

A report prepared in partial completion of
The CYBR 7930 Capstone course

Security Operations Program Design

Ethan Byrd

November, 2025

Contents

Executive Summary3

Problem Statement3

Scope3

Current Environment4

Endpoint Protection4

Vulnerability Management.....4

SIEM & Log Monitoring4

Data Loss Prevention (DLP).....4

Email Protection5

Cloud Security5

Phishing Simulation & Security Training5

Forensic Tools5

Patch Management.....5

Future State Vision: Intended Security Operations and Environment6

Unified Security Operations Center (SOC).....6

Advanced Threat Detection & Detection Engineering6

Continuous Vulnerability Management.....7

Automated Incident Response Lifecycle7

Identity & Access Governance.....7

Cloud Security Maturity7

Enhanced Data Protection & DLP Integration.....7

Comprehensive Training & Simulation Programs.....7

Structured Disaster Recovery & Business Continuity.....7

Governance, Metrics & Executive Reporting.....8

Improvement Program.....9

Phase 1: Foundational Alignment (Months 0–3).....9

Phase 2: Operational Integration (Months 3–6) 10

Phase 3: Advanced Capability Deployment (Months 6–12) 10

Phase 4: Governance & Optimization (Months 12–18) 11

Budget 12

Security Run Book..... 13

Conclusion 17

AI/LLM Usage Statement..... 18

Executive Summary

Diamond Hands Holding Inc. (DHHI) currently operates as a high-level firm specializing in Governance Risk and Compliance and Information Security Consulting services. DHHI is entering a transitional period, which will include relocating to a new headquarters and expanding its digital and personnel operations. These upcoming changes have introduced new risks that organizations' current security stance is not set up to support. While DHHI is taking beginner steps such as aligning with the NIST Framework and has begun a Security Services Directory to work towards new security and operational standards.

This report provides a modern and robust Security Operations environment that will support the initiative and mission DHHI has provided. The recommendations within this document will continue to draw from NIST best practices and publications such as SP 800-12, 800-35, and 800-100. These publications will allow DHHI to implement pieces of governance, structure, monitoring, and companywide trust and responsibility.

Problem Statement

Due to a larger attack surface during this transitional period, DHHI faces both operational and financial risk. As the company grows, new assets are added, and the company moves to a new headquarters, the current implemented approach grows outdated which will lead to further security risks and leaks, which will result in brand reputation being tarnished.

The central problem that will be addressed in this report is that DHHI lacks a modernized security operations model capable of preventing such losses during a transitional period. The security team must have a change of focus from covering up risks as they appear but have a monitoring focus to prevent problems and monitor future issues before they even appear, allowing for a smooth transition. This report will define that foundation and framework that DHHI will need to achieve that change of focus.

Scope

This report will apply to all DHHI and its subsequent ventures and the intended for usage in leadership, IT operations, Information Security teams, Stakeholders, and employees of the company. This outline will provide a fully robust design of a Security Operations Environment, which will cover vulnerability management, threat detection, incident response, access control, zero trust, application security and disaster recovery. It will also integrate services and recommendations found in previous documentation such as Security Services Directory, and NIST recommendations. This report will not provide specific vendor implementation, procurement processes, or technical implementation guides but will establish a strategic, operational foundation needed to modernize DHHI's security stance.

Current Environment

The current environment exists to ensure prevention, mitigation, and control of harm that could come from cyber threats and attacks. Without the outlined controls, DHHI would be completely open to risks and exposing critical data, business operations would be unable to continue a day-to-day basis. The current environment consists of Endpoint Protection, Vulnerability Management, Security Information and Event Management (SIEM) & Log Monitoring, Data Loss Prevention, Email Security, Cloud Security, Phishing Simulation & Training, Forensic Tools, and Patch Management. These operations form the foundational security architecture at DHHI, and identifying their strengths and weaknesses allows the organization to better understand where control deficiencies and vulnerabilities exist. Once those vulnerabilities are identified, appropriate risk assessment and remediation can take place to ensure solutions are both cost-effective and aligned with DHHI's business needs. Continuous monitoring and reporting further help leadership understand the effectiveness of current controls and provide insight into the evolving threat landscape. A strong understanding of current operations also supports a smoother transition to future-state security design. A short description of these security operations is provided below.

Endpoint Protection

DHHI utilizes preventative endpoint security tools to protect employee laptops and devices from malware, unauthorized applications, and unsafe behaviors. These tools support zero-trust principles by restricting unauthorized execution, blocking malicious processes, and ensuring encryption and monitoring are active. Endpoint protection prevents the spread of ransomware, credential theft, and data loss across the organization.

Vulnerability Management

DHHI uses a vulnerability management platform to identify, track, and prioritize system weaknesses. This platform enables the security team to detect misconfigurations, outdated software, and exploitable services before attackers can take advantage of them. While vulnerability scans occur regularly, the prioritization and remediation process remains partially manual, creating opportunities for improvement.

SIEM & Log Monitoring

DHHI maintains a Security Information and Event Management (SIEM) system that aggregates logs from key systems. The SIEM provides visibility into suspicious activity, user behavior anomalies, and potential indicators of compromise. Although SIEM monitoring exists, correlation rules, alert tuning, and centralized dashboard development are still maturing, resulting in lower efficiency and slower detection times.

Data Loss Prevention (DLP)

DHHI uses a Data Loss Prevention solution to monitor and restrict unauthorized data transfer, preventing sensitive company information from leaving the organization. DLP helps enforce

compliance, reduce insider threats, and protect intellectual property. Current DLP coverage is functional but not yet fully integrated across all cloud systems and collaboration platforms.

Email Protection

Email filtering tools block malicious attachments, phishing attempts, and spam from entering employee inboxes. These protections reduce the risk of credential theft and malware delivery. While the system effectively filters known threats, more advanced detection mechanisms and closer tuning to business workflows are needed to reduce residual social-engineering risk.

Cloud Security

DHHI uses cloud storage and access controls that incorporate multi-factor authentication and encryption. These controls ensure data integrity, secure access, and compliance with industry expectations. Although the cloud environment is protected, governance standards, configuration reviews, and automated alerts for risky activity require additional maturity.

Phishing Simulation & Security Training

The organization conducts phishing simulations and training sessions to strengthen employee readiness and reduce human-factor vulnerabilities. These exercises help identify risky behaviors and guide improvements in user education. While present, these programs lack consistent measurement and follow-up, limiting their long-term effectiveness.

Forensic Tools

DHHI maintains forensic software and hardware to investigate cyber incidents and preserve digital evidence. These tools support root cause analysis after a security event and help document incident impact. Forensic capabilities are available but used only during limited circumstances, and the organization relies heavily on manual processes.

Patch Management

Automated patch management tools help deploy operating systems and software updates across the organization. These updates reduce exposure to known vulnerabilities and support compliance with security frameworks. While patching occurs regularly, the validation process and prioritization for high-criticality assets require further development.

Future State Vision: Intended Security Operations and Environment

The purpose of this section is to describe the intended future state of Diamond Hands Holdings Inc.'s (DHHI) security operations environment. The goal of this future environment is to create an integrated, proactive, and fully aligned security program capable of protecting the organization as it grows into its new headquarters and expands its operational footprint. This future state is designed to reduce residual risk, increase operational resilience, and ensure that security becomes an embedded, organization-wide capability rather than a reactive or isolated function.

The intended security operations environment will consist of a unified Security Operations Center (SOC), advanced detection engineering practices, continuous vulnerability management, automated incident response workflows, identity and access governance, cloud security reinforcement, and a structured disaster recovery strategy. These components will operate together as a cohesive system. When fully implemented, this environment will allow DHHI to detect threats earlier, respond to incidents faster, and prevent attackers from exploiting weaknesses in the company's digital infrastructure.

A mature future-state environment also promotes strong organizational governance. Security decisions will be informed by metrics, supported by leadership, and aligned with NIST Cybersecurity Framework (CSF) 2.0 principles. Quarterly reviews will evolve into continuous monitoring, and manual processes will transition to automated pipelines. This will allow DHHI to be more confident in the accuracy of its risk assessments, more efficient in deploying new security controls, and more agile in adapting to new threats.

To support this transformation, descriptions of the intended future-state security operations are provided below.

Unified Security Operations Center (SOC)

The future SOC will serve as the centralized hub for all monitoring, alerting, and analysis activities. Rather than scattered monitoring tools and inconsistent reporting, the SOC will bring all logs, alerts, and telemetry into one environment that provides around-the-clock insight into DHHI's security posture. Analysts will be able to quickly detect anomalies, investigate suspicious events, and escalate incidents through a standardized workflow.

Advanced Threat Detection & Detection Engineering

DHHI will establish a well-defined detection engineering program to create, tune, and validate alert rules. By improving alert accuracy, the organization will reduce false positives and ensure that analysts focus on meaningful events. This capability will give DHHI earlier warning of attacks and reduce the time between threat introduction and detection.

Continuous Vulnerability Management

The future environment will replace periodic scanning with continuous vulnerability identification and automated prioritization. Instead of relying on manual judgment, vulnerabilities will be ranked based on exploit availability, asset criticality, and exposure. This ensures that the highest-risk issues are addressed first and lowers the likelihood of attackers exploiting unpatched weaknesses.

Automated Incident Response Lifecycle

DHHI will implement a structured incident response lifecycle that includes preparation, detection, containment, eradication, recovery, and lessons learned. Automation will be used where appropriate to speed up containment and reduce human error. Clear communication channels, reporting processes, and role assignments will help the organization manage incidents effectively and return to stable operations quickly.

Identity & Access Governance

The intended environment will utilize principle-of-least-privilege controls, automated provisioning and deprovisioning, strong multi-factor authentication, and regular access reviews. Advanced identity governance reduces the risk of unauthorized access and ensures that sensitive systems and data are only accessible by those who require it.

Cloud Security Maturity

Cloud services will be monitored continuously for risky configurations, unauthorized access attempts, and data movement. Improved encryption controls, audit logging, and automated compliance checks will ensure that cloud resources remain secure as the organization grows.

Enhanced Data Protection & DLP Integration

DLP will expand to cover all major communication channels—including cloud storage, email, and collaboration tools. The future state will provide better visibility into sensitive data flows, helping prevent accidental or malicious leakage.

Comprehensive Training & Simulation Programs

Security education will become a continuous lifecycle activity rather than isolated events. Annual training, quarterly phishing tests, targeted lessons for high-risk departments, and post-simulation feedback loops will strengthen the human layer of defense.

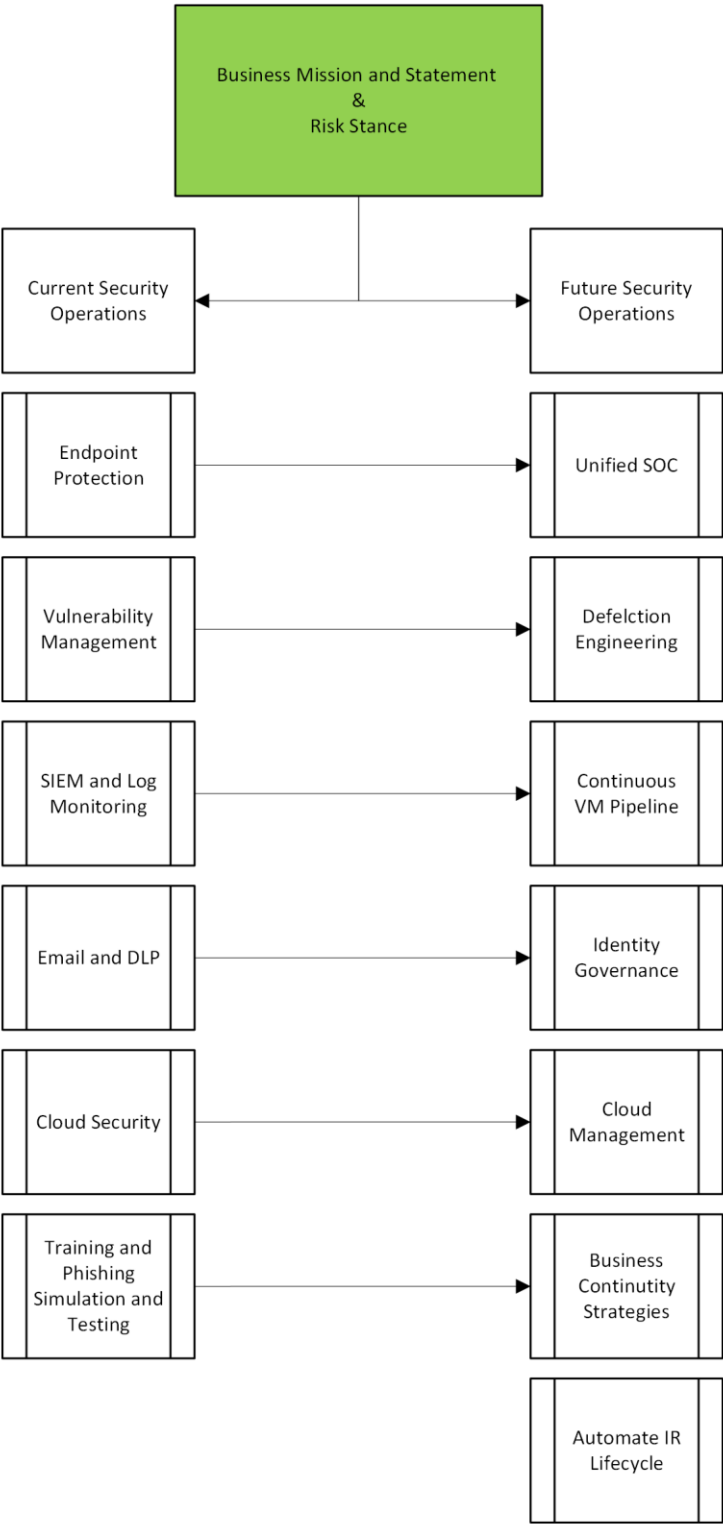
Structured Disaster Recovery & Business Continuity

DHHI will fully integrate its disaster recovery plan with its operational processes. Regular testing, dependency mapping, and documented recovery strategies will reduce downtime during catastrophic events and ensure data is restored quickly and reliably.

Governance, Metrics & Executive Reporting

The future security environment will rely heavily on measurable KPIs to guide progress. Metrics such as patch compliance, incident response time, vulnerability closure rate, and training effectiveness will be reported to executives quarterly. This allows security decisions to be grounded in data and ensures accountability across teams.

Figure 1.



Improvement Program

The purpose of this Improvement Program is to outline the structured plan that Diamond Hands Holdings Inc. (DHHI) will follow to transition from its current, partially developed security operations environment to the integrated and mature future-state security environment defined in the previous section. This program focuses on a phased approach that prioritizes foundational capabilities first, ensuring that the most critical risks are addressed promptly while supporting long-term operational scalability.

This Improvement Program emphasizes the principles found in NIST SP 800-12, SP 800-35, and SP 800-100, all of which highlight the importance of lifecycle management, governance, training, and the coordinated deployment of security services. DHHI will follow these principles by adopting a step-by-step maturity model that elevates detection, response, and governance capabilities in a logical sequence. The goal is to build a sustainable security program that supports business continuity, enhances readiness, and reduces residual risk.

The improvement process consists of four strategic phases: **Foundational Alignment, Operational Integration, Advanced Capability Deployment, and Governance & Optimization**. Each phase builds upon progress from the previous stage to ensure a smooth transition into the intended future state environment.

Phase 1: Foundational Alignment (Months 0–3)

This phase focuses on establishing the minimum foundational capabilities required to support future-state operations.

Key efforts include:

1. Establish Security Governance Structure

- Formalize roles and responsibilities already described in the SSD.
- Begin consistent, metrics-driven quarterly meetings.
- Launch uniform documentation and ticketing practices.

2. Enhance Endpoint Protection & Patch Management

- Confirm endpoint security configurations.
- Strengthen automated patch deployment across critical systems.
- Define asset criticality levels to support risk-based patching.

3. Improve Cloud Security Baselines

- Implement configuration baselines for all cloud resources.
- Enforce MFA and role-based access controls across cloud platforms.

Outcome: DHHI has a documented, standardized foundation that reduces basic, high-frequency risks.

Phase 2: Operational Integration (Months 3–6)

During this phase, the organization begins integrating existing tools into more unified workflows.

1. Centralize Log Sources Into the SIEM

- Ensure all critical systems forward logs to a single monitoring platform.
- Begin with initial rule tuning to reduce noise.

2. Launch Continuous Vulnerability Identification

- Move from periodic scanning to scheduled, repeated scanning.
- Implement threat-based prioritization using CVSS + business importance.

3. Begin Formal Incident Response Drills

- Conduct tabletop exercises to validate roles and communications.
- Develop a basic IR lifecycle aligned with NIST guidance.

Outcome: Fragmented tools begin functioning as an integrated system with consistent visibility.

Phase 3: Advanced Capability Deployment (Months 6–12)

This phase implements the future-state capabilities that provide the highest return on investment.

1. Stand Up the Unified SOC

- Assign SOC responsibility to security leadership.
- Develop SOC workflows (alert intake, case creation, escalation).
- Define SLAs for detection and response activities.

2. Deploy Detection Engineering Program

- Create and maintain detection rules mapped to MITRE ATT&CK.
- Develop a false-positive and false-negative reduction cycle.

3. Introduce Forensic Readiness and Automated IR Lifecycle

- Integrate forensic tools into the IR process.
- Automate containment actions for high-severity alerts.
- Document post-incident reporting and lessons learned.

Outcome: DHHI transitions from reactive security to initiative-taking, intelligence-driven operations.

Phase 4: Governance & Optimization (Months 12–18)

This final phase focuses on long-term sustainability, optimization, and organizational readiness.

1. Expand DLP Across All Channels

- Extend data protection to cloud storage, email, and collaboration platforms.
- Implement data handling rules for sensitive information.

2. Strengthen Employee Security Awareness Lifecycle

- Quarterly phishing simulations with role-based difficulty.
- Department-specific micro-training based on observed risk.

3. Implement Business Continuity & Disaster Recovery Testing

- Conduct annual recovery testing scenarios.
- Validate RTO/RPO targets and dependency mapping.

4. Refine KPIs and Executive Reporting

- Monthly dashboard for leadership including:
 - Mean Time to Detect (MTTD)
 - Mean Time to Respond (MTTR)
 - Vulnerability closure rates
 - Training performance metrics
- Use data to drive budgeting, staffing, and risk decisions.

Phase	Timeline (Months)	Key Focus Areas
Phase 1: Foundational Alignment	0–3	Governance, Endpoint Security, Patch Management, Cloud Baselines
Phase 2: Operational Integration	3–6	SIEM Centralization, Continuous Vulnerability Identification, IR Drills
Phase 3: Advanced Capability Deployment	6–12	Unified SOC, Detection Engineering, Automated IR Lifecycle
Phase 4: Governance & Optimization	12–18	DLP Expansion, Security Awareness Lifecycle, DR Testing, KPI Reporting

Figure 2

Budget

Security Operation	Cost Estimate	Total Per Security Operation
Centralized Threat Detection & Security Monitoring		\$112,000
SIEM Platform License	\$70,000	
Log Storage	\$22,00	
Professional Services	\$15,00	
SOC Training and Certifications	\$5,000	
Enhanced Endpoint EDR		\$69,500
EDR Solution License	\$55,00	
Deployment Services	\$10,000	
EDR Training	\$4,500	
Application Security and Development		\$30,000
SAST/DAST Tooling	\$30,000	
Security Awareness and Training		\$12,000
Phishing Simulation	\$4,000	
Annual Security Training	\$8,000	
Data Loss Prevention		\$25,000
DLP Tool License	\$25,000	

Security Run Book

The purpose of the Diamond Hands Holdings Inc. (DHHI) Master Security Run Book is to provide a unified, organization-wide operational guide for responding to cybersecurity events, managing daily security responsibilities, and ensuring consistent execution of security procedures. As DHHI transitions into its future-state security environment, the Run Book will serve as the authoritative reference for all security operations personnel, enabling effective coordination across the Security Operations Center (SOC), incident response teams, technology leadership, and supporting business units.

This Run Book is designed to align with the NIST Cybersecurity Framework (CSF) and supporting publications, including NIST SP 800-12, SP 800-35, and SP 800-100. These standards emphasize lifecycle management, continuous monitoring, governance, and structured incident handling—all elements that are reflected in the structure and intent of this Run Book. By adopting a standardized operational guide, DHHI ensures that its security program remains consistent, measurable, repeatable, and resilient.

The Run Book provides the DHHI teams with step-by-step procedures, escalation paths, communication protocols, and defined responsibilities for preventing, detecting, responding to, and recovering from security events. In addition to incident management, it outlines operational processes such as vulnerability remediation, access control coordination, detection engineering workflows, and post-incident review expectations. This framework will enable DHHI to maintain strong situational awareness, reduce response times, and ensure continuity of both business and technology operations.

The Master Security Run Book is a living document. As new tools are deployed, capabilities mature, and the threat landscape evolves, the Run Book will be updated through DHHI's governance process and version-controlled to ensure accuracy. Quarterly review cycles, led by the CISO and SOC leadership, will ensure that procedures remain relevant, aligned with organizational priorities, and reflective of the security maturity roadmap defined in this report.

Master Security Run Book Outline

1. Purpose and Scope

- Objectives of the Run Book
- Teams and audiences covered
- Systems, tools, and environments included
- Limitations and assumptions

2. Roles and Responsibilities

- Executive Leadership
- CISO and Technology Officers
- SOC Analysts (Tier 1, Tier 2, Tier 3)
- Detection Engineering Team
- Digital Forensics and Incident Response (DFIR)
- Identity and Access Management (IAM)
- Legal, HR, and Communications stakeholders
- Third-party and vendor coordination

3. Security Operations Overview

- Description of DHHI's security operating model
- Daily operational tasks
- Monitoring responsibilities and hours of coverage
- Ticketing, case management, and documentation standards

4. Threat Monitoring & Detection Procedures

- SIEM dashboards and alert categories
- Logging requirements for endpoints, servers, cloud, and network
- Detection engineering workflow
- Alert creation, validation, tuning, and documentation

5. Incident Response Lifecycle

- Incident categories (Low, Medium, High, Critical)
- Escalation paths and communication flow
- Containment, eradication, and recovery procedures
- Forensic evidence handling guidelines
- Automated response actions
- Post-incident review and lessons learned

6. Vulnerability and Patch Management

- Continuous vulnerability scanning procedures
- Validation and prioritization process
- Responsibilities for remediation
- Patching schedules and change control workflows
- Reporting and tracking KPIs

7. Identity and Access Management Procedures

- New user provisioning workflows
- Deprovisioning and access revocation
- MFA enrollment
- Privileged access requests and approvals
- Access reviews and recertification cycles

8. Data Protection and DLP Rules

- Monitoring and blocking rules
- Sensitive data handling policies
- Reporting suspicious data movement
- Exceptions and approval processes

9. Cloud Security Operations

- Cloud configuration baselines
- Access control and role assignments
- Monitoring procedures for cloud services
- Backup and recovery expectations

10. Business Continuity and Disaster Recovery

- Activation criteria
- Roles and responsibilities during disruptions
- Communication plan
- Restoration priorities and dependencies
- Testing requirements and documentation

11. Training, Awareness, and Readiness

- Required annual training modules
- Quarterly phishing testing
- Tabletop and red-team exercises
- Measurement and reporting metrics

12. Metrics, Reporting, and Continuous Improvement

- Security KPIs (e.g., MTTD, MTTR, vulnerability closure rate)
- Reporting cadence to executives
- Quarterly review cycle for Run Book updates
- Versioning and document change history.

Conclusion

Diamond Hands Holdings Inc. (DHHI) is at a pivotal moment in its organizational development. With the transition to a new headquarters, expanding operations, and a growing digital footprint, the company faces a rapidly evolving threat landscape that requires a more mature, integrated, and strategically aligned approach to security operations. This report has provided a comprehensive design for advancing DHHI's security posture, beginning with a detailed assessment of the current environment and progressing through a clear future-state vision, structured improvement roadmap, and foundational Security Run Book framework.

The analysis of DHHI's current security operations revealed several strengths, such as defined leadership roles, deployed security tools, and a baseline commitment to the NIST Cybersecurity Framework—while also identifying gaps in integration, visibility, automation, and governance. These challenges are common in growing organizations, but they also represent significant areas of risk if not proactively addressed. The Future State Vision section clearly outlines a cohesive operating model built around centralized monitoring, continuous vulnerability management, advanced detection engineering, automated incident response, and stronger identity and data governance. These capabilities align with industry's best practices and directly support DHHI's long-term business objectives.

The Improvement Program provides a phased, realistic, and prioritized roadmap for achieving that future state. By addressing foundational controls first, integrating tools and processes second, deploying advanced capabilities third, and optimizing governance last, DHHI can mature its security environment in a deliberate, sustainable manner. This approach ensures that new assets are grounded in risk reduction, operational efficiency, and organizational readiness.

Finally, the introduction and outline of the Master Security Run Book establish the operational backbone needed to support ongoing security activities. Standardized procedures, defined responsibilities, and continuous improvement cycles ensure that security operations remain consistent, measurable, and adaptable.

Implementing the recommendations in this report will not only strengthen DHHI's defenses but also enhance overall business resilience. A mature security operations environment enables better decision-making, reduces the impact of potential incidents, safeguards critical data and assets, and preserves organizational trust. By investing in these improvements now, DHHI positions itself to support future growth with confidence and to operate securely in an environment where cybersecurity is essential to long-term success.

AI/LLM Usage Statement

Answer Yes/No	In preparing for this assignment, I used assistance for the checked items	Prompt Used/Comments
No	Planning/Outlining: I used external LLM/AI assistance to plan or outline the topic.	NA
No	Research: I used external LLM/AI assistance to perform preliminary research.	NA
Yes	Composition of Text: I used external LLM/AI assistance to compose any submitted text.	I used external LLM to generate ideas for current and future assets/environment
No	Creation of Graphics or Videos: I used external LLM/AI assistance to create graphics or videos included in the submission.	NA
No	Conceptual or Critical Review: I used external LLM/AI assistance to perform a conceptual or critical review of the draft work.	NA
No	Spell Checking and Grammar Review: I used external LLM/AI assistance to perform spell checking or grammar review.	NA
No	Assistance from Other People: I received assistance from another person.	NA
No	Reuse of Previous Work: I reused by copying or repurposing work submitted for this or another course. If any use is included, how was it used, and did you seek permission from the instructor in advance?	NA
Yes	Certification: I affirm that all statements above are accurate and that the submitted work complies with the course's academic integrity policies.	