
   * **Ongoing Employee Training**: A.7.2.2 (Information Security Awareness, Education, and Training)
3. **Natural Disasters**
   * **Disaster Recovery Plans**: A.17.1.1 (Planning Information Security Continuity), A.17.1.2 (Implementing Information Security Continuity)
   * **Off-Site Backups**: A.12.3.1 (Information Backup)
   * **Securing Physical Infrastructure**: A.11.1.1 (Physical Security Perimeter), A.11.1.2 (Physical Entry Controls)

**REFERENCES**

*Acquire Infrastructure: Botnet, Sub-technique T1583.005 - Enterprise*. (2020, October 1).

MITRE ATT&CK®. Retrieved September 17, 2024, from https://attack.mitre.org/techniques/T1583/005/

*Credential Access, Tactic TA0006 - Enterprise*. (2018, October 17). MITRE ATT&CK®. Retrieved September 17, 2024, from https://attack.mitre.org/tactics/TA0006/

*Defense Evasion, Tactic TA0005 - Enterprise*. (2018, October 17). MITRE ATT&CK®. Retrieved September 17, 2024, from https://attack.mitre.org/tactics/TA0005/

Edwards, M. (n.d.). *ISO 27001:2013 – Annex A.11: Physical & Environmental Security*. ISMS.online. Retrieved September 18, 2024, from https://www.isms.online/iso-27001/annex-a-11-physical-and-environmental-security/

Edwards, M. (n.d.). *ISO 27001:2013 – Annex A.12: Operations Security*. ISMS.online. Retrieved September 18, 2024, from https://www.isms.online/iso-27001/annex-a-12-operations-security/

Edwards, M. (n.d.). *ISO 27001:2013 – Annex A.12: Operations Security*. ISMS.online. Retrieved September 18, 2024, from https://www.isms.online/iso-27001/annex-a-12-operations-security/

Edwards, M. (n.d.). *ISO 27001:2013 – Annex A.13: Communications Security*. ISMS.online. Retrieved September 18, 2024, from https://www.isms.online/iso-27001/annex-a-13-communications-security/

Edwards, M. (n.d.). *ISO 27001:2013 – Annex A.14: System Acquisition, Development & Maintenance*. ISMS.online. Retrieved September 18, 2024, from https://www.isms.online/iso-27001/annex-a-14-system-acquisition-development-and-maintenance/

Edwards, M. (n.d.). *ISO 27001:2013 – Annex A.14: System Acquisition, Development & Maintenance*. ISMS.online. Retrieved September 18, 2024, from https://www.isms.online/iso-27001/annex-a-14-system-acquisition-development-and-maintenance/

Edwards, M. (n.d.). *ISO 27001:2013 – Annex A.16: Information Security Incident Management*. ISMS.online. Retrieved September 18, 2024, from https://www.isms.online/iso-27001/annex-a-16-information-security-incident-management/

Edwards, M. (n.d.). *ISO 27001:2013 – Annex A.8: Asset Management*. ISMS.online. Retrieved September 18, 2024, from https://www.isms.online/iso-27001/annex-a-8-asset-management/

Edwards, M. (n.d.). *ISO 27001 – Annex A.9: Access Control*. ISMS.online. Retrieved September 18, 2024, from https://www.isms.online/iso-27001/annex-a-9-access-control/

G, M. (2023, April 17). *ISO 27001 - Annex A.16 - Information Security Incident Management – ISO Templates and Documents Download*. ISO Templates & Documents. Retrieved September 18, 2024, from https://iso-docs.com/blogs/iso-27001-standard/iso-27001-annex-a-16-information-security-incident-management

G, M. (2023, December 18). *ISO 27001 - Annex A.12: Operations Security – ISO Templates and Documents Download*. ISO Templates & Documents. Retrieved September 18, 2024, from https://iso-docs.com/blogs/iso-27001-standard/iso-27001-annex-a-12-operations-security

*Security and privacy controls for information systems and organizations*. (2020). https://doi.org/10.6028/nist.sp.800-53r5

G, M. (2023, December 27). *ISO 27001 - Annex A.9 - Access control – ISO Templates and Documents Download*. ISO Templates & Documents. Retrieved September 18, 2024, from https://iso-docs.com/blogs/iso-27001-standard/iso-27001-annex-a-9-access-control

Infosavvy. (n.d.). https://infocerts.com/iso-27001-annex-a-12-4-logging-and-monitoring/

*ISO 27001:2022 Annex A Control 5.23 - What's New?* (n.d.). ISMS.online. Retrieved September 18, 2024, from https://www.isms.online/iso-27001/annex-a/5-23-information-security-use-of-cloud-services-2022/

*ISO 27001 - Annex A.13 - Communications Security*. (2022, June 27). DataGuard. Retrieved September 18, 2024, from https://www.dataguard.co.uk/blog/iso-27001-annex-a.13-communications-security/

ISODOCS. (n.d.). https://iso-docs.com/blogs/iso-27001-standard/iso-27001-annex-a-13-communications-security?\_pos=1&\_sid=4341929f3&\_ss=r

*Lateral Movement, Tactic TA0008 - Enterprise*. (2018, October 17). MITRE ATT&CK®. Retrieved September 17, 2024, from https://attack.mitre.org/tactics/TA0008/

*Modify Authentication Process, Technique T1556 - Enterprise*. (n.d.). MITRE ATT&CK®. Retrieved September 17, 2024, from https://attack.mitre.org/techniques/T1556/

*NVD - CVE-2019-9510*. (n.d.). NVD. Retrieved September 17, 2024, from https://nvd.nist.gov/vuln/detail/CVE-2019-9510

*Remote Services: SMB/Windows Admin Shares, Sub-technique T1021.002 - Enterprise*. (2020, February 11). MITRE ATT&CK®. Retrieved September 17, 2024, from https://attack.mitre.org/techniques/T1021/002/

*Remote Services, Technique T1021 - Enterprise*. (n.d.). MITRE ATT&CK®. Retrieved September 17, 2024, from https://attack.mitre.org/techniques/T1021/

*Resource Development, Tactic TA0042 - Enterprise*. (2020, September 30). MITRE ATT&CK®. Retrieved September 17, 2024, from https://attack.mitre.org/tactics/TA0042/

# **APPENDIX**

# 

# **Appendix A – Risk Assessment Table**

| **ID #** | **Asset Name** | **Asset Owner** | **Threat** | **Vulnerability** | **Impact (0-10)** | **Likelihood**  **(0-5)** | **Risk (=I+L)** | **Risk Owner** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Read-Only DC | Sr. Sys Admin | Steal Credentials | Use of simple passwords | 8 | 2 | 10 | Sr. Sys Admin |
| 2 | Brampton Routers | Sr. Network Admin | DDoS Attack |  | 8 | 2 | 10 | Sr. Network Admin |
| 3 | Brampton File Server | Sr. Sys Admin | Impersonation | Use of simple passwords | 8 | 2 | 10 | Sr. Sys Admin |
| 3 | Brampton File Server | Sr. Sys Admin | Physical Damage/Sabotage | Inadequate Physical Security | 8 | 1 | 9 | Sr. Sys Admin |
| 4 | Windows 10 PC | User | Lock Screen Bypass | Bug in RDP session logic | 2 | 1 | 3 | Sr. Sys Admin |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | . |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**Appendix B – Risk Treatment Table**

This spreadsheet is a continuation from the Risk Assessment Table spreadsheet.

| **ID #** | **Computed Value of Risk** | **Proposed Risk Response** | **Description of the Proposed Response** | **Estimated Cost** | **Implementation Priority**  **(1-3)** | **Planned Start** | **Review Date** | **Planned Closure** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | $10000 | Secure Logon Procedures | Enforce strong PW policies | $2000 | 1 | 10/1/2024 | 1/1/2025 | 1/7/2025 |
| 2 | $50000 | Network Segregation | Separate networks to reduce impact | $1000 | 1 | 10/1/2024 | 1/1/2025 | 1/8/2025 |
| 3 | $1000 | Secure Logon Procedures | Enforce strong PW policies | $2000 | 1 | 10/1/2024 | 1/1/2025 | 1/8/2025 |
| 3 | $5000 | Physical Entry Controls | Card Readers, Scanners | $2000 | 1 | 10/1/2024 | 1/1/2025 | 1/8/2025 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |