High Desert Engineering Infrastructure Upgrade

Norman Shatto

Western Governors University

Abstract

High Desert Engineering (HDE) is experiencing performance problems with its current IT infrastructure. They have out-of-date employee workstations, unmanaged network devices, and do not use Multi-Factor Authentication (MFA). As a result, the company cannot provide reliable and secure support for its day-to-day operations due to a lack of modernized hardware, network security controls, and centrally managed authentication. A comprehensive overhaul of High Desert Engineering's IT infrastructure is planned to address these issues. This overhaul will replace older legacy computers with Dell desktops and monitors, installing managed network switches, next-generation firewalls, secure wireless access points, and implementing a centralized identity management system with MFA for all employees. The implementation plan will utilize phased resource allocation, scheduled hardware deployments, and structured change management to minimize disruptions to the company's normal operation. Stakeholders for the proposed project include senior management, IT personnel, departmental managers, and end-users. Senior management is seeking enhanced security, improved regulatory compliance, and reduced operational costs. The IT department wants a stable, manageable infrastructure that results in a lower volume of incident responses. Departmental managers require access to business systems that are consistently available and functional, enabling them to meet their project deadlines. Employees desire access to desktop computers that are secure, fast, and easy to navigate. The proposed implementation plan consists of a current-state assessment, deployment of new hardware and networks, enforcement of MFA, testing of new systems, training of employees, and a post-implementation assessment of the performance and security of the new systems.

Keywords: *High Desert Engineering (HDE), Multi-Factor Authentication (MFA), workstations, stakeholders*

Table of Contents

Proposal To Implement a Complete Infrastructure Overhaul at High Desert Engineering

High Desert Engineering (HDE) is a mid-sized local business based in Albuquerque, New Mexico, specializing in planning and designing commercial engineering projects. The existing IT environment at HDE has led to IT business issues, including increased cybersecurity risks, decreased system performance, frequent network outages, increased exposure to ransomware, credential theft, and data breaches. Additionally, the IT department lacks visibility into management, network traffic, and centralized identity management. HDE lacks the necessary ability to monitor and control user access. According to the National Institute of Standards and Technology (NIST), organizations that lack modern endpoint protection, network segmentation, and strong authentication mechanisms face a significantly higher risk of cyber intrusion and operational downtime (NIST, 2023). Given the continued growth of HDE and its increasing need to store sensitive design and client information, the current infrastructure no longer provides sufficient protection, scalability, and reliability to support its business operations.

A comprehensive network infrastructure, hardware, and identity security modernization solution will be implemented to enhance cybersecurity, improve operational reliability, and boost employee productivity. The solution includes the replacement of all outdated desktop computers with standardized, encrypted, business-class workstations from Dell that hosts a Windows operating system, deployment of managed Cisco enterprise network switches, installation of next-generation firewalls with intrusion prevention capabilities, implementation of secure wireless access points with segmented Virtual Local Area Networks (VLANs), and implementation of centralized identity and access management with mandatory Multi-Factor Authentication (MFA) for all employees. These solutions align with NIST zero-trust principles and industry best practices for endpoint and access security (NIST, 2023). The project also incorporates centralized logging, network monitoring, and configuration management to provide the IT department with improved visibility and administrative control over the organization's technology environment.

HDE will continue to manage multiple ongoing IT initiatives, including routine system maintenance, application support, and software engineering upgrades, during the upgrade. Concerns related to resource allocation, scheduling, risk management, and workload balancing are critical to successful implementation. Utilizing the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK) framework, the project will be implemented through structured phases, including initiation, planning, execution, monitoring and controlling, and closing (PMI, 2021). Limited staffing will be addressed through a phased implementation, cross-training of support personnel, and the selective use of vendors for specialized tasks, such as firewall configuration and network segmentation. Controls will be established to enforce budget controls through milestone-based procurement and vendor contract management. Risks such as temporary system downtime, employee resistance to MFA, and deployment delays will be mitigated through continual communication, pilot testing, and after-hours installation windows.

Stakeholders of the project include the executive leadership team, the IT department, department managers, and end-users within the organization. The executive leadership team requires demonstrable improvements in cybersecurity posture, regulatory compliance, financial risk reduction, and long-term scalability of the IT environment. The IT department requires standardized hardware, centralized management tools, improved monitoring capabilities, and reduced exposure to security incidents that increase support workloads. Department managers require stable, high-performance network access and reliable workstation systems to ensure uninterrupted delivery of engineering services to clients. Organizational end-users require secure, fast, and user-friendly access to business applications without disrupting their daily workflow excessively. The stakeholder needs assessment will ensure alignment between the project objectives and organizational priorities while establishing a governance structure for oversight, communication, and accountability.

The implementation proposal begins with a comprehensive assessment of the current state, including network topology, endpoint hardware, authentication mechanisms, and security controls. This assessment will identify performance bottlenecks, security gaps, and hardware lifecycle risks. The procurement phase will follow, where standardized workstation models, network equipment, and security appliances will be identified based on performance requirements, cost, vendor reliability, and warranty support. The deployment phase will utilize a staged rollout strategy, first upgrading the core network components, then replacing the desktop workstations, and finally implementing identity and enforcing MFA. Testing will occur at each phase to verify system performance, network segmentation, failover behavior, and authentication reliability. An employee training program will be developed to accompany the implementation of MFA, aiming to reduce employee resistance. The final phase will include a post-implementation evaluation using performance metrics, security incident reduction rates, help-desk ticket volume trends, and system uptime measurements.

This project represents the integration of several key IT management principles, including hardware lifecycle management, secure network architecture, identity and access management, risk mitigation, and project governance, into one enterprise-level modernization project. The successful implementation of this solution will significantly reduce HDE's exposure to cyber threats, enhance network reliability and employee productivity, and establish a scalable IT platform that can support future business growth and evolving regulatory requirements.

Needs Analysis

High Desert Engineering has experienced significant problems with both operational and cybersecurity issues. These issues primarily come from outdated workstation hardware, an unorganized and unmanaged network infrastructure, and poor control over access to company resources due to weak authentication controls. The consequences of these issues have resulted in an insecure and inefficient IT environment that impacts employee productivity, the safety of employees' sensitive data, and the overall reliability of HDE's operations. The most critical issue impacting HDE's employees is the inability to safely and productively perform their job duties, as the organization cannot provide reliable and efficient support for daily business operations due to a lack of modern endpoint protection solutions, network segmentation solutions, and centralized identity and access management solutions. The hardware life cycles of the employee computers have exceeded their intended lifespan, which results in employee computers often not functioning properly and frequently crashing when attempting to run applications required to perform their jobs. Additionally, the company uses unmanaged switches and operates on a flat network architecture, which limits visibility into traffic passing through the network and fails to contain threats that may originate from inside the network. Furthermore, HDE does not utilize MFA to protect against the potential loss of an employee's credentials due to phishing attempts or other forms of unauthorized network access. According to the National Institute of Standards and Technology, companies that fail to implement strong access controls and network protections are at a significantly greater risk of experiencing ransomware attacks, data breaches, and prolonged periods during which they will be unable to maintain normal business operations

(NIST, 2023). The combination of years of deferred hardware upgrades and the failure to establish formal IT governance and security policies is the two main reasons why HDE faces such high levels of risk associated with its current infrastructure vulnerabilities.

The effects of the current problem are evident across all stakeholder groups at HDE. Executive leadership is exposed to several types of risk, including financial, legal, and reputational risks. If they were to suffer a significant cyberattack or experience an extended period of time during which the company was unable to conduct business due to technical difficulties, the company would likely face contractual penalties, loss of client trust, regulatory scrutiny, and damage to its reputation in the marketplace. Furthermore, executive leadership lacks visibility into the company's current cybersecurity posture and, therefore, cannot make informed strategic technology decisions.

The IT department is significantly impacted by the current problem in many ways. The IT staff is subjected to increased workload and operational stress as they respond to frequent hardware failures, authentication issues, and network instability. The IT staff lacks centralized management tools and network segmentation controls, and troubleshooting efforts are typically reactive in nature, resulting in longer response times and an increased likelihood of unresolved vulnerabilities. The department managers are negatively impacted by unreliable systems that cause disruptions in their workflows, delays in project completion, and inefficiencies within their teams. Engineering operations rely heavily on reliable network connectivity and high-performance computing, so system downtime results in lost revenue generation and decreased client satisfaction. Other employees experience daily productivity losses due to slow computers, inconsistent network access, and security vulnerabilities that expose them to potential cyberattacks. Additionally, frustration with system performance contributes to employees' reluctance to follow IT policies and best practices related to security.

The proposed solution aligns with existing industry standards, cybersecurity frameworks, and regulatory requirements. Implementing managed network infrastructure, endpoint encryption, and centralized authentication addresses each of the five core functions of the NIST Cybersecurity Framework: identify, protect, detect, respond, and recover (NIST, 2023). Implementing VLANs and next-generation firewalls to segment the network aligns with the concept of zero-trust security, which eliminates the implicit trust within internal networks. Implementing MFA for all employee access to the network aligns with the Center for Internet Security (CIS) Critical Security Controls, specifically Control 5 for Account Management and Control 6 for Access Control Management (CIS, n.d.). This approach greatly reduces the risk of unauthorized access and lateral movement within the network. The use of encrypted workstations, access controls, and centralized logging to meet regulatory compliance aligns with the Federal Trade Commission's (FTC) Safeguards Rule for protecting sensitive customer information (FTC, 2024) and state-level data protection and breach notification laws. In terms of project governance, the implementation approach follows structured practices outlined in the Project Management Institute's PMBOK Guide, which includes effective risk management, stakeholder communication, and controlled resource allocation (PMI, 2021). Overall, these standards and regulatory alignments provide assurance that the proposed solution is not only operationally necessary but also meets the legal, ethical, and professional expectations of IT management.

Cost Analysis

Itemized Costs

Hardware:

- The Dell Pro Slim desktops are budgeted at $1,089 each (Dell Pro Slim Desktop Slim Business Computer, Dell USA, n.d.). This model offers sufficient performance in terms of RAM, SSD, security features, and manageability to support the engineers' workloads. This business-grade desktop will reduce failures, improve longevity, and lower the total cost of ownership compared to their current legacy desktops. The total cost for 60 Dell desktops is $65,340.

Monitors:

- The Dell Pro 24-inch monitors are budgeted at $189.99 each (Dell Pro 24 Inch Plus Monitor P2425H FHD IPS Display, Dell USA, n.d.). Each workstation will have two monitors, totaling 120 monitors. Using dual monitors can enhance productivity, especially while multitasking. The total cost for 120 monitors is $22,798.

Network Switch:

- The Netgear 24-port managed switch is priced at $154.59 each (Netgear JGS524NA ProSafe 24-Port Gigabit Switch, n.d.). Based on the number of desktops, printers, and other hardware, we will require a total of three switches. Using managed switches ensures network segmentation, traffic control, and improves network reliability. The total cost for three Netgear switches is $463.77.

Wireless Access Points:

- The Cisco wireless access points are budgeted at $154.99 each (Cisco Business 150AX Wi-Fi 6 2x2 Access Point, Microcenter, n.d.). Based on the building's square footage, it will require six access points. These access points will provide better wireless coverage throughout the building and more stable connections. The total cost based on 6 units is $929.94.

Perimeter Security:

- The Fortinet 80F firewall appliance is budgeted at $1,138.70, and HDE only needs one unit (Fortinet FortiGate 80F Series, AVFirewalls.com, n.d.). Implementing this firewall is crucial for reducing the risk of external threats and enforcing a secure access policy.

Software/Licensing:

- Microsoft 365 Business Premium was chosen as the software for HDE and is budgeted at $22 per unit per month (Compare Microsoft 365 Plans, Microsoft 365, n.d.). This will provide productivity tools and allow the IT department to manage devices and integrate MFA. The total for the yearly subscription for 60 employees is $15,840.

Labor:

- The internal IT department and external vendors will collaborate on this project, with an estimated completion time of approximately 200 hours. According to the U.S. Bureau of Labor Statistics, the average hourly wage for a network and computer system administrator is $41 (U.S. Bureau of Labor Statistics, 2025). The total estimated labor cost for this project is $8,200.

Category	Item	Quantity	Unit Cost	Total Cost
Hardware	Dell Pro Slim Desktop	60	$1,089	$65,340
Monitors	Dell Pro 24” Monitor	120	$189.99	$22,798
Network Switch	Netgear 24 port switch	3	$154.59	$463.77
Wireless Access Points	Cisco WAPS	6	$154.99	$929.94

Perimeter Security	Fortinet 80F Firewall Appliance	1	$1,138.70	$1,138.70
Software/Licensing	Microsoft 365 Business Premium	60 x 12 months	$22	$15,840
Labor	Internal IT labor	200 hours	Average $41/hour	$8,200
Total				$114,710.41

Justification for Costs

High Desert Engineering is facing multiple operational and cybersecurity concerns due to outdated workstation hardware, unmanaged network infrastructure, and weak authentication controls. Due to these areas of vulnerability, HDE has created an unstable and high-risk IT environment that creates barriers to staff productivity, staff data security, and reliable operation. The main concern with HDE’s inability to securely and efficiently support daily business operations is the lack of modern endpoint protection, network segmentation, and centralized identity and access management. Additionally, employee computers have exceeded their recommended life cycle, resulting in poor system performance, frequent crashes, and the inability to run new engineering applications. Furthermore, HDE utilizes unmanaged switches and operates under a flat network architecture, which does not enable monitoring of internal traffic and lacks internal threat detection capabilities. The lack of MFA creates vulnerabilities for employee credentials to be stolen, employees to be victims of phishing attacks, and unauthorized access to the network. According to NIST, organizations lacking robust access controls and network protection are exposed to significantly higher levels of risk from ransomware attacks, data breaches, and prolonged system outages (NIST, 2023). These risks are heightened due to years of deferring capital expenditures and a lack of formal IT governance and security policies, which contribute to the underlying vulnerabilities in the current state of the infrastructure.

This problem affects all stakeholder groups within HDE, including executive leadership, who are exposed to significant financial, legal, and reputation risks associated with a major cyber event or extended outage. Such events can include contractual penalties, loss of client confidence, regulatory review, and possible long-term damage to HDE's competitive position in the marketplace. Without having visibility into the organization's overall cybersecurity posture, executive leaders also limit their ability to make strategic technology decisions. IT department personnel experience increased workload and operational stress as they spend time responding to hardware failures, authentication problems, and network instabilities. Without the use of centralized management tools and segmented network controls, troubleshooting becomes reactionary rather than proactive, which increases response times and the probability of unresolved vulnerabilities. Departmental managers experience decreased productivity and efficiency due to unreliable computer systems, which cause disruptions in workflows, delays in project completion, and inefficient teamwork. System downtime impacts revenue generation and client satisfaction, as engineering operations rely on stable network connections and high-performance computing. End-user employees experience lost productivity daily due to slow computers, inconsistent network access, and security vulnerabilities that expose them to the potential of being compromised by cyberattacks.

The proposed solution complies with well-established cybersecurity frameworks and industry standards. The largest share of the budget is allocated to replacing employee workstations, which is justifiable given the importance of these workstations to engineering operations. Based on current prices for business-class Dell Pro desktops, equipped with enterprise-grade components, running Windows 11 Pro, featuring TPM security, and commercial warranty support (Dell Technologies, 2024), the cost per Dell Pro Slim Desktop is $1,089.00.

Although this is higher than entry-level consumer desktops, the cost is justifiable due to the need for long-term reliability and compatibility with engineering productivity software. With 60 workstations to be replaced, the total cost of the desktop replacements will be $65,340.00, which aligns with the costs for managing business-class desktops and supports a comprehensive desktop hardware refresh strategy.

In addition to replacing the desktops, the project also includes the purchase of 120 Dell Pro 24-inch Monitors at $189.99 per unit, totaling $22,798.00 (Dell Technologies, 2024). Dual-monitor configurations are widely accepted as a standard for improving productivity in professional and technical fields as they promote efficient multitasking, increase workflow efficiency, and reduce window switching during tasks such as design, documentation, and data analysis. The selected monitors meet Dell's commercial display requirements and are designed to offer long-term warranties and reliability.

The project will replace the current unmanaged network infrastructure with three Netgear 24-port Smart Managed Switches at $154.59 per switch, for a total of $463.77 (Netgear, 2024). Although the cost of these switches is lower than that of enterprise-level switches, they provide VLAN capabilities, quality-of-service controls, traffic monitoring, and secure remote management, all of which are unavailable in unmanaged switches. They will provide sufficient segmentation and performance to support the needs of a multi-department business operation.

The Cisco wireless access points were installed at a cost of $929.94. Each access point was priced at $154.99. Cisco wireless solutions are widely adopted in commercial settings because they offer a wide variety of secure authentication options and a single point of administration for all devices, while also functioning reliably even with a high number of connected devices. Therefore, these access points represent the entry-level price of a business-grade access point that has security features and performance far superior to those of home office-grade Wi-Fi routers. Their use in an engineering firm where network availability is critical to mission success is justified.

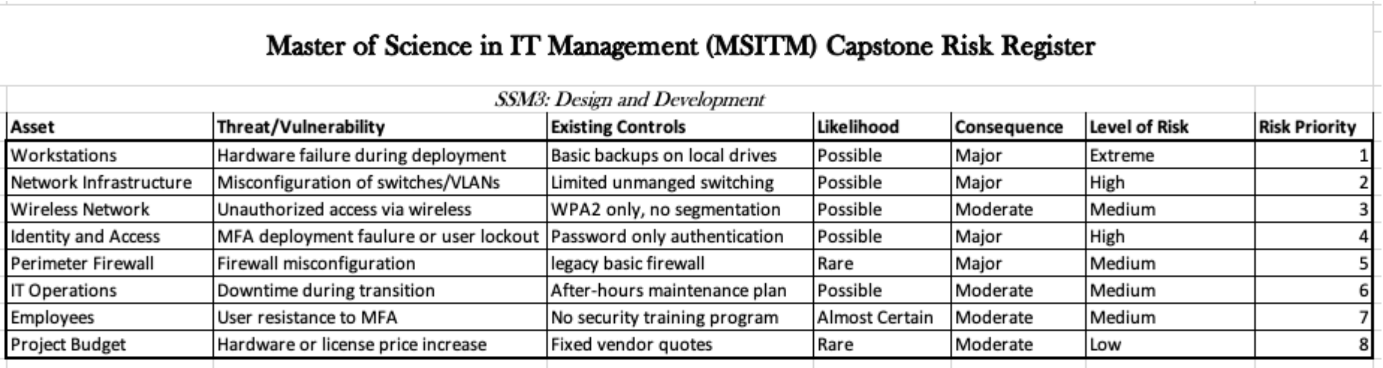
Firewall perimeter security will be accomplished with the installation of a single Fortinet FortiGate 80F Firewall Appliance costing $1,138.70, which includes enterprise threat protection capabilities. The FortiGate 80F will provide next-generation firewall services, which include intrusion prevention, deep packet inspection, malware filtering, and centralized logging. In comparison to standard routers and traditional firewalls, this solution significantly reduces exposure to external threats and can help meet regulatory requirements by enforcing current network security practices.

Security and identity software will be implemented using Microsoft 365 Business Premium for 60 users, at a monthly cost of $22 per user, resulting in an annual software license fee of $15,840. Microsoft 365 Business Premium includes Microsoft's standard productivity applications, as well as Azure Active Directory, multi-factor authentication, mobile device management through Microsoft Intune, conditional access, and endpoint protection. When comparing the cost of Microsoft 365 Business Premium to Microsoft 365 Business Standard at a cost of $12.50 per user per month plus third-party MFA, device management, and endpoint security products, Microsoft 365 Business Premium is less expensive and greatly simplifies the integration of all the required components for MFA and access control.

Internal IT labor and vendor labor costs are expected to total 200 hours at an average rate of $41 per hour, totaling $8,200. This average hourly rate is based on the national average wages for Network and Systems Administrators reported by the United States Bureau of Labor Statistics, which fall within the average of $41 per hour, depending on the level of experience

(U.S. Bureau of Labor Statistics, 2025). These 200 hours of internal IT labor and external vendor labor account for time spent conducting infrastructure assessments, system imaging, workstation deployment, switch/wireless configuration, firewall installation, MFA enforcement, testing, documentation, and employee training. The inclusion of labor costs in the project budget ensures that the total project cost accurately reflects the actual utilization of organizational resources.

Risk Assessment



Master of Science in IT Management (MSITM) Capstone Risk Register

SSM3: Design and Development

Asset	Threat/Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Workstations	Hardware failure during deployment	Basic backups on local drives	Possible	Major	Extreme	1
Network Infrastructure	Misconfiguration of switches/VLANs	Limited unmanged switching	Possible	Major	High	2
Wireless Network	Unauthorized access via wireless	WPA2 only, no segmentation	Possible	Moderate	Medium	3
Identity and Access	MFA deployment faulure or user lockout	Password only authentication	Possible	Major	High	4
Perimeter Firewall	Firewall misconfiguration	legacy basic firewall	Rare	Major	Medium	5
IT Operations	Downtime during transition	After-hours maintenance plan	Possible	Moderate	Medium	6
Employees	User resistance to MFA	No security training program	Almost Certain	Moderate	Medium	7
Project Budget	Hardware or license price increase	Fixed vendor quotes	Rare	Moderate	Low	8

Quantitative and Qualitative Risks

The proposed network infrastructure, hardware, and MFA present multiple measurable quantitative risks, including cost, downtime, and potential security breaches. The project's hardware deployment failures will result in a direct dollar amount at risk due to hardware failure. If the Dell Pro Slim workstation fails, it can result in the need for replacement units costing over $65,000, as well as a loss of productivity. Quantifiable risks include network misconfigurations resulting from changes made during the cutover of switches and firewalls, which can lead to a single day of total downtime for a sixty-person engineering firm, resulting in thousands of dollars of lost billable time. Risks to cybersecurity, while not always quantifiable, present the greatest potential for high-quantitative exposure. A successful external breach resulting from firewall misconfiguration or poor wireless security can easily incur thousands of dollars in expenses for remediation, litigation, fines from government agencies, and damage to reputation. As defined in the PMBOK Guide, all quantitative risks must be analyzed using established risk assessment techniques to evaluate the risk in terms of both its probable financial impact and probable disruption to the project schedule to determine the overall expected monetary value of potential loss (PMI, 2021).

All qualitative risks associated with the project also have a significant impact, but affect the behaviors and actions of employees, the operational performance of the organization, and the cultural environment of the organization. A key qualitative risk is employee pushback against the adoption of MFA. Although MFA significantly enhances the organization’s security posture, it can initially be perceived by users as annoying, repetitive, and frustrating, causing delays in MFA adoption, which in turn increases the number of requests to the help desk. Any type of network outage during the project's deployment phase will present qualitative operational risks, such as decreased confidence in the IT Department among stakeholders or temporary disruptions to critical engineering processes. In addition to network outages, if the training provided to employees is insufficient, they may misuse systems, create weak passwords, or bypass security controls, thereby negating the benefits of the entire solution. Qualitative risks are assessed based upon their likelihood and degree of impact to the satisfaction of stakeholders, continued workflow, and the trust of the organization (PMI, 2021). Together, the quantitative and qualitative assessments provide a comprehensive picture of both the measured financial exposure and the intangible operational and behavioral challenges that must be addressed to successfully implement the project.

Cost-Benefit Analysis

An evaluation of the costs and benefits of measures taken to reduce project risk was conducted through a cost-benefit analysis for each of the identified project risks, determining whether the expenditures for these reductions would be economically justifiable in comparison to the probable economic loss associated with each identified project risk. The largest dollar amount of financial risk exposure is related to cyber threat risks, including firewall misconfigurations, unsecured wireless connections, and poor authentication processes. Hardware deployment risk also presents measurable financial exposure. For example, a hardware workstation failure could necessitate purchase or replacement costs, exceeding $65,000, and productivity loss due to system downtime could further increase these costs. In terms of the project's operational aspects, potential network outages during transition periods could have additional negative effects on billable time and the timely delivery of project results. The cost of implementing proactive controls, such as staged deployment, after-hours transition operations, vendor-supported hardware, and testing, is negligible compared to the potential adverse impacts on both the financial and operational performance of the business in the event of uncontrolled system failures. PMI defines successful investment in risk management as occurring when the cost of responding to identified threats is significantly less than the probable financial impact of those same threats (PMI, 2021). This cost-benefit analysis clearly indicates that the financial benefits of proactively managing project risks far exceed the costs of acting.

Mitigation of Risks

The risk management process for the project will include the identification of potential risks associated with the project's scope, including risks associated with the hardware, network, and MFA aspects of the project, and will address these risks through the application of the PMBOK Guide to mitigate the likelihood and consequences of these identified risks. Risks associated with the technical components of the project, such as hardware failure, incorrectly configured firewalls, or network failures, will be mitigated through staged deployment, pre-implementation testing, standardized configurations, and rollback processes. Risks to cybersecurity will be addressed by implementing multiple layers of security controls, which include next-generation firewalls, encryption for wireless communications, network segmentation using VLANs, and mandatory MFA for all users accessing the network. Risks associated with operational issues, such as downtime, will be managed using after-hours transition operations, parallel system validation, and written recovery procedures. Risks associated with human factors, such as resistance to MFA and misuse of systems, will be managed through required security awareness training for employees, employee documentation of proper usage, pilot user group assessments, and responsive help desk support during the transition period. Additionally, financial risks associated with fluctuating prices and budget overruns will be managed through fixed-price agreements with vendors, competitive bidding, and the utilization of a contingency fund. The PMBOK also states that once an organization has established its approach to addressing risks during a project, it is essential to monitor those risks continuously and adjust them accordingly throughout the project lifecycle to ensure that the remaining risks are acceptable to the organization (PMI, 2021). Continuous monitoring, change control, and ongoing stakeholder communication will be maintained throughout the project's implementation to mitigate risks.

Justification of Approach

High Desert Engineering is experiencing declines in system performance, increased cyber exposure, and inefficient operations due to outdated computer hardware, unmanaged networks, and the absence of MFA. All these areas create a very unsafe business environment to cyber threats, system downtimes, and loss of productivity. A full upgrade of all employee computers, a managed network, enterprise wireless access, a next-generation firewall, and MFA via Microsoft 365 Business Premium directly addresses the root causes of the business problem and meets the current industry standards for security and performance.

Before selecting the recommended solution, several alternative solutions were evaluated. One potential solution that was considered was to retain the current computer equipment and add MFA and a new firewall. This would help improve overall safety from cyberattacks and provide stronger identity-based protection; however, this option did not address the declining system performance and hardware failures experienced by the legacy computers. Another option that was reviewed was moving all systems to a completely cloud-hosted virtual desktop environment. The cloud-hosted virtual desktop infrastructure offers several advantages, including centralized management and high levels of security, but it requires significantly higher ongoing expenses, increased network bandwidth, and additional training for employees unfamiliar with working within a virtual desktop environment. Overall, when compared to the two options above, the selected hybrid option of upgrading the computer equipment and improving the networks and identities represents the best combination of cost containment, operational performance, and reduction of cyber threat risks.

This project will utilize a hybrid predictive project management methodology that is aligned with the PMI's PMBOK framework. This type of methodology encompasses the formalized phases of initiation, planning, execution, monitoring and controlling, and closure, which are suitable for infrastructure projects with a known and defined scope, budget, and timeline (PMI, 2021). A completely agile methodology was considered, but it was not selected because of the need to acquire specific types of hardware, to develop and implement a specified network architecture, and to implement a new firewall, all of which must occur in a sequence and timeframe that can be controlled, which are all characteristics of a predictive model. Additionally, this project will incorporate some degree of agility using phased deployments, pilot tests, and iterative testing cycles during the execution phase. This is consistent with PMI's guidance regarding the importance of adapting methodologies to fit the complexities, risks, and needs of stakeholders involved in each project, rather than adhering to a singular methodology (PMI, 2021).

Initiation of the plan to implement the selected solution will begin with a detailed assessment of the current state and validation of requirements, followed by the acquisition of required hardware and software, and a staged deployment. The deployment will take place in stages, starting with the core infrastructure of network switches, firewalls, and wireless access points, prior to replacing workstations and implementing MFA. The cutover transition will occur outside of normal business hours to minimize the impact on operations, and rollback processes will be developed prior to the cutover. Training and change management will be incorporated into the execution phase to minimize user resistance, especially as users transition to MFA. Stakeholders and project team members will maintain continuous communication, monitor identified risks and changes to the project, and provide status updates relative to planned scope, budget, and performance through the monitoring and controlling phase.

Operational and strategic decision-making will be enhanced using Key Performance Indicators (KPIs) and data modeling. The operational KPIs to be utilized include system uptime, Mean Time To Repair (MTTR), the number of security incidents, the rate of failed authentication attempts, the volume of help desk tickets received, and average workstation performance metrics. The strategic KPIs to be utilized include reductions in cybersecurity risk, increases in the company's compliance posture, trends related to employee productivity, and technology Return on Investments (ROI). The data collected and modeled will compare pre-implementation and post-implementation performance data, with a specific focus on improvements in network reliability, frequency of security incidents, and employee productivity. This data-driven evaluation approach aligns with modern IT governance practices that promote decision-making informed by evidence and continuous improvement. Additionally, by establishing direct relationships between technical performance metrics and business results, including reduced downtime, faster project completion, and decreased security vulnerability, this project will contribute to its long-term operational resiliency and strategic growth objectives.

Project Resource Management Plan

Resource management for a successful implementation of the hardware, network, and MFA upgrade at HDE is key, as the IT Department will need to continue providing support for day-to-day operations and other current IT projects while completing the upgrades. This resource management plan has identified the human, technical, financial, and operational resources necessary to perform the design and implementation of this project, ensuring that all other ongoing IT obligations are fully supported while the project is being executed. The resource management plan utilizes PMI's guidance for managing the acquisition, development, and control of resources to achieve optimal performance and avoid conflicts (PMI, 2021).

Resources

The primary human resources required for this project are the IT Manager (Project Manager), Network Administrator, Systems Administrator, Help Desk Technicians, and employee end-users from various departments, who will test and train at the pilot level. The IT Manager is responsible for overseeing aspects of the project, including project governance, scheduling, risk management, coordinating with vendors, and communicating with stakeholders. The Network Administrator is responsible for configuring switches, deploying wireless access points, installing firewalls, segmenting VLANs, and testing network security. The Systems Administrator will configure workstation images, encrypt devices, configure Microsoft 365, administer identities, enforce MFA, and perform other systems administration functions. The Help Desk Technicians will be responsible for supporting workstation deployments, resolving user problems during cutover, and providing initial support to end-users throughout the transition period. End-users will test the usability of the new technology and report any issues they find before it is rolled out company-wide. To accommodate multiple projects simultaneously, IT staff workloads will be balanced through staggered schedules, temporary task reassignment, and the implementation of after-hours deployment windows, ensuring that normal IT services are not disrupted.

Technical resources required for the successful completion of the project include 60 Dell Pro Slim Desktop Computers, 120 Dell 24-inch Monitors, three Netgear 24-port managed switches, six Cisco wireless access points, one Fortinet FortiGate 80F firewall appliance, and

Microsoft 365 Business Premium licenses for each employee. Network configuration utilities, security monitoring dashboards, backup systems, and endpoint management platforms will also be utilized. The technical resources support the most fundamental components of the project, including workstation replacement, network segmentation, secure wireless implementation, and centralized authentication with MFA. During the configuration phase of the project, test environments and sandbox networks will be utilized to protect production systems while other IT services are being implemented simultaneously.

Financial resources include the approved project budget of $114,710.41, which includes all hardware, software licensing, and labor costs. All procurement activities will be conducted with an approved vendor, utilizing fixed-price quotes to minimize financial risks. A 10% contingency reserve will be held for any unplanned expenses resulting from unexpected changes in pricing, as well as for emergency hardware replacement. Tools for tracking financial activity will be implemented to monitor expenditures against baseline budgets and ensure that other concurrent projects within the department do not exceed the total amount of money allocated.

Facilities resources include server closets, network racks, and secure storage for undeployed hardware. Deployment activities will be scheduled to occur in the evenings or on weekends to minimize disruption to the engineering and administrative staff. Operational resources include internal documentation systems, change management platforms, asset management databases, and ticketing systems to track the progression of deployments and issue resolutions while other projects are simultaneously being worked on.

Since the IT Department must simultaneously maintain routine system maintenance, provide software support, and undertake other initiatives, resource allocation will be matrix-style, where employees will split their time between operational tasks and project tasks. There will be weekly resource allocation review sessions to identify scheduling conflicts, workload imbalances, and emerging constraints. Priority will be dynamically adjusted based on system criticality and business impact. PMBOK emphasizes the importance of continuously optimizing resources to prevent burnout, cost overruns, and performance degradation when managing multiple projects simultaneously (PMI, 2021). This structured approach to coordinate resources will allow the project to move forward efficiently without disrupting ongoing it services.

Justification of Resources

The human resources involved in this project will be responsible for the technical success of the project and for achieving the organization's performance goals. The IT Manager will serve as both the Project Manager and will be responsible for providing governance, scheduling, coordinating with vendors, overseeing the budget, and communicating with stakeholders. The IT Manager will support the organization in achieving its objectives of cost control, regulatory compliance, and operational stability by ensuring the project remains aligned with the organization’s strategic objectives and business priorities, as outlined by PMI (PMI, 2021). The Network Administrator is being utilized due to the complexity of implementing and configuring managed switches, firewall policies, wireless security, and VLAN segmentation. These tasks are crucial to achieving the organization's goals of enhanced uptime, secure data transfer, and reduced vulnerability to cybersecurity threats. The Systems Administrator is needed to image workstations, implement endpoint encryption, configure Microsoft 365, implement identity management, and enforce MFA for all users. The Systems Administrator will directly support the organization's objectives of creating standardized computing environments, increasing access controls, and decreasing system vulnerabilities. The Help Desk Technicians are required to deploy hardware and software to end-users, troubleshoot user issues during cutovers, and decrease operational disruptions to meet the organization's objectives of increased productivity and employee satisfaction. Pilot testing of employee end-users will enable the organization to assess usability and system performance before full deployment, thereby supporting business continuity and adoption.

The justification for hardware resources is the basis of the physical modernization objectives of this project. Replacing legacy workstations with business-class Dell Pro Desktops and dual monitors will directly support the organization's performance, reliability, and productivity objectives by allowing employees to utilize current engineering and business applications on equipment that does not experience performance degradation. Standardizing the hardware will enhance the organization's ability to manage the equipment's lifecycle, reduce maintenance variability, and lower the total cost of ownership for long-term support, thereby supporting the organization's financial performance and operational efficiency. The justification for utilizing the managed Netgear switches is that they will allow the organization to segment traffic, implement quality of service controls, and centrally manage traffic. These functionalities are mission-critical for protecting sensitive engineering data, facilitating secure intra-departmental communications, and minimizing the organization's risk of lateral movement within the network. The justification for the Cisco wireless access points is that they will provide secure, high-speed wireless connectivity across the organization. Reliable wireless access will facilitate workforce mobility, collaboration, and operational flexibility, all of which are important to the organization's competitiveness in delivering engineering services. The justification for the Fortinet FortiGate 80F Firewalls is that they are the organization's primary perimeter defense system. They provide intrusion detection and prevention, threat intelligence, traffic filtering, and centralized logging to support the organization's objectives of reducing cybersecurity risks and improving regulatory compliance.

The justification for software and licensing resources is that they provide the necessary functionality for enforcing security, managing identity, and enhancing productivity across the entire enterprise. Microsoft 365 Business Premium licenses are required to support core business communications as well as to provide centralized identity, device management, endpoint protection, and mandatory MFA. This unified platform will support the organization's multiple objectives of secure access control, regulatory compliance, collaboration efficiency, and data availability. The utilization of MFA will directly support the organization's objective of reducing credential-based attacks and protecting intellectual property and client data.

The justification for the financial resources, including the approved project budget and contingency reserve, is to ensure predictable execution and mitigate risk. The fixed-price vendor contracts will provide the organization with protection against market price volatility and support budgetary stability, thereby aligning with the organization's financial governance objectives. The contingency reserve will enable the organization to respond quickly to unforeseen procurement or technical issues without jeopardizing the project or other IT operations.

The justification for facilities and operational resources is to ensure the secure and efficient deployment of hardware and software resources, while maintaining business continuity. Server closets, secure storage areas, staging rooms for workstation imaging, and network racks will provide the organization with a controlled and secure environment to handle the physical aspects of the hardware assets. The organization can minimize the risk of theft, damage, deployment errors, and configuration inconsistencies by utilizing these resources effectively. The justification for utilizing change management systems, asset tracking tools, and ticketing platforms is to ensure that deployment activities are documented, auditable, and compliant with the organization's operational governance. The utilization of these resources will directly support the organization's performance objectives of accountability, audit readiness, and service quality.

The justification for allocating the organization's resources across multiple concurrent projects is the use of a matrix resource management structure. The organization will balance the operational support of the existing IT infrastructure with the execution of strategic modernization initiatives by staggering project schedules, working late hours when necessary, and dynamically prioritizing task lists. The PMBOK states that effective resource optimization across concurrent projects is necessary to prevent burnout, schedule delays, and cost overruns and maintain organizational performance (PMI, 2021). This approach will ensure that the project enhances the organization's overall performance.

Resource Allocation Plan

Manpower will be distributed among team members via a matrix-style model, where they spend a portion of their time providing operational IT support and the remainder working on projects. The IT Manager will act as both the Project Manager and allocate approximately 20% of their time per week to project oversight, governance, vendor coordination, and communication with stakeholders. The IT Manager's involvement in day-to-day operational tasks does not diminish because they are also involved in the overall project direction. The Network Administrator will work full-time during the network infrastructure phase, concentrating on installing switches, configuring firewalls, deploying wireless networks, and segmenting VLANs. It is expected that this full-time allocation will minimize the possibility of incorrect configuration or downtime. The Systems Administrator will work full-time during the workstation imaging, Microsoft 365 configuration, and MFA enforcement phase to ensure uniformity in workstation configurations and encryption, as well as protection of end-user identities. Help Desk Technicians will provide workstation delivery on an intermittent basis and will transition to full-time support personnel once the systems are fully operational, providing assistance in resolving any authentication, software, or hardware issues quickly. End-users will be engaged on a very minimal basis for pilot testing to test usability without interfering with normal business operations. The distribution of manpower will maintain a balance between technical focus and service continuity. Service continuity is one of the key principles outlined in the PMBOK Guide for managing resources across multiple projects (PMI, 2021).

The hardware resources will be allocated using a phased deployment plan to limit the number of business disruptions caused by simultaneous deployments of new hardware. First, core infrastructure hardware, including Netgear switches, Cisco wireless access points, and a Fortinet firewall, will be deployed to establish the foundation of a secure network. These devices will be deployed in sequence, tested, and validated before the production cutover to ensure that there is always a functioning network. Following the deployment of the core infrastructure hardware, workstation hardware will be deployed in waves by departments, rather than being rolled out company-wide simultaneously. This staged deployment plan ensures that at least 80-90% of users always have access to a functioning network, providing IT personnel with the opportunity to resolve problems with the early deployment wave before the entire network has been fully deployed. Legacy hardware will be decommissioned only after it has been successfully validated that the new systems are functioning properly.

Software resources, including Microsoft 365 Business Premium licenses, will be allocated to users by the organization's identity management system. Licenses will initially be allocated to pilot users during system testing and later will be allocated to all employees when MFA is rolled out. The phased provisioning of licenses allows IT to test authentication and access policies before enforcing them. Software resources will be allocated directly to user role definitions to limit the number of services and permissions provided to users. Identity management of software resources enables the tracking of licenses in real-time, enforces security policies, and manages costs while supporting the organization's collaborative and security objectives.

Funding for the project will be allocated on a stage-gated basis. Capital expenditures will be funded only after the prior stages of the project have been completed successfully. Funding will be initially allocated for the development of the infrastructure design and procurement, followed by funding for the subsequent deployment of the network, workstation acquisitions, and MFA implementations. The funding allocations are designed to promote cost discipline and reduce exposure to sunk cost risk due to changing project circumstances. A 10% contingency fund will be maintained by IT Leadership to address potential unplanned hardware failure or emergency licensing requirements. The funding allocation model supports the organization's financial governance objectives, including controlling costs, meeting audit requirements, and optimizing capital expenditures, while also providing sufficient funds to respond to emerging risks.

Due to other internal IT initiatives, project resources will be dynamically rebalanced each week, using forecasts of workload and trends in help desk tickets. Priority will be given to system criticality and business impact. In the event of operational emergencies, project resources may be temporarily reallocated to restore critical services, and the project schedule will be adjusted accordingly. Dynamic rebalancing of resources is consistent with PMBOK guidelines, which require continuous monitoring and optimization of resource utilization throughout the project life cycle to support sustained organizational performance (PMI, 2021).

Resource type	Role	Allocation method	Project phase
Manpower	IT Manager (Project Manager)	20% time weekly	All phases
Manpower	Network Administrator	Full time during infrastructure phase	Execution
Manpower	System Administrator	Full time during hardware and MFA	Execution
Manpower	Help Desk Technician (2)	Part time deployment and full time support	Execution and support
Manpower	End Users	Limited testing participation	Testing
Hardware	Dell Pro Desktops (60)	Assigned to employees in phased rollout	Deployment
Hardware	Netgear managed switch (3)	Installed subsequently to maintain uptime	Infrastructure
Hardware	Dell monitors (120)	Installed with desktops	Deployment
Hardware	Cisco WAPs (6)	Staggered deployment by building zones	Infrastructure
Hardware	Fortinet FortiGate 80F firewall	Integrated at network core	Infrastructure
Software	Microsoft 365 Business Premium (60)	Assigned through centralized identity system	All phases
Financial	$114,710.41 project budget	Released in stage-gated funding increments	All phases
Financial	10% contingency reserve	Held by IT committee	Risk response

Gaps and Impact on Other Projects

High Desert Engineering has significant shortcomings in its current IT environment, which adversely affect its productivity, safety, reliability, and strategic IT alignment. The largest issue is that HDE uses outdated workstation hardware that does not meet today's expectations for performance of modern engineering and commercial applications. These older systems are frequently causing system crashes, they are operating at slower than acceptable levels, and many of them do not operate with newer versions of software that have been developed since their introduction. This results in decreased employee productivity and increased demand on technical support. Project delivery timelines are negatively impacted because engineering teams rely on high-performance computing to complete design, modeling, and client deliverables. The proposed workstation upgrade will close this performance gap by providing consistent endpoint performance, decreasing the number of system failures, and increasing user productivity within each department.

Another significant gap in the organization's current network infrastructure and security architecture is the flat network structure, which utilizes unmanaged switches. The lack of visibility into network traffic and the inability to create an effective network segmentation create an opportunity for lateral movement if a cyber incident were to occur. This gap presents HDE with serious cybersecurity risks, including the spread of ransomware, unauthorized internal access, and a potential network-wide outage. The proposed deployment of managed switches, VLAN segmentation, enterprise wireless access points, and a next-generation firewall will fill this gap by implementing layers of security controls, providing proactive network monitoring, and segregating sensitive systems from general user network traffic. This security modernization will benefit HDE's organizational risk reduction goals and improve overall system reliability.

A third performance gap is related to identity and access management. Currently, HDE only utilizes password-based authentication without any form of multi-factor verification. Therefore, there is a high risk that credentials can be compromised due to phishing attacks or reused passwords. This gap represents a systemic vulnerability in HDE’s current cybersecurity position and compromises regulatory readiness and client confidence. The installation of a centralized identity management tool, combined with the enforcement of mandatory multi-factor authentication, will address this critical gap by implementing robust authentication controls across all systems. This will dramatically decrease the risk of unauthorized access to systems and subsequent data exfiltration. As a result, HDE will have greater control over the protection of its intellectual property and its regulatory posture regarding data protection and cybersecurity standards.

Operationally, these existing gaps also create additional IT support burdens, reactive maintenance models, and limited scalability to support the growth of IT capabilities as the company expands. Without standard hardware and centrally managed tools, troubleshooting issues takes longer, complicates patch deployment, and reduces the time available for IT personnel to work on strategic initiatives. Once these fundamental gaps are closed, the project will allow the IT Department to evolve from a reactive support model to a proactive service delivery model that better aligns with organizational performance and strategic objectives.

Additionally, the proposed project is expected to have a positive impact on other active IT projects currently underway. There may be some short-term, temporary resource conflict as network administrators and systems engineers split their time between performing operational support tasks and conducting project-related deployment activities. There may also be some temporary delay in lower-priority initiatives, such as minor software updates or non-critical system enhancements, during peak deployment times. To minimize the impact on other initiatives, project deployment activities will be scheduled to take place outside of regular business hours. Phased deployments will be implemented to minimize disruptions to dependent systems and users. Bi-weekly resource-planning meetings will be held to proactively manage workload conflicts between this project and concurrent initiatives.

In the long term, the successful completion of this project will positively enable and enhance the acceleration of both active and future IT projects. When an organization has standard hardware, securely segmented networks, and centrally managed identity credentials in place, future projects will be easier, faster, and less expensive to deploy. The organization will experience reduced technical limitations, reduced security risk when integrating new systems, and improved overall success rates for all IT projects. By addressing the existing performance and security gaps identified in this proposal, the proposed project will resolve current operational deficiencies while establishing a scalable and secure technology foundation that will support the organization's ability to successfully execute strategic IT initiatives.

Project Plan

Scope

This project will completely modernize the endpoint, network, and identity security infrastructure for High Desert Engineering. Activities in scope for this project include replacing 60 employee desktop computers with new systems, providing each employee with a dual-monitor configuration, deploying managed network switches, installing enterprise wireless access points, implementing a next-generation firewall, and enforcing MFA via Microsoft 365 Business Premium. This project also includes staff training, testing of all systems and processes, creation of all necessary documentation, and an evaluation of system performance after the project. All software application redevelopment, significant data center upgrades and restructuring, and third-party application migration not associated with authentication or network security are out of scope.

Assumptions

This project is based on several key assumptions. First, the funding and approval from the executive level will be available before purchasing begins. Second, vendor delivery schedules will be completed within the time frames provided by vendors. Third, all existing network cables and facility spaces can accommodate the new hardware installed as part of this project, without requiring any structural renovations. Fourth, IT personnel will be available to assist with the completion of this project while simultaneously supporting routine operations due to staggered staffing. Fifth, there will be no material changes to government regulations affecting technical specifications for this project during its duration.

Project Phases

Phase 1: Project initiation and planning (March 2, 2026 - March 20, 2026)

Phase one sets up the foundation for the project. By the end of this phase, an approved project charter will be in place, stakeholders will have been identified, technical requirements will have been validated, a risk baseline, a communications plan, and a governance structure will be established, and schedules will have been approved by all parties involved. It is at this point that strategic alignment occurs between the Executive Leadership, IT Management, and Departmental Stakeholders. At the conclusion of this phase, the approved charter and baseline schedule serve as formal authorization to begin procurement and implementation.

Phase 2: Design and Procurement (March 23, 2026 - April 17, 2026)

In Phase two, the detailed network, security, and workstation architecture will be completed. Additionally, all vendor selections will be made for desktops, switches, wireless access points, firewalls, and software licenses. All purchases will be completed through fixed-price vendor contracts to eliminate financial risk. The Phase will conclude once all hardware and licensing orders are placed and delivery schedules are confirmed.

Phase 3: Infrastructure Deployment (April 20, 2026 - May 22, 2026)

Phase three concentrates on deploying the fundamental network and security infrastructure. At this time, managed switches, wireless access points, VLAN segmentation, and the Fortinet firewall will be deployed and configured in staged cutovers. Prior to granting production access, the network's performance and security will be validated through controlled testing. Phase three must be completed before proceeding with endpoint deployments, ensuring that workstations can only connect to a secured and segmented network.

Phase 4: Workstation and MFA Deployment (May 26, 2026 - June 30, 2026)

Phase four will consist of workstation imaging, replacement of legacy computers by department, Microsoft 365 configuration, and enforcement of multi-factor authentication for all users. Pilot group testing will be used to introduce MFA to reduce adoption risk. Help desk staff will provide direct user support during the cutover process to minimize the impact on productivity. Phase four will be concluded when all employees are operating on new hardware with active MFA protection.

Phase 5: Testing, Training & Optimization (July 1, 2026 - July 17, 2026)

Comprehensive performance, security, and user acceptance testing will be conducted to ensure the solution's stability. Mandatory security and MFA training will be completed by employees. During phase five, system tuning, performance optimization, and remediation of any deployment defects will occur. Sign-off from executives and departments will verify that business and technical objectives have been achieved.

Phase 6: Project Closeout & Evaluation (July 20, 2026 - July 31, 2026)

The final phase will formally bring the project to a close. All technical documentation, asset inventories, and operational procedures will be completed. Additionally, KPIs such as system uptime, authentication success rates, helpdesk ticket volume, and security incidents will be compared to pre-implementation baselines. The lessons-learned report and executive performance summary will be delivered to leadership. Upon receipt of executive approval, the project will be officially closed.

Phase	Project Activities	Start Date	End Date	Key Milestones
Phase 1: Project initiation and planning	Project charter approval, stakeholder identification, requirements validation, risk baseline	March 2, 2026	March 20, 2026	Project charter approved, budget is authorized
Phase 2: Design and procurement	Final architecture design, vendor selection, hardware/software selection	March 23, 2026	April 17, 2026	All vendor contracts completed, hardware orders submitted
Phase 3: Infrastructure deployment	Switch installation, firewall deployment, WAP install,	April 20, 2026	May 22, 2026	Network core fully operational and security validated

	VLAN configuration			
Phase 4: Workstation and MFA deployment	Workstation imaging and rollout, Microsoft 365 configuration, MFA enforcement	May 26, 2026	June 30, 2026	All users migrated to the new system with MFA enabled
Phase 5: Testing, training, and optimization	Performance testing, security validation, employee training	July 1, 2026	July 17, 2026	User acceptance tasting completed
Phase 6: Project closeout and evaluation	Final documentation, KPI measured, lessons learned	July 20, 2026	July 31, 2026	Formal project closure and stakeholder approval

Timelines

Phase	Start Date	End Date	Milestone
Initiation and planning	March 2, 2026	March 20, 2026	Project charter approved
Design and procurement	March 23, 2026	April 17, 2026	All hardware ordered
Infrastructure deployment	April 20, 2026	May 22, 2026	Network core operational
Workstation and MFA deployment	May 26, 2026	June 30, 2026	100% of users are migrated
Testing and training	July 1, 2026	July 17, 2026	User acceptance training sign-off
Closeout and evaluation	July 20, 2026	July 31, 2026	Executive closure approval

A general overview of the entire project timeline from March 2, 2026, to July 31, 2026, will be discussed next. As stated above, there are three competing realities that need to be balanced to develop the overall project timeline: the technical complexity of the project, the need to continue operating as a normal business entity, and reasonable human and vendor constraints. Each phase has a length based on the technical complexity of each task, the number of people and vendors available to perform each task, and the dependency of each task on others that must be completed prior to its completion. These considerations are consistent with the PMBOK guidelines for developing a schedule and managing resource constraints (PMI, 2021).

The first phase of initiation and planning (March 2, 2026 - March 20, 2026) will be approximately 18 days long. An eighteen-day phase is sufficient for a project of this size and risk level. In Phase 1, the project charter will be finalized and formally accepted, stakeholders will be identified, and requirements will be validated. The risk register will be developed, and the first drafts of the communication plan and governance structure will be created. Phase 1 is not just paperwork. The items listed require meetings with company leaders, IT personnel, department managers, and many other individuals who will be responsible for their regular daily duties. An eighteen-day phase allows sufficient time to collect input from the various parties involved, revise the necessary documentation, and obtain formal approval of these documents prior to proceeding with the remaining phases of the project.

In phase 2, design and procurement (March 23 - April 17, 2026), will last approximately 24 days. Phase 2 was established to allow adequate time to create the final architectural designs for the network, security, and workstation standards. The architecture design process will involve multiple iterations and reviews, both internally and externally, to ensure compliance with budgetary requirements. Additionally, procurement activities will be conducted to obtain quotes from vendors, review the options provided, secure approval of the selected vendor, and process the purchase orders. Generally, vendors require a minimum of several business days to a couple of weeks to process and confirm orders, especially for larger quantities of equipment and licensing. Therefore, establishing a 24-day duration for this phase will provide a buffer for refining designs and realistic vendor lead times, without placing subsequent phases at risk.

The third phase, infrastructure deployment (April 20 - May 22, 2026), will last approximately 32 days. Phase 3 has been established to allow for a longer period of deployment for the core network changes, due to the increased technical complexity and risk. All changes to the core network will be implemented using managed switches, firewalls, VLANs, and wireless access points. Changes such as these must be implemented with great care to avoid impacting operations. Many of the changes to the core network will be implemented during evenings or weekends to minimize downtime. However, implementing changes during non-business hours naturally extends the calendar time required. Additionally, Phase 3 will involve the validation and testing of routing, segmentation, security policies, and failover behavior. Establishing a 32-day duration for this phase will provide sufficient time for staged cutovers, troubleshooting, and refining prior to introducing production traffic to the new infrastructure.

The fourth phase, workstation and MFA deployment (May 26 - June 30, 2026), will last approximately 35 days. A 35-day duration for this phase is considered reasonable, given the number of users and the need to continue operating the business as usual while replacing the end-user computers. The tasks included in this phase will be the imaging and deployment of 60 new desktops, the configuration of dual monitors, the migration of user data, the verification of application functionality, and the configuration of Microsoft 365 and MFA for all users. Implementing MFA will require piloting with a test group, followed by expanding in waves to avoid overwhelming the help desk. This approach to implementing MFA is consistent with industry best practices for endpoint and identity rollouts in operational environments.

In the fifth phase, testing, training, and optimization (July 1 - July 17, 2026), were established for a duration of approximately 17 days. At this stage of the project, all the major technical components of the system should be deployed. However, the system still needs to be tested. Phase 5 will include performance testing, security testing, and UAT. Also included in Phase 5 will be formal training sessions and reinforcement for MFA, security awareness, and any new workflows. Time will be allowed in Phase 5 to correct any defects discovered during UAT, refine configurations, and reduce help-desk tickets that normally occur after large implementations. A 16-day duration for Phase 5 is believed to be sufficient to bring the system into a stable state and obtain formal acceptance from the stakeholders.

For the last phase, project closure and evaluation (July 20 - July 31, 2026), it will have a duration of approximately 12 days. The primary focus of phase 6 will be to document the project's outcomes, update the asset inventory, measure the KPIs against the baseline values for the project, capture lessons learned, and document executive reporting and formal project closure. While phase 6 appears to be shorter than the previous phases, most of the technical work for the project will have been completed by the beginning of phase 6. Therefore, the primary focus of phase 6 will be on evaluation, governance, and knowledge transfer, which should be completed within the established timeframe if adequate documentation and tracking are maintained throughout the project, as suggested by the PMBOK Guide (PMI, 2021).

The minimal time differences between phases are planned for review purposes, to address any issues, and to adjust the project schedule. The use of these buffer periods will help manage uncertainty and minimize the risk that minor delays in one phase could significantly impact the project, resulting in costly overruns in subsequent phases. Overall, the project timeline has been designed to be aggressive enough to meet the project's objectives within a five-month timeframe, while allowing for staffing limitations, vendor constraints, risk management practices, and the continued operation of the business without disruption.

Dependencies

There are several key dependencies in this project. The procurement for the project will be completed upon receiving approval for the project's leadership funding. The workstation and MFA deployments will require that the network infrastructure be successfully installed and configured. There will also need to be a functioning authentication system so that employees can receive their required training. The testing and acceptance of all hardware must occur prior to closing out the final phase of the project, which is contingent upon validating KPI's and receiving executive sign-off.

Risk Factors

The success of the network infrastructure, hardware, and MFA upgrade at HDE depends on successfully managing various risk categories, including human, financial, and environmental risks. Each of these risk categories presents different types of risks to the project's scope, schedule, cost, and performance. Understanding and managing each type of risk will help ensure that the project remains stable and provides the desired results to the business.

Human risk categories represent the largest number of uncertainties for the project and have the greatest impact on the adoption, quality of execution, and continuity of service. The most significant human risk is user resistance to change when implementing MFA. Users may view MFA as a hurdle to their workflow and, therefore, may reduce their acceptance of MFA, disregard security policies, increase calls to the help desk, attempt to circumvent security controls, and so on. If user resistance to change is not effectively addressed through education and communications, the value of MFA may be diminished regardless of the quality of the technical implementation.

Another human risk category includes excessive workload and burnout of the IT department resources. The personnel performing the work for this project are the same individuals who manage day-to-day IT operations and support other concurrent projects. An overworked IT department is more likely to make mistakes, compromise the quality of its work, delay responses to emergencies, and experience burnout. Both risks are increased when a high volume of deployments occurs simultaneously.

The final two human risk categories include skill gaps and limited experience. Although IT personnel may have basic networking and systems administration knowledge, the technical complexity associated with advanced firewall configurations, VLAN segmentation, and enforcing enterprise-level MFA introduces new layers of complexity. A lack of experience in these areas can result in incorrect configurations, creating security vulnerabilities, or extending the time required to troubleshoot technical issues. Additionally, if a project has a dependency on a specific person, it creates a single point of failure, where the project is jeopardized if that person is unable to perform their duties due to illness, resignation, or other reasons.

Communication failures among the stakeholders involved in this project create a human-centered organizational risk. Poor communication among IT, departmental managers, and executive leaders can create unrealistic expectations, poorly aligned deployment timetables, and decreased confidence in the project. If employees are not provided with adequate information regarding deployment timelines, cutover expectations, and training requirements, there will likely be a significant increase in operational disruptions and employee dissatisfaction.

Financial risk categories directly impact the project's ability to stay within budget and generate a return on investment. There are three primary financial risk categories for this project, including hardware and software price volatility, unplanned labor costs, and cost overruns resulting from scope creep.

Hardware and software price volatility is a financial risk category since market conditions, supply chain disruptions, or vendor pricing adjustments can increase the cost of hardware and software products after a budget has been approved. Since this project will be purchasing large quantities of enterprise-class hardware and paying annually for cloud services, even small price increases can have a significant impact on the total project cost.

An unplanned labor expense is a second financial risk category for the project. Although internal labor hours are estimated to be 200 hours, unplanned technical difficulties, such as firewall misconfiguration, data migration issues, and workstation failures, can cause labor to exceed the planned labor hours. Labor may need to be contracted, or the professional services of vendors may be utilized to correct a technical issue, thereby increasing the project’s cost.

Cost overruns resulting from scope creep are a third financial risk category for the project. Once stakeholders see the benefits of the improvements, they may request additional hardware upgrades, software enhancements, or security features. While these additions may provide business value, they also introduce additional, unapproved expenses that can exceed the project's approved budget of the project unless formally managed through change management processes.

Downtime and the corresponding lost revenue are an indirect, yet substantial financial risk category. Regardless of how long the outage lasts, whether it is a few minutes or several days, there can be lost revenue due to unbilled engineering hours and delayed project completions. These opportunity costs do not appear as a direct line item on the project budget; however, they impact the company's overall financial performance and should be included in the overall financial risk assessment.

Environmental risk categories encompass both physical and organizational risks that are outside the direct control of the project and can have a significant impact on its outcome. Physical risks include the possibility of facility-based disruptions, such as power outages, HVAC failures in server closets, or physical access restrictions that prevent the installation of infrastructure. The hardware and network components installed in the rack environment require stable power and consistent temperature conditions. Any deviation from these conditions can prevent timely deployment, damage the equipment, or disrupt testing.

Depending on the location of the organization, natural disaster risks such as severe weather, flooding, or wildfires are also possible environmental risks. Natural disasters can delay shipment of materials, destroy recently shipped hardware, or delay on-site installation activities. If a natural disaster occurs during a critical deployment window, the entire project schedule may be severely impacted.

Another environmental risk category includes the possibility of supply chain disruptions. Depending on global economic conditions, there may be a shortage of semiconductor components, international shipping may be delayed, or vendors may have backlogged inventory. If any of these conditions occur, the delivery of the hardware can be delayed, which in turn may delay the dependent phases of the project, ultimately negatively affecting the overall project schedule.

Regulatory and external compliance changes are the last environmental risk category. Compliance changes can be made to data protection, cybersecurity, and privacy laws during the project's life cycle, and may necessitate the redeployment of security controls, authentication methods, or log collection mechanisms. Changes of this nature can add both cost and time to the project.

By understanding the risks at the beginning of the project, the organization can take proactive steps to mitigate and manage the risks through a variety of methods, including, but not limited to: change management, employee training, fixed-price contracts, establishing a reserve fund for contingency spending, staging the deployment of the solution, and monitoring risks throughout the project. A comprehensive understanding of the risks associated with this project will ensure that the proposed solution is completed on time, within budget, and provides sustained operational value.

Important Milestones

1. Project authorization and charter approval (March 2, 2026 - March 6, 2026):

The first step formally allows the project to move forward after the project charter, budget baseline, scope boundaries, and governance structure have been approved. The significance of this milestone is that without formal authorization, there can be no procurement, staffing allocations, or technical execution. This milestone formally establishes executive sponsorship, funding commitment, and accountability for outcomes.

2. Requirements and risk baseline finalized (March 9, 2026 - March 20, 2026):

This milestone represents the combination of all technical, security, and business requirements validation activities, including the project risk register. During this time, the project team validates functional requirements for workstation, network performance, wireless coverage, firewall security, and MFA enforcement with business stakeholders. Once this milestone has been met, the project team initiates design and procurement activities with an approved baseline, thereby minimizing the likelihood of rework and scope creep during the remainder of the project.

3. Vendor selection and procurement approval (March 23, 2026 - April 3, 2026):

The third milestone in this project signifies the completion of evaluating vendors, comparing prices, and approving contracts for all hardware and software components. In addition to evaluating vendors, this milestone also involves obtaining final quotes for desktops, monitors, switches, wireless access points, firewalls, and Microsoft 365 licenses. The approval of the quotes obtained during this window is essential for the project's financial governance, as it establishes pricing, delivery terms, and warranty conditions prior to releasing capital funds.

4. Hardware and licensing acquisition complete (April 6, 2026 - April 17, 2026):

The fourth milestone in this project confirms that all physical hardware and software licenses have been received, inventoried, and prepared for deployment. This milestone includes verifying the integrity of shipments, tracking serial numbers, and ensuring that licenses are assigned. Meeting this milestone prevents downstream implementation delays caused by material shortages or missing licenses. Additionally, meeting this milestone enables the technical team to begin configuring and imaging their computers prior to deployment.

5. Core network and security infrastructure live (April 20, 2026 - May 22, 2026):

The fifth milestone in this project indicates the successful deployment and validation of the underlying network and security environment. By this point, the managed switches, VLAN segmentation, wireless access points, and Fortinet firewall should be fully deployed, configured, and tested. Before migrating production traffic, security policies, traffic filtering, and network performance metrics must be thoroughly validated. As a result of the significance of this milestone, all subsequent phases in this project rely upon the stability and security of the core infrastructure.

6. Workstation and MFA deployment complete (May 26, 2026 - June 30, 2026):

The sixth milestone in this project marks the completion of migrating all 60 employees to new Dell Pro desktops, dual-monitor configurations, Microsoft 365 Business Premium accounts, and the implementation of mandatory MFA. This will involve deploying the new systems in waves, by department, with help desk support available during each cutover. Meeting this milestone will mark the operational transition to the new IT environment and represent the most significant changes experienced by end-users within the company.

7. User acceptance testing approved (July 1, 2026 - July 17, 2026):

The seventh milestone in this project verifies that all business users and department managers have formally accepted the new systems based on performance, usability, and security standards. During this phase, the project team completes full system testing, cybersecurity validation, and employee training. All defects found during UAT will be corrected prior to giving final acceptance. Meeting this milestone will ensure that the solution meets both the technical specifications and business requirements before the project is closed.

8. Executive project closure and final approval (July 20, 2026 - July 31, 2026):

The final milestone in this project marks the formal completion of the project. At this point, key performance indicators will be compared against pre-implementation baselines. Additionally, lessons learned will be documented, and all final documentation will be provided.

Executive management will then provide formal approval for project closure. After this milestone, the project will transition into operational support and post-implementation governance.

Details of Project Launch

Prior to the formal kickoff of the project, a comprehensive stakeholder engagement and communication plan will be developed. This plan will identify the executive sponsors, department managers, IT staff, and end users. This plan will also detail the methods of communication, reporting frequencies, and feedback mechanisms to ensure consistent and open communication between stakeholders throughout the project lifecycle. As part of developing this plan, a project communication toolkit will be created. The toolkit will contain an overview of the project, including the business case, a high-level timeline, expected impacts on end-users, and anticipated benefits (Karin, 2025). This toolkit will be consistently utilized during the launch and throughout the project to ensure that the messaging remains aligned.

Following the approval of the project charter by Executive Leadership, a formal kickoff meeting will be held to mark the official launch of the project. The kickoff meeting will include representatives from Executive Leadership, Department Managers, IT Personnel, and selected End Users to ensure a consensus across the organization. Best practices indicate that the kickoff meeting will set the cultural tone for the project, clarify expectations, and establish a collective sense of ownership about the project outcomes (Indeed Editorial Team, 2025). At the meeting, an overview of the project background and business problem will be provided, followed by a detailed review of the proposed solution, scope boundaries, implementation timeline, and major milestones. Using a structured responsibility framework, roles and responsibilities will be identified and defined for all parties involved in the project. Additionally, the governance model for making decisions and escalating issues will be formally outlined. Issues related to initial project risks, mitigation strategies, and user impacts will also be discussed. Following the meeting, all questions will be answered and the immediate next steps confirmed.

In conjunction with the kickoff meeting, the project governance will also be formally established. An executive-level Project Sponsor will provide strategic guidance and ensure alignment with organizational objectives, while the IT Manager will serve as the Project Manager, with full authority to execute the project, schedule it, and coordinate resources. Establishing a governance structure ensures accountability, facilitates timely decision-making, and eliminates ambiguity related to authority and responsibility, two of the most common reasons projects fail (PMI, 2021). The governance roles and escalation procedures will be formally documented and communicated during the launch to reinforce organizational support and leader engagement.

A central location for storing all project-related documentation will be established during the launch to support transparency, collaboration, and audit-readiness. All project documents will be stored on a secure, shared platform accessible to authorized stakeholders. These documents will include the project charter, risk register, communication plans, architecture diagrams, procurement records, meeting minutes, and training materials.

Following the kickoff meeting, a company-wide project announcement will be sent to all employees. The announcement will outline the objectives of the modernization effort, the expected benefits to daily operations, the high-level timeline for deployment, and what users can expect during the transition. Status updates regarding the project will be made available on a regular basis to keep employees engaged, informed about the project's progress, and provide advance notice of any activities that may impact users. Feedback mechanisms will be included in these communications to ensure that employee concerns and questions are addressed in a timely manner.

The structured launch strategy outlined above utilizes industry best practices for stakeholder engagement, governance, and communication. The strategy is specifically designed to create trust, generate early momentum, and create a sense of ownership in the project across all levels of the organization. By incorporating formal governance, proactive communication, executive sponsorship, and user engagement from the beginning, the project launch will significantly increase the likelihood of successfully implementing and sustaining the operational use of the project solutions.

Strategy for Implementation

High Desert Engineering's implementation strategy for its network infrastructure, hardware, and MFA project will utilize a customized hybrid predictive methodology, based on PMI's PMBOK Guide. In this methodology, HDE has combined the structured control and predictability of a traditional predictive life cycle with a few limited adaptive elements to accommodate the testing of technology, phased deployment, and the need for user adoption. A predictive methodology has been selected because well-defined project parameters and requirements were established prior to initiating the project. The use of adaptive elements in the methodology, such as pilot testing and the gradual migration of users to the new environment, can help mitigate the risks associated with operational disruption while increasing the likelihood of successful user acceptance without compromising control over the process.

The implementation strategy is designed from an IT Operations standpoint to provide for continued service delivery during the transition to the new environment. The core infrastructure components, including managed switches, the Fortinet Firewall, and wireless access points, will be deployed first in a controlled staging environment and then integrated into the production environment. Standard operating procedures, configuration baselines, and rollback procedures will be developed and completed prior to cutover to ensure the ability to deliver the required services in the new environment and maintain a stable environment. After-hours deployment windows, parallel system validations, and increased Help Desk staffing will be implemented during the cutovers to minimize the impact on the business. The operational controls included in the implementation strategy meet the requirements for IT service management best practices, including providing for availability, incident response readiness, and change control throughout the project's execution.

Enterprise architecture principles are also incorporated into the implementation strategy to provide for long-term scalability, interoperability, and alignment with business goals. The future-state architecture was established based on standardized endpoint platforms, segmented network layers, centralized identity management, and cloud-integrated services. The deployment of infrastructure components will be accomplished using a layered architecture model that defines a clear separation between access, distribution, core, and security layers. This will ensure that future systems, including cloud applications, analytics platforms, and remote work services, can integrate seamlessly into the environment without requiring a large-scale redesign. By deploying the components based on defined architectural standards and configuration templates, the project has reduced technical debt and supported long-term IT governance objectives.

Rather than treating disaster recovery and business continuity as add-ons to be completed after the initial deployment, they are being embedded directly into the implementation strategy. Firewall configurations, network segmentation, and Microsoft 365 identity services are being implemented with built-in redundancy, off-site identity authentication, and cloud-based continuity capabilities. System imaging and standardized workstations enable rapid restoration of devices in the event of hardware failure. Full system backups and configuration snapshots will be taken before each major cutover, enabling rapid rollback if needed. Post-deployment testing will include recovery validation for authentication services and critical network components. This approach meets the fundamental requirements for disaster recovery planning.

Information security and assurance are the basis for the entire implementation strategy. Security-by-design principles will be applied across all phases of execution. The deployment of the Fortinet next-generation firewall, VLAN segmentation, secure wireless encryption, endpoint encryption, and mandatory MFA will directly support the confidentiality, integrity, and availability objectives (Fortinet, n.d.). Centralized identity through Microsoft 365 enables conditional access, audit logging, and continuous authentication monitoring. Security testing, including vulnerability validation, access verification, and log review, will be completed before granting full production access. These controls meet the functional requirements of the NIST Cybersecurity Framework, specifically the functions of identify, protect, detect, respond, and recover (NIST, 2024).

Documentation Deliverables

The project will produce standard, structured documentation to help ensure governance, operational continuity, audit readiness, and long-term sustainability for all components of the IT environment. The core documentation includes the project charter that has been formally approved, detailed network and security architecture diagrams, configuration standards for both hardware and software, MFA policy and user guide, deployment runbooks, an updated risk register documenting all risks identified during the project and mitigated at completion, an up-to-date asset inventory record of all hardware, software and other assets purchased or otherwise acquired during the project, and training documentation and user manuals for end-users. A formal post-project implementation evaluation report and a formal "lessons learned" document will also be prepared. Documentation will be retained in a single, centrally located, secure storage location to facilitate controlled access to authorized personnel, version tracking, and auditable history. The documentation will provide assurance that the organization can sustain the upgrades made to the IT environment over time, audit those changes as necessary, and scale the new environment, if required, in accordance with industry-recognized IT governance and operations best practices.

Hardware and Software Deliverables

The hardware portion of the deliverable package includes a complete installation of standardized and scalable endpoints and networks necessary to operate in the new and modernized IT environment. The hardware included in this portion of the deliverable package consists of 60 Dell Pro desktop units configured with dual monitors, three Netgear managed switches, six Cisco wireless access points, and one Fortinet FortiGate 80F firewall. These hardware elements will provide the physical foundations necessary for a highly available operation, a segmented and secure network environment, and deliver each end-user a high-performance computing experience. All hardware will be tracked through an inventory process, tagged, and documented as part of our asset management process to support the tracking of the hardware's life cycle, manage warranties, and plan for future upgrades.

The software deliverable package will contain Microsoft 365 Business Premium licenses for each user, primarily, along with all the identity, endpoint management, and security-related configurations. Within the Microsoft 365 Business Premium license, there are multiple configuration options related to Intune device management profiles, centralized identity policies, multi-factor authentication enforcement, endpoint encryption settings, and conditional access rules. In addition to the Microsoft 365 Business Premium license, standardized workstation images, security monitoring configuration, and cloud-based collaboration services will also be delivered. Together, the software deliverable package will allow for secure access control, centralized administration, compliance alignment, and improved organizational productivity.

Evaluation Framework

The evaluation framework for the upgrade of HDE's network infrastructure, hardware, and MFA projects establishes the standards and criteria for all aspects of the project, ensuring that project deliverables meet the required quality standards and business objectives. This framework was developed based on the three core processes for managing project quality, as identified in the PMBOK Guide: plan quality management, manage quality, and control quality (PMI, 2021). Combined, these three processes provide the definition of quality to be achieved within the project, methods to build quality into the project, and verification that quality has been achieved during the project life cycle. In addition, the evaluation framework has been developed in accordance with current IT and security best practices, including the NIST Cybersecurity

Framework and CIS Critical Security Controls, ensuring that both the performance of the technical capabilities and the information assurance requirements of the project are met.

In the plan quality management phase, quality standards, acceptance criteria, and performance metrics will be formally defined and documented prior to the commencement of project execution. Requirements for quality will include hardware reliability standards, network uptime targets, security control baselines, and user authentication success thresholds. These criteria will be documented in the project quality management plan and compared against similar industry benchmarks, such as secure configuration standards and identity security best practices. Historical baseline performance data for system uptime, help-desk ticket volumes, authentication failure rates, and endpoint performance will be collected prior to implementation for comparative evaluation purposes. This planning phase will ensure that quality expectations are well-established, measurable, and traceable to business and regulatory requirements (PMI, 2021).

The manage quality phase will be addressed throughout the project's execution by incorporating quality assurance practices directly into each project activity. Standards for configuration, procedures for change control, peer reviews, and technical validations will be implemented to ensure that deliverables are created properly the first time. Network devices, firewall rules, and MFA policies will be configured according to documented templates and vendor-recommended best practice guidelines. Pilot deployments and phased rollouts will be used as quality assurance tools to test performance and usability before releasing to production. The effectiveness of the training will be evaluated through user feedback and successful authentication rates during the early deployment waves. These activities represent the PMBOK's focus on quality assurance as a proactive process to prevent defects, as opposed to reactive quality assurance, which detects them after the fact (PMI, 2021)

The control quality process will be used to formally measure, inspect, and verify that deliverables were created to meet defined acceptance criteria. Testing after the deployment of the new systems will include network performance testing, security control verification, vulnerability scanning, MFA authentication testing, and UAT. Performance measures related to quantity, such as system uptime, MTTR, trends in help-desk tickets, and the frequency of security incidents, will be collected and compared against historical baselines. Any variances from the quality standards will prompt corrective action through formal change control. Executive management and department heads will serve as the final approval authorities by formally signing off on UAT and KPI results. This inspection-based verification process aligns with the PMBOK's requirement to verify that deliverables comply with the requirements prior to project closure (PMI, 2021).

This evaluation framework supports best practices for information security and assurance through ongoing monitoring of controls related to the five functions of the NIST Cyber Security Framework: identify, protect, detect, respond, and recover (NIST, 2024). The CIS critical security controls will be utilized as practical examples of acceptable benchmarks for access control, asset management, secure configuration, and continuous monitoring (CIS, 2023). Through the integration of these technical standards into the project quality evaluation process, the framework ensures that the project is evaluated based on its performance relative to both the scheduled and budgetary objectives, while also ensuring that the project contributes to enhancing the company's cybersecurity posture and operational resilience.

This multi-layered evaluation framework provides structured, data-driven assurance that the project outcome will meet the intended business, operational, and security objectives. By utilizing the PMBOK quality management processes, along with widely recognized cybersecurity and IT governance standards, the organization is assured that the final solution is verifiable, auditable, and consistent with industry best practices for quality assurance and acceptance.

References

CIS Critical Security Controls. (n.d.). CIS. https://www.cisecurity.org/controls

"Compare Microsoft 365 Plans: Microsoft 365." *Compare Microsoft 365 Plans | Microsoft 365*, www.microsoft.com/en-us/microsoft-365/business/compare-all-microsoft-365-business-products-b?ef_id=_k_CjwKCAiAxc_JBhA2EiwAFVs7XFw9_XRhoU2RvEWtXaldzEVGc-u-F_qZF6vBvqsjmSXsrUHUFoRm6BoCll8QAvD_BwE_k_&OCID=AIDcmmq8c1jdfb_SEM__k_CjwKCAiAxc_JBhA2EiwAFVs7XFw9_XRhoU2RvEWtXaldzEVGc-u-F_qZF6vBvqsjmSXsrUHUFoRm6BoCll8QAvD_BwE_k_&gad_source=1&gad_campaignid=21842944472&gbraid=0AAAAADcJh_vyOl41gKyVVL3shec7kXmeb&gclid=CjwKCAiAxc_JBhA2EiwAFVs7XFw9_XRhoU2RvEWtXaldzEVGc-u-F_qZF6vBvqsjmSXsrUHUFoRm6BoCll8QAvD_BwE. Accessed 6 Dec. 2025.

Dell Pro Slim Desktop with AI - Slim Business Computer | Dell USA. (n.d.). Dell. https://www.dell.com/en-us/shop/desktop-computers/dell-pro-slim-plus-desktop/spd/dell-pro-qbs1250-plus-slim-desktop

Dell Pro 24 Inch Plus Monitor P2425H - FHD IPS Display | Dell USA. (n.d.). Dell. https://www.dell.com/en-us/shop/dell-pro-24-plus-monitor-p2425h/apd/210-bmgh/monitors-monitor-accessories

Fortinet FortiGate 80F Series | AVFirewalls.com. (n.d.). https://www.avfirewalls.com/fortigate-80f.asp?srsltid=AfmBOorotzIM1lbANq8pl6N01t0YiKdu3k77UImVpGiZBGXAJ7X3r_7A0kY

FTC safeguards rule: What your business needs to know. (2024, December 23). Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

Indeed Editorial team. "How To Host a Successful Project Kickoff Meeting in 7 Steps." *Indeed Career Guide*, 19 Nov. 2025, ca.indeed.com/career-advice/career-development/kickoff-meeting?gclsrc=aw.ds&aceid=&gad_source=1&gad_campaignid=15513873562&gbraid=0AAAAADfh6_u23FSnXk71lWLPaqcb-2fV-&gclid=Cj0KCQiA6NTJBhDEARIsAB7QHD1gNTrs9vPZ4M6jHdM1_9grSnvmtqH8Kgc9y8EbMWrr29KTZfM9ysIaAk2xEALw_wcB.

Karin. (2025, January 23). *Project communication toolbox*. Swelife. https://swelife.se/en/swelifes-projects/project-communication-toolbox/

Micro Center. *Cisco Business 150AX Wi-Fi 6 2x2 Access Point - Micro Center*. https://www.microcenter.com/product/661368/cisco-business-150ax-wi-fi-6-2x2-access-point

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* [Report]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Netgear JGS524NA ProSafe 24-Port Gigabit Switch from PCLiquidations. (n.d.). https://www.pcliquidations.com/netgear-jgs524na-prosafe-24/p/155164?srsltid=AfmBOoqUfvGkOhUcGVgXfgl4xIfakxNgdW_xkmrl0amvgipC97gF3GfKJBQ

"Network and Computer Systems Administrators." *U.S. Bureau of Labor Statistics*, U.S. Bureau of Labor Statistics, 28 Aug. 2025, www.bls.gov/ooh/computer-and-information-technology/network-and-computer-systems-administrators.htm.

Project Management Institute. (2021). A Guide to the Project Management Body of Knowledge (PMBOK Guide). *PMBOK Guide*. https://library.fbe.uii.ac.id/index.php?p=show_detail&id=5900&keywords=

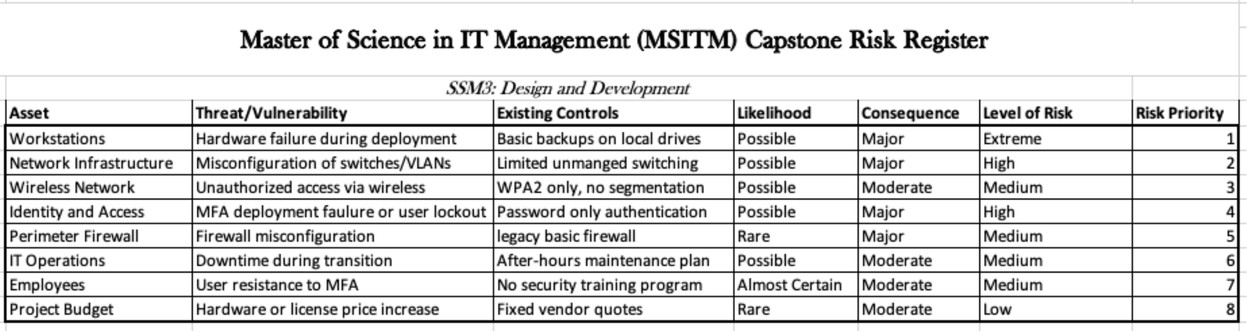
What is the CIA Triad and Why is it important? | Fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/cia-triad

Tables

Itemized Costs

Category	Item	Quantity	Unit Cost	Total Cost
Hardware	Dell Pro Slim Desktop	60	$1,089	$65,340
Monitors	Dell Pro 24" Monitor	120	$189.99	$22,798
Network Switch	Netgear 24 port switch	3	$154.59	$463.77
Wireless Access Points	Cisco WAPS	6	$154.99	$929.94
Perimeter Security	Fortinet 80F Firewall Appliance	1	$1,138.70	$1,138.70
Software/Licensing	Microsoft 365 Business Premium	60 x 12 months	$22	$15,840
Labor	Internal IT labor	200 hours	Average $41/hour	$8,200
Total				$114,710.41

Risk Assessment



Master of Science in IT Management (MSITM) Capstone Risk Register

SSM3: Design and Development

Asset	Threat/Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Workstations	Hardware failure during deployment	Basic backups on local drives	Possible	Major	Extreme	1
Network Infrastructure	Misconfiguration of switches/VLANs	Limited unmanged switching	Possible	Major	High	2
Wireless Network	Unauthorized access via wireless	WPA2 only, no segmentation	Possible	Moderate	Medium	3
Identity and Access	MFA deployment faulure or user lockout	Password only authentication	Possible	Major	High	4
Perimeter Firewall	Firewall misconfiguration	legacy basic firewall	Rare	Major	Medium	5
IT Operations	Downtime during transition	After-hours maintenance plan	Possible	Moderate	Medium	6
Employees	User resistance to MFA	No security training program	Almost Certain	Moderate	Medium	7
Project Budget	Hardware or license price increase	Fixed vendor quotes	Rare	Moderate	Low	8

Resource Allocation Plan

Resource type	Role	Allocation method	Project phase
Manpower	IT Manager (Project Manager)	20% time weekly	All phases
Manpower	Network Administrator	Full time during infrastructure phase	Execution
Manpower	System Administrator	Full time during hardware and MFA	Execution

Manpower	Help Desk Technician (2)	Part time deployment and full time support	Execution and support
Manpower	End Users	Limited testing participation	Testing
Hardware	Dell Pro Desktops (60)	Assigned to employees in phased rollout	Deployment
Hardware	Netgear managed switch (3)	Installed subsequently to maintain uptime	Infrastructure
Hardware	Dell monitors (120)	Installed with desktops	Deployment
Hardware	Cisco WAPs (6)	Staggered deployment by building zones	Infrastructure
Hardware	Fortinet FortiGate 80F firewall	Integrated at network core	Infrastructure
Software	Microsoft 365 Business Premium (60)	Assigned through centralized identity system	All phases
Financial	$114,710.41 project budget	Released in stage-gated funding increments	All phases
Financial	10% contingency reserve	Held by IT committee	Risk response

Project Phases

Phase	Project Activities	Start Date	End Date	Key Milestones
Phase 1: Project initiation and planning	Project charter approval, stakeholder identification, requirements validation, risk baseline	March 2, 2026	March 20, 2026	Project charter approved, budget is authorized
Phase 2: Design and procurement	Final architecture design, vendor selection, hardware/software selection	March 23, 2026	April 17, 2026	All vendor contracts completed, hardware orders submitted
Phase 3: Infrastructure deployment	Switch installation, firewall deployment,	April 20, 2026	May 22, 2026	Network core fully operational and security validated

	WAP install, VLAN configuration			
Phase 4: Workstation and MFA deployment	Workstation imaging and rollout, Microsoft 365 configuration, MFA enforcement	May 26, 2026	June 30, 2026	All users migrated to the new system with MFA enabled
Phase 5: Testing, training, and optimization	Performance testing, security validation, employee training	July 1, 2026	July 17, 2026	User acceptance tasting completed
Phase 6: Project closeout and evaluation	Final documentation, KPI measured, lessons learned	July 20, 2026	July 31, 2026	Formal project closure and stakeholder approval

Timeline

Phase	Project Activities	Start Date	End Date	Key Milestones
Phase 1: Project initiation and planning	Project charter approval, stakeholder identification, requirements validation, risk baseline	March 2, 2026	March 20, 2026	Project charter approved, budget is authorized
Phase 2: Design and procurement	Final architecture design, vendor selection, hardware/software selection	March 23, 2026	April 17, 2026	All vendor contracts completed, hardware orders submitted
Phase 3: Infrastructure deployment	Switch installation, firewall deployment, WAP install, VLAN configuration	April 20, 2026	May 22, 2026	Network core fully operational and security validated
Phase 4: Workstation and MFA deployment	Workstation imaging and rollout, Microsoft 365 configuration, MFA enforcement	May 26, 2026	June 30, 2026	All users migrated to the new system with MFA enabled

Phase 5: Testing, training, and optimization	Performance testing, security validation, employee training	July 1, 2026	July 17, 2026	User acceptance tasting completed
Phase 6: Project closeout and evaluation	Final documentation, KPI measured, lessons learned	July 20, 2026	July 31, 2026	Formal project closure and stakeholder approval