# **Redacted** Security Assessment

Skyler A. Silverio

Western Governors University

## Table of Contents

## Summary

**Redacted** provides design and construction to commercial and residential properties in **Redacted**. **Redacted** has less than 15 employees, including architects, engineers, IT personnel, accountants, and laborers. They recently moved in from their home office to a small office in the local South Bay area. **Redacted**’s IT infrastructure is handled by their internal IT person; however, they needed additional support to address additional security concerns.

The owner of **Redacted** contacted me to perform a security assessment to understand better their current security posture and how it can be improved. **Redacted** feared its current security posture was lacking and its security controls were insufficient, putting its assets at risk. **Redacted** stressed the importance of staying within budget, so I needed to provide cost-effective solutions. **Redacted** also required all security control recommendations to be implemented in a month.

The project's initial phase was to have **Redacted** complete a security assessment checklist. I reviewed the security assessment checklist with **Redacted** to better understand the weaknesses in **Redacted**'s security posture. The checklist assessed **Redacted**’s physical, logical, and administrative controls. The project's next phase was to examine the checklist with **Redacted** to determine which gaps should be remediated. Based on their risk appetite, timeline, and budget, **Redacted** decided to focus on the lack of a password policy, security awareness program, unpatched systems, backup strategy, physical deterrent, and detective controls. The following phase focused on drafting all documents related to the logical control’s supporting documentation, the password policy, and the security awareness program. The fourth phase finalized all the documents above. Also, **Redacted** and I aligned on details with the security controls implementation, such as milestones and constraints. I also procured security cameras, a smart lock, an external hard drive, and Dropbox. The fifth phase initiated the implementation of all the security controls. **Redacted** installed security cameras inside the office and smart locks in the office's entrance. I coordinated with **Redacted** to test and deploy patches. I created online and offline backups using Dropbox and the external hard drive. The organization was notified of the changes and received all the new documents. This included each employee to be trained in the security awareness program. The final phase reviewed and monitored the success of new security controls. Certification was provided to each employee who completed the security awareness program. As a result of the security assessment, **Redacted** substantially increased its security posture.

## Review of Other Work

Proper patch management is a necessity in all organizations. The systems will be at risk of being exploited if not properly managed. Jones (n.d.) states, "A patch management process lays out the steps associated with updating software and hardware." Jones (n.d.) included four tactics for a more effective patch management process: make sure your inventory is current, enforce and review your specific policies, monitor and report, and demonstrate and publish. During the security assessment, we took inventory of all the assets to understand the versions of the systems, established and distributed a new policy specific to patch management, created a testing environment to monitor and document patches before deployment, and communicated with **Redacted** on the progress of the patch management process and its policy. Overall, this substantially increased **Redacted**'s security posture and is a layer in the defense-in-depth strategy.

Cloud storage can allow an organization to scale its data storage needs. Haq et al. (2021) note that cloud storage has many advantages, such as easy accessibility, security, scalability, data syncing, and little data corruption. **Redacted** proceeded with Dropbox as their online storage since the advantages address the organization's needs. Backups are now synced automatically for each user. This addressed a component of **Redacted**'s security gaps, initiating the backup strategy process and ultimately increasing the organization's security posture.

Compromising a password is an avenue a threat can utilize to obtain access to an organization's system; thus, an organization must set up a policy to establish user password guidelines. NCC Group (n.d.) details a password policy that should specify no upper limit on the length of passwords, not based on dictionary words, and the user account is made temporarily inactive after several consecutive failed authentication attempts. **Redacted** and I ensured each of these was included in the new password policy. Each employee was notified and received the password policy. This directly impacted all employees since each employee would have to follow the new policy, resulting in a considerable increase in **Redacted**'s security posture.

## Changes to the Project Environment

**Redacted** recently moved into a new office. Before the security assessment, their office had a standard lock to enter their office and no security cameras on the premises. The security assessment saw the implementation of a smart lock and the installation of security cameras. Employees now have a code that they memorized and a key for the smart locks. The security cameras detect movement to trigger the record button. Video records are stored in their offline storage and are deleted every two weeks.

Patch management and a backup strategy were also implemented. **Redacted** now updates its systems to the most up-to-date patch regularly. They use an external hard drive as the on-site storage and Dropbox as their cloud storage. The offline backup is differentially updated every two weeks, and the online backup is synced to each user. I created documents that supplement the new implementations.

Additionally, **Redacted** did not have any documentation regarding security or IT, such as procedures, policies, and work instructions. Administrative controls did exist at **Redacted**. I created a security awareness program to identify phishing emails and social engineering tactics. All employees needed to be trained in these subjects, and I provided the employees with a certificate upon completion. I also created a password policy for all employees to follow. The password policy details an acceptable password and how to handle a password if compromised.

## Methodology

For **Redacted**'s security assessment, I utilized the ADDIE methodology. This specific methodology is a five-step process: analysis, design, development, implementation, and evaluation.

The analysis phase was conducted once the security assessment checklist was completed. **Redacted** and I reviewed the organization's gaps and determined which gaps will be addressed. Gaps that were addressed were determined by **Redacted**'s risk appetite. At the end of the review, **Redacted** wanted to implement security cameras, smart locks, patch management, online and offline backups, a security awareness program, and a password policy. During this phase, we were attentive to the timeline and budget.

The design phase focused on administrative controls and any additional documentation that is needed for the remaining security controls. From this phase, the security awareness program, password policy, and relevant logical control documentation were initiated. This provided a roadmap for the implementation of the various controls.

The development phase finalized all aforementioned documents. Also, since this phase preceded the implementation phase, **Redacted** and I met to ensure we were aligned on the implementation phase and that all controls were ready to be implemented. This included procurement of the physical controls.

The implementation phase saw the installation of security cameras and smart locks. The locks were all programmed to a code that was decided by **Redacted**. I coordinated with **Redacted** to implement patch management and a backup strategy and created documents related to these two logical controls. All **Redacted**'s employees received the security awareness program and were tested on their knowledge. They also received all newly created documents, such as the password policy patch management and backup strategy documents.

Finally, the evaluation phase reviewed and monitored the implementation of the security controls. As a result of training, any related certification was provided to the employees who demonstrated they understood the material.

### Project Goals and Objectives

| | Goal | Supporting objectives | Deliverables enabling the project objectives |
|---|---|---|---|
| 1 | Understand the current security posture of **Redacted** | 1. a. Complete the security assessment checklist | 1. a.i. Completed Security assessment checklist |
| | | 1. b. Review the security assessment checklist with **Redacted** | 1. b.i. Completed Security assessment checklist |
| | | 1. c. Determine the gaps that will be addressed from the security assessment checklist | 1. c.i. Completed Security assessment checklist |
| 2 | Plan the remediation of the security gaps | 2.a. Determine the physical controls to be implemented | 2. a.i. Research which physical controls best fit the needs and budget of the organization. |
| | | | 2.a.ii Work with **Redacted** to discuss the implementation of the physical controls |

| | | | |
|---|---|---|---|
| | | 2. b. Determine the logical controls to be implemented | 2. a.i. Research which logical controls best fit the needs and budget of the organization. |
| | | | 2.b.ii. Determine the necessary documentation needed to supplement the logical controls. |
| | | | 2.b.iii Work with **Redacted** to discuss the implementation of the logical controls |
| | | 2. c. Determine the administrative controls to be implemented | 2. c.i. Research which administrative controls best fit the needs of the organization. |
| | | | 2.c.ii. Design and develop relevant documents |
| | | | 2. c.iii Work with **Redacted** to discuss the implementation of the administrative controls |
| 3 | Implementation of security controls | 3.a. Physical controls implemented | 3. a.i. Procurement of physical controls |
| | | | 3.a.ii. Installation of physical controls |
| | | 3. b. Logical controls implemented | 3. b.i. Coordinating with **Redacted** on the implementation of various logical controls |
| | | | 3.b.ii. Finalizing relevant documentation for their respective logical controls |
| | | 3. c. Administrative controls implemented | 3. c.i. Finalizing relevant documentation for their respective administrative controls |
| 4 | Notify **Redacted** on the addition of various security controls | 4.a. **Redacted** will review the security controls to the entire organization in a meeting. | 4.a.i. Reviewing the security controls that are implemented in a meeting |
| | | 4.b. **Redacted** will send an email with all relevant documents. | 4.b.i. Sending an email of all relevant security control documents to the organization |

Goal 1: Understand the current security posture of **Redacted**. To begin the security assessment process, I needed a complete understanding of the current security posture of **Redacted**. This allowed me to properly provide **Redacted** with correct remediation for their security gaps by implementing various adequate security controls. To accomplish this, three objectives needed to be achieved.

Objective 1.a.: Complete the security assessment checklist. The security assessment checklist was the primary way to determine the security gaps of **Redacted**. **Redacted** and I referenced the completed security assessment checklist. This objective will have one deliverable.

Deliverable 1.a.i.: Completed security assessment checklist. The completed security assessment checklist facilitated detailing **Redacted**’s security posture.

Objective 1.b.: Review the security assessment checklist with **Redacted**. As a result of reviewing the security assessment checklist with **Redacted**, we determined the project's scope and gained a clearer idea of the timeline, budget, and other potential constraints. This objective had one deliverable.

Deliverable 1.b.i.: Completed security assessment checklist. **Redacted** and I needed a completed security assessment checklist to review the security assessment checklist. Reviewing the completed security assessment checklist decided which security controls to implement.

Objective 1. c.: Determine the gaps that will be addressed from the security assessment checklist. Based on the gaps presented, their risk appetite, timeline, and budget, **Redacted** focused on the lack of a password policy, security awareness program, outdated systems, backup strategy, physical deterrent, and detective controls. This objective had one deliverable.

Deliverable 1.c.i.: Completed security assessment checklist. Gaps were unable to be addressed unless the security assessment checklist was completed. Without it, **Redacted** failed to make justified business decisions regarding its security gaps.

Goal 2: Plan the remediation of the security gaps. As a result of completing the security assessment checklist, reviewing it, and determining the gaps, **Redacted** and I planned the remediation of the security gaps. We decided where to purchase the physical controls and how to implement the logical controls and drafted the administrative goals. To accomplish this goal, three objectives needed to be met.

Objective 2.a.: Determine the physical controls. We determined that **Redacted** will install security cameras and smart locks. Two deliverables were needed to achieve this objective.

Deliverable 2.a.i.: Research which physical controls best fit the needs of **Redacted**. I found that a smart lock with a keypad, Wi-Fi, deadbolt lock, and a security camera with motion sensing best fit **Redacted**’s needs.

Deliverable 2.a.ii: Work with **Redacted** to discuss the implementation of physical controls. I requested approval from **Redacted** on the physical control to purchase. I coordinated with **Redacted** to establish when and how to install physical controls.

Objective 2.b.: Determine the logical controls. We determined that **Redacted** will implement a patch management and backup strategy. The backup strategy included an on-site and off-site backup. Three deliverables were needed to achieve this objective.

Deliverable 2.b.i.: Research which logical controls best fit the needs of **Redacted**. I found that Dropbox, as the online storage, and an external hard drive, as the offline storage, best suit the needs of **Redacted**. Regularly scheduled and tested patches by the in-house IT person were decided to fix the organization's patch management issues.

Deliverable 2.b.ii.: Determine the necessary documentation needed to supplement the logical controls. Each logical control required supporting documentation to be created. I ensured the frequency and method of backups and how to test and release patches were included in the relevant documentation.

Deliverable 2.b.iii. Work with **Redacted** to discuss the implementation of logical controls. I notified **Redacted** of the patch management and backup strategy that needs to be implemented. I worked with the IT personnel to review the implementation details and date.

Objective 2.c.: Determine the administrative controls. We determined a security awareness program and password policy will be needed. Three deliverables were required to achieve this objective.

Deliverable 2.c.i.: Research which administrative controls best fit the needs of **Redacted**. I decided that the security awareness program should include training about phishing and social engineering tactics. The password policy needs to address how to handle passwords if compromised and the strength of the password.

Deliverable 2.c.ii.: Design and develop relevant documents. I previously created a security awareness program and password policy template that can be altered for **Redacted**.

Deliverable 2.c.iii. Work with **Redacted** to discuss the implementation of administrative controls. **Redacted** needed to approve the details in the password policy. We scheduled the rollout of the security awareness program and the deadline for the training to be completed.

Goal 3: Implementation of Security Controls. **Redacted** installed physical controls first. The logical controls took longer than expected due to delays in procurement and creating the supporting documents. Administrative controls were quicker due to templates I previously made. **Redacted** and I were in constant communication with this entire implementation process to ensure success. Three objectives were met in this goal.

Objective 3.a.: Physical controls implemented. **Redacted** implemented all physical controls. Two deliverables will be required to complete this objective.

Deliverable 3.a.i: Procurement of physical controls. I notified **Redacted** about which security cameras and smart locks to purchase. They approved both physical controls, and they arrived earlier than expected.

Deliverable 3.a.ii.: Installation of physical controls. **Redacted** and I installed the security cameras inside the office and the new smart lock in the main entrance.

Objective 3.b.: Logical controls implemented. **Redacted** implemented all logical controls. Two deliverables were required to complete this objective.

Deliverable 3.b.i.: Coordinating with **Redacted** on implementation of various logical controls. **Redacted**'s IT personnel and I faced issues testing the patches in the test environment. We could not proceed with deployment until approved by the heads of **Redacted**. This resulted in not meeting our expected deadline for this delivery. I worked with **Redacted** to back up their data offline and online.

Deliverable 3.b.ii.: Finalizing relevant documentation for their respective logical controls. We had to delay finalizing the documentation due to the delay in the implementation. In the backup strategy policy, I detailed that the external hard drive will be used to back up the data differentially every two weeks. Dropbox is synced automatically to each user. In the patch management policy, I noted that the patches must be tested before deployment.

Objective 3.c.: Administrative controls implemented. I created a password policy and security awareness program dedicated only to **Redacted** and its personnel. We finalized details regarding the training for the employees. Two deliverables were required to complete this objective.

Deliverable 3.c.i.: Finalizing relevant documentation for their respective administrative controls. I finalized all the documents and had them approved by **Redacted**.

Goal 4: Notify **Redacted** of the addition of various security controls. Once all security controls were implemented, I notified **Redacted** of the completion. **Redacted** created a meeting and drafted an email to discuss the implementations with the employees. Two objectives needed to be met to complete this goal.

Objective 4.a.: **Redacted** will review the security controls for the entire organization in a meeting. **Redacted** detailed all the security controls implemented in the organization.

Deliverable 4.a.: Reviewing the security controls that are implemented in a meeting. **Redacted** reviewed all the security controls implemented in a meeting and the importance of the new security controls. Additionally, **Redacted** notified the organization of the deadline for the training.

Objective 4.b.: **Redacted** will send an email with all relevant documents. Supplementing the meeting, **Redacted** sent an email with all relevant documents. This provided the exact process of all the security controls implemented and policies that must be followed. This objective also saw the employees completing the training and receiving a certificate of completion.

Deliverable 4.b.: Sending an email of all relevant security control documents to the organization. **Redacted** sent an email following the meeting with all relevant security control documents. All employees also needed to complete all the training.

## Project Timeline

| Milestone or deliverable | Planned Duration (hours or days) | Actual Duration (hours or days) | Actual start date | Actual end date |
|---|---|---|---|---|
| Completed security assessment checklist | 3 days | 3 days | April 22, 2024 | April 25, 2024 |
| Review the security assessment checklist with **Redacted** | 1 day | 1 day | April 26, 2024 | April 26, 2024 |
| Determine the gaps that will be addressed from the security assessment checklist | 1 day | 1 day | April 26, 2024 | April 26, 2024 |
| Research which security controls (physical, logical, and administrative) best fit the needs and budget of the organization | 5 days | 5 days | April 29, 2024 | May 3, 2024 |

| | | | | |
|---|---|---|---|---|
| Determine the necessary documentation needed to supplement the security controls (logical and administrative). | 3 days | 2 days | May 1, 2024 | May 3, 2024 |
| Design and develop relevant documents for the administrative controls | 3 days | 3 days | May 1, 2024 | May 4, 2024 |
| Work with **Redacted** to discuss the implementation of the security controls (physical, logical, and administrative) | 5 days | 4 days | May 6, 2024 | May 9, 2024 |
| Procurement of physical controls | 2 days | 2 days | May 8, 2024 | May 9, 2024 |
| Installation of physical controls | 2 days | 2 days | May 10, 2024 | May 11, 2024 |
| Coordinating with **Redacted** on the implementation of various logical controls | 5 day | 7 days | May 13, 2024 | May 20, 2024 |
| Finalizing relevant documentation for their respective logical controls | 2 days | 3 days | May 13, 2024 | May 16, 2024 |
| Finalizing relevant documentation for their respective administrative controls | 2 days | 1 day | May 14, 2024 | May 14, 2024 |
| Review the security controls that are implemented in a meeting with **Redacted**’s employees | 1 day | 1 day | May 22, 2024 | May 22, 2024 |
| Sending an email of all relevant security control documents to the organization | 1 day | 1 day | May 22, 2024 | May 22, 2024 |

## Unanticipated Requirements

One unanticipated component occurred during the implementation of patch management. I did not expect this milestone to take longer than expected. This was due to the in-house IT personnel not being available in the middle of the implementation. There were also issues in the testing environment, where patches were not updated to the correct version or were not on time. The IT personnel were able to fix this issue when they returned by creating a PowerShell script. I notified the **Redacted** contacts of the delays and documented the solution to the problem.

## Conclusions

Prior to the security assessment, **Redacted** struggled with its physical, administrative, and logical controls. The security assessment succeeded in increasing **Redacted**'s security posture. **Redacted** saw an immediate impact on the security posture due to the quick installation of security cameras and smart locks. Each employee now needs to memorize a code to access the office. All systems were updated to a newer patch, and the IT personnel are properly managing and testing the patches before deployment. This will be a regular process and will affect the security of the organization's current and future assets. Also, an online and offline backup strategy was created. **Redacted** now uses Dropbox, which is synced up regularly, and an external hard drive, which is regularly backed up. Lastly, administrative controls yielded an immediate impact because all employees must follow any new policies and training.

Following the project's completion, I sent a survey to **Redacted** regarding the effectiveness of the security controls and the organization's satisfaction with them. They noted that every employee had been trained in the security awareness program and received a certificate of completion. The employees expressed high satisfaction regarding the content of the program. They also stated that they were very satisfied with the logical controls and the relevant policies. A defense-in-depth strategy has been implemented with all security controls implemented, substantially increasing **Redacted**'s security posture. It is important to note that **Redacted** continues to follow the policies created. If not followed, **Redacted**'s security posture will revert to the state prior to the security assessment.

## Project Deliverables

Appendix A contains the security cameras purchased. They were installed inside the office. They provided detective and deterrent measures against threats. Records from the security cameras are saved in the new online storage for two weeks, where they will be deleted to save storage space.

Appendix B shows the installed smart lock. The smart lock was installed at the office entrance and required the person to enter a code to access the premises, increasing the security posture of **Redacted**.

Appendix C displays the certificate of completion for the security awareness program. Each employee must complete the training as required in the new administrative policy. The program details how to identify phishing emails and social engineering tactics.

Appendix D displays the external hard drive that **Redacted** will use for offline storage. This is part of the backup strategy implemented as there will also be an online cloud storage, Dropbox, used. The external hard drive will be used biweekly to back up the data differentially.

# References

Haq, S. U., Asif, A., Khan, A. A., Rehman, A., Badr, A., & Shah, M. A. (2021). *Review of deep learning models for sentiment analysis*. *Xisdxjxsu Journal*, *17*(6), 276–283. https://www.xisdxjxsu.asia/V17I6-26.pdf

Jones, A. (n.d.). *The Patch Management Process: A Full Overview (plus the steps most teams miss)*. Puppet by Perforce. https://www.puppet.com/blog/patch-management-process

NCC Group. (n.d.). *Password policies in practice: Measuring the effectiveness of password management* [White paper]. NCC Group. Retrieved August 12, 2024, from https://research.nccgroup.com/wp-content/uploads/2020/07/password-policies.pdf

## Appendix A

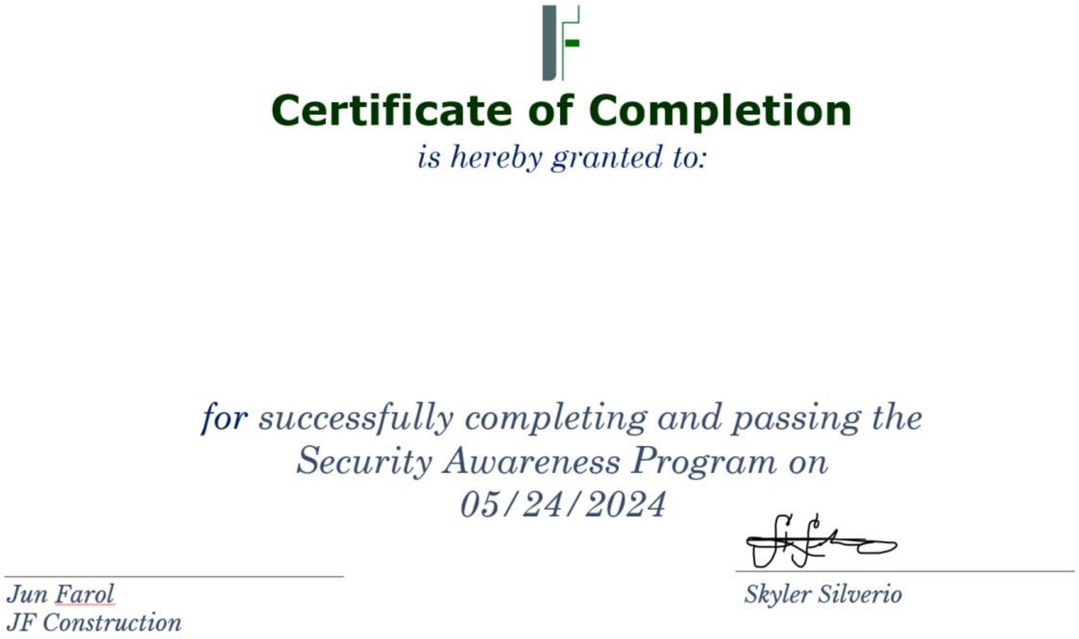
FS IPC101-5M-D Security Camera

## Appendix B

### DL270026D Trilogy By T2 Smart Lock

## Appendix C

### Security Awareness Program Certificate of Completion



**Certificate of Completion**

*is hereby granted to:*

*for successfully completing and passing the Security Awareness Program on 05/24/2024*

*Jun Farol*
*JF Construction*

*Skyler Silverio*

## Appendix D

### Western Digital 10TB Elements Desktop External Hard Drive