Performance Assessment - Cybersecurity Graduate Capstone - Task 3

Western Governors University

Khalid Diriye

C796 - Cybersecurity Graduate Capstone

Dr. Wendy Campbell

12/16/23

Table of Contents

Technology Supported Security Solution

Introduction

Ali Clinic faced significant security problems as the clinic was impacted by the WannaCry (Kaspersky. 2023, July 6) ransomware attack, which encrypted critical data and rendered workstations and servers unusable, halting the clinic's operations and leaving the company at a standstill. To resolve this crisis, Ali Clinic's executive management opted to pay the cybercriminals to regain access to their data. However, this was a temporary solution as there was an impending threat of future malware attacks. Ali Clinic hired Endpoint Security to conduct a risk assessment, provide a solution, and create a comprehensive plan for a system overhaul. In this paper we take a look at the post-implementation of the solution and how the solution has impacted Ali Clinic and its stakeholders.

Consensus-based policies

The consensus-based policies developed for the project solution to security issues at Ali Clinic were established to address the ongoing malware attacks the clinic was facing to do this the solution enhanced the security posture of the clinic's infrastructure and ensured compliance with industry standards standards such as HIPAA (Health Insurance Portability and Accountability Act) (Office for Civil Rights (OCR). 2022, October 19), HITRUST (Health Information Trust Alliance) (HITRUST alliance. (n.d.-b), ISO (International Organization for Standardization) 27001 (International Standards Organization Security Control Framework. (n.d.-a)), and NIST (National Institute of Standards and Technology) SP (Special Publication) 800-53 (NIST SP 800 53. (n.d.)).

Standards and Practices

The standards and practices such as NIST SP 800-53 will be used to leverage a comprehensive catalog of security and privacy controls which is used to implement security measures to protect patient data from a variety of threats. HIPAA and HITRUST adhere to the compliance of world-leading healthcare industry standards HITRUST works with healthcare facilities to meet HIPAA compliance and provides a certification validating the facility's ability to effectively manage data, information risk, and compliance. HIPAA is a federal law to protect patient health information (PHI) from being disclosed to unauthorized entities. These two healthcare standards focus on healthcare-specific requirements ensuring confidentiality, integrity, and availability of patient data. ISO 27001 is best known for information security management systems (ISMS) and it provides companies with guidance on the implementation, maintenance, and continual improvement of information security management systems. This standard is relevant because the solution is using Azure technologies which is already ISO 27001 compliant. Finally, an agile approach methodology will be used as it facilitates flexibility, adaptability, and continuous stakeholder engagement throughout the project. Agile principles help address emerging security threats and maintain structured, manageable iterations.

Cybersecurity Problem Addressed

The cybersecurity problem addressed at Ali Clinic covers several facets highlighted below. Ali Clinic was impacted by the WannaCry ransomware attack that encrypted critical data rendering workstations and servers alike useless. To resolve this Ali Clinic executive management paid the cybercriminals in order to get their data back but it was only a matter of time before another malware attack commenced so they permanently resolved the ongoing attacks Endpoint Security was hired to provide guidance, create an implementation plan for system overhaul and provide security assessment.

1. **Vulnerabilities and Outdated Infrastructure**

a. The existing hardware which included outdated server hardware and networking equipment reached end of life, and vulnerabilities were present in the system such as CVE-2019-1471 (CVE-2019-1471. NVD. (n.d.-a)) which allows remote code to be executed on host systems when the host server improperly validates input, CVE-2020-3231 (Cisco. 2023, November 7) which allows unauthenticated attackers to forward broadcast traffic before being authentication on a port, and SYNful Knock (Santos, O. 2015, September 15) which is a type of backdoor that affects routers where the attacker gains complete control of the router and the network after successfully replacing firmware. The security solution aimed to identify and address these vulnerabilities, implementing updates and upgrades to secure the infrastructure.

2. Lack of Security Awareness

a. Employees lacked sufficient security awareness and training which led an employee at the company to install the initial malware infection that spread across the network affecting multiple systems. This can be avoided in the future with the security solution which includes a comprehensive training program to enhance the security knowledge of the Ali Clinic IT staff, ensuring they can effectively manage and maintain security measures.

3. Compliance Gaps

a. Ali Clinic being a healthcare facility is required to meet healthcare standards to avoid putting their patients at risk. The clinic needed to comply with healthcare industry standards such as HIPAA, HITRUST, NIST SP 800-53, and ISO 27001. The security solution focused on closing compliance gaps and ensuring the clinic met the necessary legal and regulatory requirements. This involved having the compliance and legal departments heavily involved in the implementation of the new security solution.

Decision Making

The solution supported decision-making by addressing the specific needs of the clinic's environment through a set of policies, standards, and practices. One crucial aspect was risk prioritization, achieved through a comprehensive security assessment that identified and ranked vulnerabilities based on severity and potential impact. This approach enabled the clinic to focus on addressing the most critical risks first, enhancing overall security. Aligning with industry standards (NIST, HIPAA, HITRUST, ISO 27001) was another key element. This ensured that the technologies chosen, including Microsoft Azure and Red Hat Linux, met the necessary security requirements to be chosen vendors. This alignment not only facilitated decision-making in selecting secure technologies but also ensured compliance with healthcare industry standards (HIPAA and HITRUST). The adoption of an agile methodology played a significant role in supporting decision-making throughout the project. Agile practices such as short iterations, continuous feedback loops, and stakeholder engagement, provided the flexibility to adapt to emerging security challenges. This iterative approach allowed the project team to make informed decisions based on real-time feedback and evolving requirements. Consideration of the clinic's limited resources and budget constraints was also integrated into the solution. The implementation of a hybrid SaaS and On-Premise model, utilization of open source software (Uptime Kuma (Louislam. (n.d.))), and strategic technology choices were tailored to align with the clinic's specific environment. This approach ensured that the solution met the clinic's needs effectively while staying within budgetary constraints.

Cybersecurity Assurance Criteria

Automation

The solution implemented for Ali Clinic aligns with cybersecurity assurance criteria by addressing the aspects of promoting automation in cybersecurity, improving and modernizing

security, and implementing industry-standards security tools and infrastructure/environment. The solution promotes automation in cybersecurity by continuous monitoring and evaluation as the project incorporates automated monitoring systems such as Uptime Kuma and Microsoft Defender for Cloud (Microsoft. (n.d.)). These tools enable continuous tracking of security events, system performance, and compliance status. Automation in monitoring enhances the clinic's ability to detect and respond to emerging threats in a quick fashion and ensures patient care is not affected. With vulnerability assessment tools such as Rapid7 InsightVM (InsightVM Documentation. (n.d.)), Nessus (Nessus. (n.d.)), and OpenVAS are used to identify and assess vulnerabilities across the clinic's infrastructure, streamlining the process and ensuring a more comprehensive evaluation.

Modernization of Security

The project improves and modernizes security by infrastructure upgrades and use of a more up-to-date methodology such as agile. The project involves the modernization of the clinic's infrastructure moving off end-of-life (EOL) software and hardware such as Windows Server 2016 in the data center which reached end-of-life 11/01/2022, Cisco networking equipment such as Cisco 2811 router, Cisco PIX 515 firewall, and Cisco 2960 switches have reached EOL as well and are vulnerable to attacks by malicious cybercriminals. The solution implemented a hybrid SaaS and On-Premise model includes the adoption of Microsoft Azure (n.d.)) and Red Hat Linux (Red Hat Customer Portal. (n.d.)), enhancing the overall security posture with up-to-date and secure technologies. For networking the solution used a Cisco ISR 1100 router (Cisco. 2023, August 3) and Cisco Catalyst 9300 Switches (Cisco. (2023, December 5) which are in support and offer advanced features and better security capabilities. For each sprint, we'll be using agile methodology throughout the project which promotes continuous improvement and adaptation of evolving security challenges. Short iterations and regular evaluations contribute to an environment that can quickly respond to emerging threats and security advancements.

Industry Standards Alignment

The project's industry standards align with NIST SP 800-53, HIPAA, HITRUST, and ISO 27001. Microsoft Defender for Cloud will continuously check if systems are compliant and identify issues that may be hindering achieving compliance. The solution implemented these standards, so the clinic ensures that its security measures meet recognized benchmarks to protect patient data and effective patient care. The security tools used will include popular and widely used vulnerability assessment tools such as Rapid7 InsightVM, Nessus, and OpenVAS which will ensure that the clinic follows established practices for vulnerability management and penetration testing. Microsoft Defender for Cloud will be used as a monitoring solution keeping track of security posture and recommending changes in the cloud and on-premise systems. These tools are widely recognized and trusted in the cybersecurity industry.

Data Collection and Implementation Elements

Digital Evidence

The solution for Ali Clinic is designed to address data collection and implementation elements with a focus on collecting digital evidence for analysis or forensics and implementing confidentiality, integrity, and availability. It does this by logging and monitoring systems and using vulnerability assessment tools. The logging and monitoring monitor systems in the project incorporate Uptime Kuma and Microsoft Defender for Cloud, to collect digital evidence related to system and security events. These logs provide a comprehensive record of activities aiding in forensic analysis for cases of security incidents. The vulnerability assessment tools that are used are InsightVM, Nessus, and OpenVAS which are utilized to conduct vulnerability assessments. These tools not only identify vulnerabilities but also generate detailed reports that serve as digital evidence. This evidence is crucial for analyzing potential threats and weaknesses in the clinic's infrastructure.

Implementation of CIA

The project implements confidentiality, integrity, and availability by being compliant with industry standards such as HIPAA, HITRUST, NIST SP 800-53, and ISO 27001, which inherently emphasize confidentiality, integrity, and availability of data. Adhering to these standards ensures that patient information is handled with the utmost care and meets regulatory requirements. The implementation of secure infrastructure contributes to confidentiality, integrity, and availability by upgrading systems to use a hybrid SaaS and On-Premise model that make use of cloud technologies such as Microsoft Azure (ISO 27001 compliant (Stevevi. (n.d.)) and for on-premise we're using Red Hat Linux. These technologies provide secure environments for storing and processing sensitive healthcare information. The role that Endpoint Security plays is that they provide penetration testing and vulnerability management which enhances the integrity of the clinic's systems. By identifying and addressing vulnerabilities, the solution ensures that the integrity of patient data is maintained. This approach is pivotal in safeguarding patient data and maintaining the overall security posture of Ali Clinic.

Investigation and Mitigation of Cybersecurity Incidents and Crimes

The project solution implemented at Ali Clinic incorporates a robust approach to investigating and mitigating cybersecurity incidents and crimes within the environment. The process involves proactive measures, continuous monitoring, and well-defined incident response procedures. For incident detection, we will be using Uptime Kuma for uptime and certification detection and Microsoft Defender for Cloud for on-prem and cloud threat detection and protection. These two tools will be deployed to monitor system and security events continuously. These tools help in the early detection of anomalies, potential security breaches, or any unusual activities within the environment. Additionally, the vulnerability assessment tools used by Endpoint Security (InsightVM, Nessus, and

OpenVAS) will be used during the security assessment phase and will play a crucial role in identifying vulnerabilities. Addressing these vulnerabilities promptly reduces the likelihood of exploitation and potential incidents.

Incident Investigation

Incident investigation is focused on forensic analysis, logging, and documentation. Here we can see that in the event of a suspected incident or breach, the collected digital evidence from monitoring systems and vulnerability assessments serves as a foundation for forensic analysis. Endpoint Security, equipped with expertise in penetration testing and vulnerability management, conducts thorough investigations to understand the nature and scope of incidents. The project emphasizes the use of version-controlled repositories in Microsoft Azure DevOps (Chcomley. (n.d.)). This includes incident response plans, procedures, and outcomes. The documentation in Azure DevOps is valuable for post-incident analysis, ensuring that lessons learned contribute to ongoing improvement.

Incident Mitigation

Incident mitigation points to the use of agile which is adopted in the project to facilitate a quick response to emerging security threats. Short iterations and continuous stakeholder engagement enable the team to adjust security measures promptly based on incident findings. Additionally, the use of a business continuity plan in the implementation aligns with CISSP (Certified Information Systems Security Professional) best practices (Infosec. (n.d.)), and ensures that predefined strategies are documented to help mitigate the impact of incidents. This includes recovery strategies, incident response procedures, and communication plans to minimize downtime.

Audits and Improvement

For legal and compliance the project includes legal and compliance audits that the legal and compliance department will be doing throughout the project’s implementation, the involvement of

both legal and compliance ensures that incident response and mitigation efforts comply with relevant regulations and laws, mitigating legal consequences. Finally, the efforts on continuous improvement where a lessons learned report will be generated post-incident, involves evaluation of the effectiveness of incident response actions, adjusting security measures, and enhancing staff training based on real-world incidents.

Cybersecurity Plans

In crafting a comprehensive cybersecurity strategy for Ali Clinic, our solution aligns with industry-recognized regulatory standards, ensuring a robust defense against potential threats. The implementation adheres to prominent frameworks such as NIST SP 800-53, ISO 27001, HIPAA, and HITRUST, attesting to the commitment to the highest standards of security and compliance. This section outlines the tools and repositories employed, such as Microsoft Azure DevOps and Terraform, which play pivotal roles in source code management, infrastructure deployment, and adherence to established cybersecurity procedures.

Regulatory Compliance

The solution is aligned with regulatory compliance which is focused on industry standards such as NIST SP 800-53, HIPAA, HITRUST, and ISO 27001. The solution is aligned with each of these standards and frameworks ISO 27001 and NIST SP 800-53 will provide a comprehensive set of security controls and guidelines that are crucial for safeguarding patient data and ensuring the confidentiality, integrity, and availability of information. HIPAA and HITRUST compliance will be used to prioritize compliance with the HIPAA and the HITRUST standards. These regulations set specific requirements for securing sensitive patient health information.

Applications

The applications, source code, and guides will be done through using Microsoft Azure DevOps Repositories which will allow for version control and management of source code. For example, security measures, such as scripts for encryption mechanisms using RedHat Linux (RHLE) 8, are stored in these repositories, providing a centralized and versioned location to achieve a robust software development life cycle (SDLC) that will ensure secure code is being used in the project. Terraform will also be part of the project to template all infrastructure configuration as part of the project in the planning and design phase, a detailed Infrastructure as Code (IaC) plan is developed using Terraform, a popular tech stack for building out systems and configuring networking resources. This plan includes specific configurations, such as the deployment of Red Hat Linux (RHEL) and Microsoft Azure VMs, contributing to a transparent and replicable infrastructure setup.

Post-Implementation Environment

The post-implementation environment explores various aspects of the efficiency of the solution, analysis of new data collected, the summative evaluation plan, post-implementation risks, and how the security solution aligns with and meets the needs of project stakeholders. These aspects are critical in ensuring that the implemented security measures not only address the current challenges of malware attacks but also adapt to the evolving digital threat landscape, thus maintaining the integrity and resilience of the system.

Efficiency of the Solution

The efficiency of the solution post-implementation involves assessing how well the new systems or processes meet the clinic’s cybersecurity needs. The solution's efficiency is reflected in its ability to effectively mitigate threats, streamline security processes, and improve overall system performance, ensuring reduced vulnerability to attacks and improved response times to security incidents. For example, the use of Microsoft Defender for Cloud helps the clinic automate

vulnerability scanning, enhancing the efficiency of identifying and addressing potential security weaknesses. The infrastructure updates and upgrades provide us the ability to make use of both the cloud and on-prem technologies such as Microsoft Azure and Red Hat Linux. This upgrade increases security and compliance with industry standards as Azure is already ISO 27001 compliant (Stevevi. (n.d.)). The use of compliance monitoring from Microsoft Defender for Cloud helps the clinic's security posture and compliance by ensuring that its systems have met the requirements of HIPAA, HITRUST, NIST SP 800-53, and ISO 27001. Along with this security training is provided to all staff to ensure proper handling and understanding of new security measures which helps protect the clinic from employees in the future exposing the systems to threats. Finally, continuous monitoring and evaluation are established to ensure the clinic stays up-to-date in its security posture using tools like Uptime Kuma and Microsoft Defender for Cloud.

New Data

New data generated post-implementation will greatly help increase incident resolution time and better meet service-level agreements (SLA) with customers. The improved security monitoring using tools like Microsoft Defender for Cloud, provides a more efficient collection and analysis of security logs, enhancing the ability to monitor and respond to threats. The enhanced compliance reporting from the solution enables more systematic accurate compliance reporting, aiding in meeting standards such as HIPAA and HITRUST. The compliance checks from Microsoft Defender for Cloud keeping the clinic on track and in compliance with healthcare industry standards will greatly help the clinic's image and provide the patients with better care. The incident response process is streamlined as more data is available to help debug and diagnose issues allowing for quicker and more organized response to security incidents, minimizing disruption to business operations. The use of new data will also help in allowing for data-driven decision-making, this will help in making informed decisions about the future of security strategies and where to invest time in maturing security practices at Ali Clinic.

Summative Evaluation Plan

The summative evaluation plan goes over several components. The evaluation assesses the overall success and effectiveness of the project and measures against initial goals and objectives. To meet compliance the solution aligns with HIPAA, HITRUST, ISO 27001, and NIST SP 800-53 standards. A comprehensive security assessment is conducted to validate the effectiveness of the implemented solution. A key performance indicator (KPI) analysis is conducted to evaluate KPIs such as reduction in vulnerabilities, incident response time, and system uptime. Stakeholder feedback is necessary so feedback is collected and analyzed from stakeholders to assess the project's impact and effectiveness. The plan of action and milestones are highlighted below.

- Week 1-8: Initial risk assessment by Endpoint Security and compliance verification by the legal and compliance department.
- Week 9-12: Review and analysis of KPIs.
- Week 13-20: Stakeholder feedback collection.
- Week 21-26: Final evaluation and report generation.

Control Deficiency Analysis

The control deficiency analysis was not required in the project solution because the solution provides a comprehensive and robust system, addressing all known vulnerabilities and risks detected in the risk assessment. The project uses tools like Azure Boards Analytics and Microsoft Defender for Cloud to provide a more holistic view of the system's security posture and performance. With the use of continuous monitoring tools (Uptime Kuma and Microsoft Defender for Cloud), any control deficiencies will be identified and addressed in real-time. This will allow all relevant stakeholders to be aware of any threats the clinic is facing and potential avenues for mitigation.

Post-Implementation Risks

There are various post-implementation risks each with specific likelihoods, potential impacts, and mitigation strategies. One of the notable risks is the moderate likelihood of challenges in identifying all vulnerabilities, which could have a high impact due to the oversight of crucial security weaknesses such as employees not having a matured knowledgebase to identify vulnerabilities. However, this risk is mitigated through continuous security assessments and prioritizing risks. Another risk considered is the potential delay in infrastructure upgrades, which, while low in likelihood, could moderately impact subsequent phases and project timelines. Achieving compliance with multiple standards poses a moderate likelihood of hurdles with high potential impact, including severe consequences and legal ramifications. This is addressed through regular compliance reviews and strict adherence to standards done by the legal and compliance department using tools like Microsoft Defender for Cloud to monitor the clinic's compliance. The creation, designing, and implementation of a robust business continuity plan is another risk, with moderate likelihood and impact, potentially affecting the clinic's response to incidents. Mitigation involves comprehensive planning and regular testing. Training and knowledge transfer issues with a low likelihood and impact, are significant for staff effectiveness and are countered with training and support given by Endpoint Security, IT, and Executive Management. The challenges in setting up continuous systems are anticipated to have a moderate likelihood and impact, related to the expertise required for interpreting log output. This is addressed by engaging skilled IT professionals and providing ongoing training. Lastly, potential delays in documentation of the project closure are considered low in both likelihood and impact but are crucial for insights and future improvements, addressed through timely documentation and review processes using tools like Azure Boards Analytics for tracking project progress and documentation.

Project Stakeholders

The project's stakeholder needs are met in the solution as the Endpoint Security team is responsible for guiding and supervising the implementation. The needs are that the project provides

an effective and secure technology solution that aligns with the clinic's cybersecurity requirements. This is met through the enhanced tools systems like Microsoft Defender for Cloud which streamlines their workflow and improves their ability to safeguard the clinic's IT infrastructure. The Executive Management role is ensuring resources are available during the solution implementation and aligning the solution with the clinic's mission and goals. The needs are that the security solution supports the clinic's operational objectives without compromising budgetary constraints or strategic direction. Their needs are met through the implementation of a robust cybersecurity framework that assures that the clinic is well-protected against cyber threats, aligning with their goal of maintaining a safe and efficient healthcare environment. The Legal and Compliance team's role is to ensure the clinic remains compliant with legal standards throughout the implementation. Their needs are that the solution adheres to healthcare industry regulations such as HIPAA and HITRUST along with using comprehensive frameworks such as NIST SP 800-53 and ISO 27001. Their needs are met through the automated compliance features of using Microsoft Defender for Cloud which eases the process of ensuring ongoing adherence to legal and regulatory requirements. Finally, the patient's role as the end beneficiary of the secured environment, as their data is being protected. Their needs are assurance that their personal and health data is protected, maintaining their trust in the clinic, and enhancing the clinic's reputation. Their needs are met by the strengthened security measures which increase patient's confidence in how their data is handled, thereby boosting their trust in the clinic.

Post-implementation Maintenance Plan

The post-implementation maintenance plan for the security solution at Ali Clinic focuses on continuous monitoring and evaluation to ensure effectiveness and sustainability. The use of continuous monitoring systems is used at Ali Clinic to detect and respond to emerging threats effectively. This is a critical component of the maintenance plan as it ensures ongoing vigilance against potential security risks. The tools like Uptime Kuma, an open-source monitoring system, are

utilized for on-premise systems and Microsoft Defender. These tools provide real-time monitoring capabilities allowing the clinic to quickly detect and address operational or security issues as they arise. For the cloud, Microsoft Defender for Cloud is used like it’s used on-premise. This tool ensures that the systems hosted in the cloud maintain a robust security posture and meet requirements set by HIPAA, HITRUST, NIST SP 800-53, and ISO 27001. With continuous compliance monitoring, Ali Clinic will know the status of each of its systems and whether they are compliant with industry standards. These tools collectively ensure that both on-premise and cloud-based systems are continuously monitored for security threats, performance issues, and compliance with relevant standards.

Cybersecurity Domains

The security solution at Ali Clinic addresses the cybersecurity domain Cyber Risk Management and Oversight by focusing on compliance (Microsoft Defender for Cloud), risk assessments (Endpoint Security), and aligning security strategies with the clinic's goal of securing patient data and providing better care. This includes organization charts, cybersecurity-related policies and procedures, strategic plans, personnel qualifications, risk assessment, data loss prevention analysis, IT audit schedule and reports, and cybersecurity training policies and materials. Next, Cybersecurity Controls this domain is addressed through continuous monitoring and infrastructure upgrades (Networking, Azure, Red Hat Linux) to meet security standards. This involves physical access controls, baseline security configuration standards, patch management policies and procedures, penetration test results and reports, vulnerability assessment, and continuous monitor strategies. Finally, Cyber Resilience, the project establishes a robust business continuity plan and enhances the clinic’s ability to respond to security incidents. This covers cybersecurity event logs and reports, business or corporate continuity plans, resilience testing results and reports, cyber incident response plans, and crisis management plans.

References

Office for Civil Rights (OCR). (2022, October 19). Summary of the HIPAA Privacy Rule. HHS.gov. *https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html*

Kaspersky. (2023, July 6). *What is WannaCry ransomware?*. www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

NIST SP 800 53. (n.d.). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Nessus: A security vulnerability scanning tool. Nessus. (n.d.). https://www.cs.cmu.edu/~dwendlan/personal/nessus.html

Welcome to InsightVM. Welcome to InsightVM | InsightVM Documentation. (n.d.). https://docs.rapid7.com/insightvm

Cisco 1000 Series Integrated Services Routers Data Sheet. Cisco. (2023, August 3). *https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/datasheet-c78-739512.html*

Cisco Catalyst 9300 Series Switches Data Sheet. Cisco. (2023, December 5). *https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html*

Louislam. (n.d.). *A fancy self-hosted monitoring tool*. GitHub. https://github.com/louislam/uptime-kuma

Microsoft. (n.d.). *What is Microsoft Defender for Cloud?*. Microsoft Defender for Cloud | Microsoft Learn. https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

Chcomley. (n.d.). *What is Azure DevOps?*. Azure DevOps | Microsoft Learn. https://learn.microsoft.com/en-us/azure/devops/user-guide/what-is-azure-devops?view=azure-devops

Chcomley. (n.d.). *Work tracking metadata reference for analytics - Azure DevOps*. Work tracking metadata reference for Analytics - Azure DevOps | Microsoft Learn. https://learn.microsoft.com/en-us/azure/devops/report/analytics/entity-reference-boards?view=azure-devops

CISSP: Business Continuity Planning and exercises. Infosec. (n.d.).

https://resources.infosecinstitute.com/certifications/cissp/cissp-business-continuity-planning-exercises

Stevevi. (n.d.). *ISO/IEC 27001 - azure compliance*. ISO/IEC 27001 - Azure Compliance | Microsoft Learn.

https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-iso-27001

Information security policy template. FRSecure. (2023, June 21).
https://frsecure.com/information-security-policy-template/