Document

Executive Summary

Description

The organization has undertaken a comprehensive security maturity assessment across various controls, domains, and maturity tiers. The assessment measures the organization's standing in terms of repeatability, risk awareness, and adaptability. The scope includes evaluating the implementation and effectiveness of security controls related to administrative, governance, human resource, incident response, legal, physical, and technical domains.

The maturity model assesses the organization's security posture based on its ability to implement, maintain, and continuously improve security controls. The tier levels reflect the organization's capability, ranging from Risk-Informed (Tier 1) to Optimizing (Tier 4).

Key Observations

High-level patterns and trends indicate that the organization has established a foundational level of security maturity, with many controls falling within the Repeatable (Tier 2) and Adaptive (Tier 3) categories. Notable strengths include:

- Implemented data classification systems and document management practices.
- Established incident response plans and forensic capabilities.

- Deployed various technical controls such as DLP, encryption, and UEBA solutions.

However, systemic issues and areas for improvement include:

- Inconsistent documentation and evidence of control implementation.
- Limited automation and integration of security controls.
- Gaps in comprehensive coverage and advanced threat detection capabilities.

Action Items

To enhance its security maturity posture, the organization should prioritize the following actions:

1. **Enhance Documentation and Evidence Collection**: Improve documentation of security controls, policies, and procedures. Ensure that evidence of control implementation is collected and maintained.
2. **Automate and Integrate Security Controls**: Implement automation where possible to streamline security processes and integrate disparate security tools to enhance overall security posture.
3. **Advance Threat Detection and Response**: Expand detection capabilities to include advanced threat protection and improve incident response processes through regular tabletop exercises and training.
4. **Implement Continuous Improvement Mechanisms**: Establish regular review cycles for security controls, policies, and procedures to ensure they remain effective and aligned with business objectives.

By addressing these areas, the organization can progress toward higher maturity tiers, enhancing its overall security posture and better protecting its assets.

Findings (for each control)

Administrative **Control Information**
- Control ID: A.1 - Control Description: Develop a multi-tiered classification system with: clear categories (e.g., Public, Internal, Confidential, Highly Confidential), specific handling procedures for each level, visual indicators (watermarks, headers, footers), guidelines for conversion between classifications, regular review processes for reclassification. Train all personnel on proper classification and create decision trees to help employees determine appropriate classifications.

Analysis
The organization has a defined multi-tiered classification system with clear categories, handling procedures, and visual indicators. However, it lacks evidence of personnel training and has a coverage of 78%, which is below the 80% threshold required for Tier 3. The presence of decision trees and regular review processes supports a Tier 2 classification.

Tiering
Tier 2

Administrative **Control Information**
- Control ID: A.2 - Control Description: Establish formal processes that: document justification for access requests, require managerial approval for accessing sensitive information, implement time-limited access privileges, create formalized revocation procedures, maintain detailed access logs. Conduct quarterly access reviews to verify all access remains appropriate and necessary.

Analysis
The organization demonstrates proactive least-privilege management, real-time revocation, and robust logging and review mechanisms. All core elements of control A.2 are present, automated, and consistently applied, placing the organization in Tier 4. However, there is an opportunity to strengthen evidence collection for audit readiness.

Tiering
Tier 4

Administrative **Control Information**
- Control ID: A.3 - Control Description: Create comprehensive document management systems that: apply unique identifiers to all sensitive documents, track document version history, record distribution details, implement check-in/check-out procedures, set automatic expiration dates for sensitive materials, establish secure destruction protocols (including certificates of destruction). Deploy document management software that enforces these controls automatically. (SharePoint, Cavelo, Echo Mark)

Analysis
The organization meets the core requirements of the Repeatable level and incorporates several adaptive features. However, it lacks automatic expiration dates inside the DMS, advanced monitoring and tracking technologies, and a documented incident response process, limiting its maturity to Tier 3.

Tiering
Tier 3

Administrative **Control Information**
- Control ID: A.4 - Control Description: In addition to corporate data retention obligations, establish data retention policies that are optimal for employee activity reviews. Many documents are dynamic now such as Office 365 and Google Workspace documents. It might be necessary to capture document static copies whenever there is data transit.

Analysis
The organization has policies in place, captures dynamic documents, and has basic lifecycle management. However, gaps remain in legal consultation, automated destruction, and formal auditing/documentation of deletion processes, placing it in Tier 2.

Tiering
Tier 2

Governance **Control Information**

- Control ID: G.1 - Control Description: Establish someone is the organization as the ultimate authority and accountable for Trade Secret protection. This person may also be the cybersecurity delegated leader.

Analysis

No analysis is available for this control.

Tiering

None

Governance **Control Information**

- Control ID: G.2 - Control Description: Reporting on weekly, monthly or quarterly insider security metrics including data classification statistics, incident reporting, employee exit summaries, incentives, tabletop results, and progress indicators

Analysis

The organization tracks a broad set of insider-threat related metrics and reports them quarterly to the Executive Committee, including metrics like data classification coverage, DLP violations, and incident counts. However, the metrics lack comprehensiveness, notably missing incentive programs and tabletop result reporting. The organization performs trend analysis and benchmarking against FS-ISAC peers. Despite a robust reporting cycle, there's no clear evidence of iterative changes to measurement approaches based on review outcomes.

Tiering

Tier 3

Human Resource **Control Information**

- Control ID: H.1 - Control Description: Develop a comprehensive training program that: includes initial onboarding training on trade secret protection, delivers role-specific training for employees with greater access, provides quarterly refresher courses, uses scenario-based learning and real-world examples, tests comprehension through assessments, tracks completion and comprehension metrics, addresses social engineering awareness. Supplement formal training with regular communication through newsletters, posters, and other awareness materials.

Analysis

The organization has a comprehensive training program with annual delivery to all employees and role-specific tracks for various departments. Metrics are collected and tracked, including DLP violation rates and phishing simulation click rates. However, there are gaps in continuous improvement, formal social-engineering scenario training, and structured recognition/compensation for Security Champions. The training program is supported by multiple communication channels.

Tiering

Tier 3

Human Resource **Control Information**

- Control ID: H.2 - Control Description: Background checks should include inventor disclosure, github, social media, and signs of any criminal records.

Analysis

The organization's background check process covers several required areas like credit, criminal records, and social media reviews for sensitive roles. However, it omits inventor disclosure and GitHub reviews. Verification is conducted via a third-party vendor without independent research or separate investigative services. There's no evidence of continuous improvement or metrics to assess effectiveness.

Tiering

Tier 1

Human Resource **Control Information**

- Control ID: H.3 - Control Description: It's imperative that employees do not make the organization liable for receiving trade secrets from the new employees past employer. The employee must sign and agree not violate the past employees confidentiality obligations. Additionally the employee should list any IP they own that might be applicable before starting employment.

Analysis

The organization has a defined onboarding process that includes signing confidentiality and IP assignment agreements, and an HR review of prior employer obligations. However, there's no evidence of consistent enforcement or documentation of IP

disclosure reviews. Role-specific IP or trade-secret training is not provided beyond general security awareness training.

Tiering
Tier 2

Human Resource **Control Information**
- Control ID: H.4 - Control Description: Companies should be creative to support incentives for championing proprietary data protection and valuable IP. Incentives include rewards for process improvements, consistent awareness testing results, and creation of large amounts of classified proprietary data

Analysis
The organization has an incentive program, including the Quarterly Innovation Awards Program and the Security Champions Program, with monetary rewards, certificates, and gift cards. However, the program lacks a dedicated manager, formal governance, and additional recognition mechanisms like performance review integration. Continuous improvement is implied through quarterly CISO meetings but lacks systematic surveys or structured improvement cycles.

Tiering
Tier 2

Human Resource **Control Information**
- Control ID: H.5 - Control Description: Create thorough offboarding processes that: include exit interviews focused on confidentiality obligations, require signed acknowledgment of ongoing obligations, recover all company property and credentials, maintain detailed checklists for HR and IT departments, perform comprehensive access termination (including cloud services and third-party accounts), conduct forensic imaging of devices when appropriate, send reminder letters about confidentiality obligations. Implement different levels of exit procedures based on risk assessment of the departing employee. Implement standard reviews of the last 6 months of activity. If there are any suspicious activities, it may be necessary and advantageous to conduct this research before an exit interview commences.

Analysis
No analysis is available for this control.

Tiering
None

Human Resource **Control Information**
- Control ID: H.6 - Control Description: Establish a formalized program that: creates clear reporting channels for suspicious behavior, trains supervisors on warning signs, implements behavioral analytics to detect anomalies, conducts enhanced monitoring of high-risk positions, forms a cross-functional response team, develops investigation protocols, establishes remediation processes. Ensure the program balances security with employee privacy and workplace culture. Consider an anonymous reporting tool or whistleblower incentives.

Analysis
The organization has some elements of an insider threat program, such as reporting channels and a response team, but lacks formal documentation, behavioral analytics, enhanced monitoring, and remediation processes. The program is rated Tier 0 – Partial to None due to the absence of key components and continuous improvement processes.

Tiering
0

Incident Response **Control Information**
- Control ID: I.1 - Control Description: Develop a specialized plan for trade secret incidents that: creates a dedicated response team with legal, IT, HR, and executive representation, establishes containment procedures to limit exposure, defines escalation paths based on severity, documents evidence collection requirements, includes communication templates for various scenarios, outlines coordination with law enforcement, details remediation requirements. Conduct regular tabletop exercises to test the plan's effectiveness. Make sure to quarantine and create discrete communication lines if the insider may be in this response group

Analysis
The organization has a stated plan and a dedicated response team, but lacks a formal

plan document and comprehensive procedures. The plan is considered Tier 2 – Repeatable because it meets the criteria of having a dedicated team, some procedures, and tabletop exercises, despite the lack of full documentation and regular reviews.

Tiering
2

Incident Response **Control Information**
- Control ID: I.2 - Control Description: Build forensic capabilities that: maintain appropriate tools for evidence collection, establish chain of custody procedures, deploy enhanced logging on critical systems, create secure evidence storage facilities, train key personnel on forensic principles, maintain relationships with external forensic experts, develop templates for preservation notices. Implement automated forensic collection capabilities for critical security events.

Analysis
The organization demonstrates structured forensic capabilities with tools, trained personnel, and documented processes, including a legal-reviewed chain-of-custody procedure. However, it lacks automated forensic collection for critical security events and has incomplete validation practices, resulting in a Tier 3 – Adaptive rating.

Tiering
3

Incident Response **Control Information**
- Control ID: I.3 - Control Description: Prepare for potential legal action: document all trade secret protection measures, maintain evidence of reasonable steps taken, prepare templates for cease and desist letters, establish relationships with specialized IP litigation firms, develop criteria for pursuing legal remedies, create procedures for emergency injunctive relief, establish valuation methodologies for trade secrets. Review and update preparation annually with legal counsel.

Analysis
The organization has begun documenting some trade secret protection measures, such as using SharePoint with DLP and Azure Information Protection, but lacks specificity and formal relationships with IP litigation firms, legal templates, and valuation

methodologies. It is rated Tier 1 – Risk Informed for meeting the baseline effort but lacking key components for higher maturity.

Tiering
1

Legal **Control Information**
- L.1 - Develop tailored confidentiality agreements for different stakeholders (employees, contractors, vendors, partners). Include specific language identifying: clear definition of what constitutes confidential information, specific obligations for handling and protecting information, duration of confidentiality obligations (extending beyond employment/relationship), consequences of breach, return/destruction of confidential information upon termination. Regularly review agreements with legal counsel to ensure they remain enforceable in all relevant jurisdictions.

Analysis
The organization demonstrates some tailoring of confidentiality agreements for employees but lacks separate agreements for contractors, vendors, and partners. The agreements include some core content elements like liquidated damages and indefinite trade-secret protection, and they have been reviewed by external counsel. However, there are significant gaps in stakeholder coverage, precise content, and advanced enforcement provisions. The organization is placed in Tier 1 due to a total score of 5 points from the scoring rubric.

Tiering
Tier 1

Legal **Control Information**
- L.2 - Draft enforceable non-compete agreements that: define reasonable geographic limitations, set appropriate time restrictions (typically 1-2 years), specifically identify prohibited competitive activities, offer consideration (something of value) in exchange for the restriction, include provisions addressing inevitable disclosure concerns. Customize agreements based on employee role and access to sensitive information. Verify compliance with local laws, as enforceability varies significantly by jurisdiction.

Analysis

The organization has non-compete agreements in place for 14.5% of its workforce, tailored by role and jurisdiction, but lacks documented compliance checks with local laws and specific provisions like geographic limitations and prohibited competitive activities. The organization demonstrates a basic understanding of non-compete agreements but lacks depth in key areas, resulting in a Tier 1 maturity level with a total score of 5.

Tiering

Tier 1

Legal **Control Information**

- L.3 - Require all employees and contractors to sign agreements that: clearly establish company ownership of all intellectual property developed during employment, include "work for hire" provisions, cover inventions, ideas, processes, and improvements, address potential rights to pre-existing intellectual property, establish reporting requirements for new innovations.

Analysis

The organization has comprehensive IP agreements with "work for hire" provisions and mandatory pre-existing IP disclosure. Employees regularly acknowledge IP obligations through annual training, and there is robust documentation of employee-created IP. The organization meets all five assessment criteria at a level aligning with Tier 3 (Adaptive).

Tiering

Tier 3

Legal **Control Information**

- L.4 - The ability to re-screen employees with the same vigor as pre-employment is powerful tool to both encourage good behavior, but also alert on drastic life changes.

Analysis

No analysis is provided for this control.

Tiering

None

Physical **Control Information**

- P.1 - Establish layered physical security: deploy electronic access control systems with unique credentials, install CCTV monitoring with 90+ days of footage retention, create mantrap entries for highly sensitive areas, implement visitor management systems with escort requirements, install tamper-evident seals on sensitive equipment, conduct regular security sweeps for unauthorized devices, establish clear desk and clear screen policies. Document physical security measures to demonstrate reasonable protections in case of litigation.

Analysis

The organization satisfies core Tier 2 criteria with electronic access control, 90-day CCTV retention, visitor management, and documentation of security measures. Mantrap entries are implemented for two data centers, meeting the "some advanced features" requirement. However, the lack of tamper-evident seals, regular unauthorized-device sweeps, and formal role-based access or simulation exercises prevents the organization from reaching Tier 3.

Tiering

Tier 2

Physical **Control Information**

- Control ID: P.2 - Control Description: Develop comprehensive disposal procedures: deploy cross-cut or micro-cut shredders (at minimum DIN Level P-4), contract with certified destruction vendors for bulk materials, maintain chain of custody documentation, ensure witnessed destruction with certificates, implement secure wiping protocols (NIST 800-88 compliant) for electronic media, deploy degaussing equipment for magnetic media, establish physical destruction requirements for end-of-life hardware. Conduct regular audits of disposal practices to ensure compliance.

Analysis

The organization has implemented disposal procedures for paper, hard drives, and electronic media, using certified vendors and NIST-compliant wiping. They have a vendor audit program but lack internal audits, policy reviews, and training records. The practices are mostly consistent with Tier 2, but there are gaps in tailoring disposal methods to data sensitivity and in continuous improvement mechanisms.

Tiering
Tier 2

Technical **Control Information**
- Control ID: T.1 - Control Description: Use data classification tools that classify data according the schema above. Privacy data is typically found using regex based expression given its uniform value. Proprietary data may be manually applied tagging, but also using contextual language models that identify more common documents such as legal, financial, and research documents.

Analysis
The organization uses Microsoft Purview Information Protection for automated classification and manual tagging for high-sensitivity documents. While they report metric improvements and some governance through data stewards, they lack formal governance structures, integration with other security processes, and leadership initiatives for evaluating new technologies, aligning with Tier 1.

Tiering
Tier 1

Technical **Control Information**
- Control ID: T.10 - Control Description: Establish visual warnings (watermarks on critical documents), access review summary emails, and pop-ups (toasts) that remind or warn users of the mishandling of sensitive data. Tools such as Harmonics Security and the Enterprise Managed browser may have this functionality. Also overlaps with DRM

Analysis
The organization does not have visual warnings, pop-up deterrents, or summary review emails in place, despite using Microsoft Purview for classification. They demonstrate basic awareness through manual reviews and a user-feedback loop but lack a deterrent system, aligning with Tier 1.

Tiering
Tier 1

Technical **Control Information**
- Control ID: T.2 - Control Description: Use an asset inventory tool to audit the classification of data across the enterprise and consistently confirm scanning and compliance. Account for shadow IT or unsanctioned data access or exit points

Analysis
The organization uses ServiceNow IT Asset Management and Netskope CASB for asset inventory and shadow-IT detection, respectively. While they have reasonable coverage and some formal processes, they lack automated data classification integration, regular review cycles for shadow-IT detection, and clear role definitions, placing them at Tier 2.

Tiering
Tier 2

Technical **Control Information**
- Control ID: T.3 - Control Description: Deploy enterprise DLP solutions that: monitor and filter outbound communications (email, web, FTP), detect sensitive data patterns using content inspection, block unauthorized transmissions of protected data, log attempted policy violations, integrate with email gateway and web proxy servers. Configure policies to identify trade secret information using keyword lists, regular expressions, and fingerprinting of sensitive documents. Many of these functions may overlap a managed browser

Analysis
The organization has deployed Forcepoint DLP with reasonable coverage across email, web, endpoints, and USB. While they have basic content inspection and monitoring, they lack fingerprinting, formal integration evidence, automated response playbooks, and comprehensive KPI tracking, resulting in a Tier 2 classification.

Tiering
Tier 2

Technical **Control Information** - Control ID: T.4 - Control Description: Implement a layered encryption strategy: deploy full-disk encryption for all endpoints (laptops, desktops, mobile devices), use file-level encryption for sensitive documents (AES-256 or higher), ensure encrypted communications channels (TLS 1.3, VPN), implement

encrypted databases for sensitive information, establish strong key management procedures with appropriate key rotation. Utilize hardware security modules (HSMs) for cryptographic key storage and operations. **Analysis** The organization shows awareness and intent to implement a layered encryption strategy with some foundational controls in place, such as BitLocker, TDE, TLS 1.3, VPN, and FDE. However, there is a lack of evidence to confirm that these controls are fully operational and consistently applied. Key management practices are described with reasonable detail, but there is no supporting evidence. The absence of file-level encryption for documents and post-quantum measures are noted as gaps. **Tiering** Tier 1

Technical **Control Information** - Control ID: T.5 - Control Description: Deploy multi-layered access controls: implement role-based access control (RBAC) frameworks, require multi-factor authentication for all sensitive systems, create segregated network zones for critical information, employ privileged access management (PAM) solutions, implement just-in-time access for highly sensitive systems, conduct regular entitlement reviews. Configure systems to automatically revoke access after periods of inactivity. **Analysis** No analysis is available for this control as the 'analysis' field is empty. **Tiering** None

Technical **Control Information** - Control ID: T.6 - Control Description: Deploy DRM solutions that: apply persistent protection to sensitive files, control viewing, editing, copying, and printing permissions, enable remote wiping of protected documents, maintain audit trails of document access and usage, expire document access automatically, prevent screen capture when viewing protected materials. Integrate DRM with authentication systems to provide seamless user experience while maintaining protection. **Analysis** The organization has implemented Azure Information Protection (AIP) for sensitive documents with features like view-only, no-print, expiration dates, remote revocation, and screen-capture blocking. However, there is a lack of evidence for integration with authentication systems, metrics, monitoring, or formal processes governing DRM usage. Persistent protection for copied or moved files is not demonstrated. **Tiering** Tier 1

Technical **Control Information** - Control ID: T.7 - Control Description: The use of enterprise managed browser can be a critical barrier to preventing uploads to non-sanctioned domains, files sharing services, email and more. These advanced browser

may also limit screen shots, copy/paste, and other functions. Enterprise browsers are critical to limited corporate access to outside domains. **Analysis** The organization uses Managed Microsoft Edge with Zscaler web filtering across 100% of the workforce on managed devices. Policies exist and are generally enforced, but there is a lack of evidence, exclusive use, legal backing, comprehensive DLP integration, and screen-capture controls. Weekly web analytics reviews imply regular monitoring, but the scope and detail are not described. **Tiering** Tier 2

Technical **Control Information** - Control ID: T.8 - Control Description: Create defense-in-depth with: next-generation firewalls with application awareness, network segmentation with security zones, encrypted VPN access for remote workers, intrusion detection/prevention systems, data flow monitoring, regular vulnerability scanning, web application firewalls for customer-facing applications. Implement advanced threat protection solutions that can detect anomalous data movement patterns. **Analysis** The organization reports using Palo Alto NGFWs, a 6-zone segmentation strategy, and Darktrace for anomaly detection. However, there is a lack of detailed network diagram, configuration details, and evidence of how these components are integrated. Some specific security controls like encrypted VPN, dedicated IDPS, and data-flow monitoring tools are not detailed. Advanced threat protection is not confirmed to be tuned for anomalous data movement patterns. **Tiering** Tier 1

Technical **Control Information**
- T.9
- UEBA and the use of other logging event and correlation tools (Sometimes included in SIEM) to create rules and alerts based on confidential file movements. Creating baselines and reviewing anomalous activity as it occurs

Analysis
The organization has achieved Tier 3 ("Adaptive") for its UEBA implementation, with a fully integrated UEBA and SIEM solution, advanced rule creation and alerting, some insider-threat analysis, and regular retrospectives for continuous improvement. Key strengths include comprehensive deployment with dedicated monitoring, advanced rule logic, and ongoing fine-tuning. However, areas for improvement include documenting detailed playbooks, showing evidence of successful threat hunting, integrating UEBA

alerts into incident-response workflows, refining alert thresholds, and formalizing the continuous improvement process.

Tiering
Tier 3

Conclusion & Recommendations

Description

The organization demonstrates a varied maturity level across different controls, with some achieving Tier 2 (Repeatable) and others reaching Tier 3 (Adaptive) or Tier 4 (Optimizing). The overall strength lies in the defined processes and some level of automation observed in controls such as data classification, access management, and incident response. However, weaknesses are evident in the lack of comprehensive documentation, insufficient training and awareness programs, and the absence of advanced security measures in certain areas.

Areas to Improve

1. **Enhance Documentation and Evidence Collection**: Many controls lack comprehensive documentation and tangible evidence to support their maturity levels. Ensuring that all processes are well-documented and evidenced is crucial.
2. **Improve Training and Awareness**: Controls related to human resources, such as training programs and background checks, show gaps in role-specific training, continuous improvement, and formal recognition programs.
3. **Implement Advanced Security Measures**: Several technical controls, such as data loss prevention, encryption, and user and entity behavior analytics (UEBA), require enhancements to move to higher maturity tiers. This includes implementing advanced detection capabilities, integrating with other security processes, and automating responses.

4. **Strengthen Governance and Compliance**: Governance controls, including reporting metrics and legal agreements, need improvement in comprehensiveness, iteration on measurement approaches, and integration into security strategies.

Tasks to Complete

1. **Develop a Comprehensive Training Curriculum**: Include role-specific training, scenario-based learning, and continuous improvement mechanisms to enhance the maturity of human resource controls.
2. **Implement Automated Forensic Collection and UEBA**: Enhance incident response capabilities by deploying automated forensic collection for critical security events and refining UEBA rules and alerts.
3. **Expand Data Classification and DLP**: Extend automated or semi-automated classification to a broader range of documents and integrate classification outputs with DLP, access control, and monitoring systems.
4. **Formalize Governance and Reporting**: Establish a dedicated governance council, enhance metric comprehensiveness, and tie metric outcomes to policy updates and security strategy adjustments.
5. **Conduct Regular Reviews and Tabletop Exercises**: Regularly review and update incident response plans, conduct tabletop exercises, and track metrics to drive continuous improvement in incident response and other critical areas.

By addressing these areas and completing the outlined tasks, the organization can improve its overall maturity level, strengthen its security posture, and better protect its trade secrets and intellectual property.