[redacted] Infrastructure Partners Portfolio Security Overview

Assessment Overview

Project Objective

Objectives of this Exercise:

- Identify and evaluate controls across three key areas:
  - Management Controls – Management of the information technology security system and the management and acceptance of risk.
  - Operational Controls – Security methods focusing on mechanisms implemented and executed primarily by people, including media safeguards and inventory controls.
  - Technical Controls – Hardware and software controls provide automated protection to the system or applications.
- Collect, scan, and assess identity management, security groups/ACLs, isolation and segregation mechanisms, web application firewall configs, dependency versions, logging and accounting mechanisms, data-at-rest and data-in-transit cryptography, access control mechanisms, and more.
- Outline the potential impact and severity of each vulnerability, weakness, and risk, including observed deviations from standard information security best practices and principles.
- Present information that identifies the root causes behind the vulnerabilities, weaknesses, and risks identified in the assessment while conveying a message of how those problems relate to the inherent security posture.
- Provide a full due diligence report, including information such as vulnerability/weakness/risk details, risk mitigation recommendations, assessment methods, information system statistics, and more.

Cybersecurity Risk Assessment Methodology

Abacus Group's cybersecurity risk assessment methodology is modeled from the standards outlined in NIST SP 800-115, Technical Guide to Information Security Testing and Assessment and CIS. The methodology includes four phases: Planning, Data Collection, Analysis, and Reporting. The process of this assessment aggregates and analyzes huge amounts of data and security findings across all analyzed technologies and services. The assessment methodology systematically organizes, prioritizes, and ranks only the most meaningfully impactful from the perspective of both the magnitude of impact as well as ease of exploitation, as outlined in section of this report.

Phase 1: Planning
The Planning phase involves determining the scope of the assessment, identifying the in-scope cloud platforms, and defining the objectives. This phase also outlines the assessment approach, defines the roles and responsibilities of the assessment team, and establishes the timeline for the assessment.

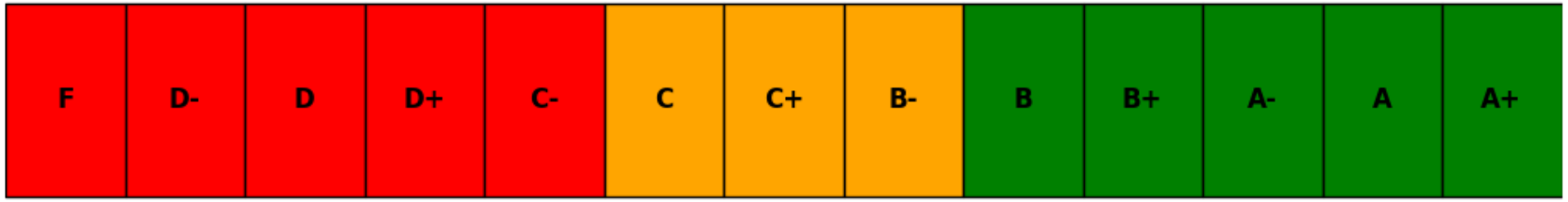
Phase 2: Data Collection
The Data Collection phase involves gathering information about the cloud platforms in scope, including their configuration, architecture, and security controls. This phase also includes identifying potential vulnerabilities, threats, and risks associated with the cloud platforms.

Phase 3: Analysis
The Analysis phase involves reviewing and analyzing the data collected in the previous phase. This phase assesses the effectiveness of the security controls in place and identifies any gaps or weaknesses in the security posture of the cloud platforms. During all analyses specific care is taken to understand the context of the environment, the presence of any compensating controls, and the practical impact to the organization.

Phase 4: Reporting
The Reporting phase involves documenting the findings of the assessment. This phase includes creating a comprehensive report that summarizes the assessment results, identifies improvement areas, and provides recommendations for enhancing the security posture of the cloud platforms.

Executive Overview – RAG Status

Organization Reviewed	Grade Assessed
[redacted]	B
[redacted]	A
[redacted]	[redacted]
[redacted]	B+
[redacted]	C
[redacted]	[redacted]
[redacted]	C
[redacted]	B
[redacted]	B



Executive Summary – [redacted] (1 of 2)

The observed cybersecurity posture for [redacted] is adequate, though there are opportunities for improvement. Currently, [redacted] has a more than reasonable security posture when considering the business context.

Key Recommendations

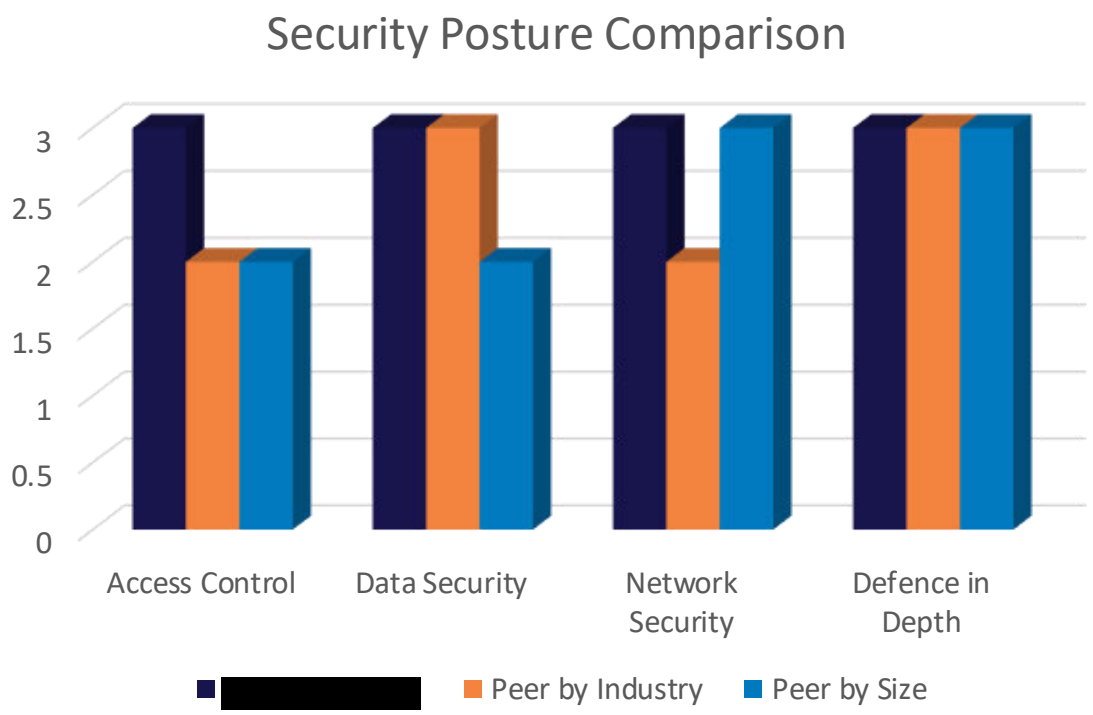
Based on the results and the context identified during this assessment, Abacus Group's vCISO team recommends the following key initiatives for 2025.

Recommendation: Implementation of a Password Manager

- Though few systems require authentication across the organization's team members, it is highly recommended that [redacted] implement a password management solution. With such a solution, team members can safely create, store, and use passwords for organizational systems.
- The absence of this solution introduces a number of inherent risks to the organization, including supporting poor password habits. Without a centralized and secure storage location for passwords, users may be tempted to reuse passwords, use passwords that are easy to remember, or insecurely store passwords in a text file or spreadsheet. All of these habits substantially increase the potential for account compromise.

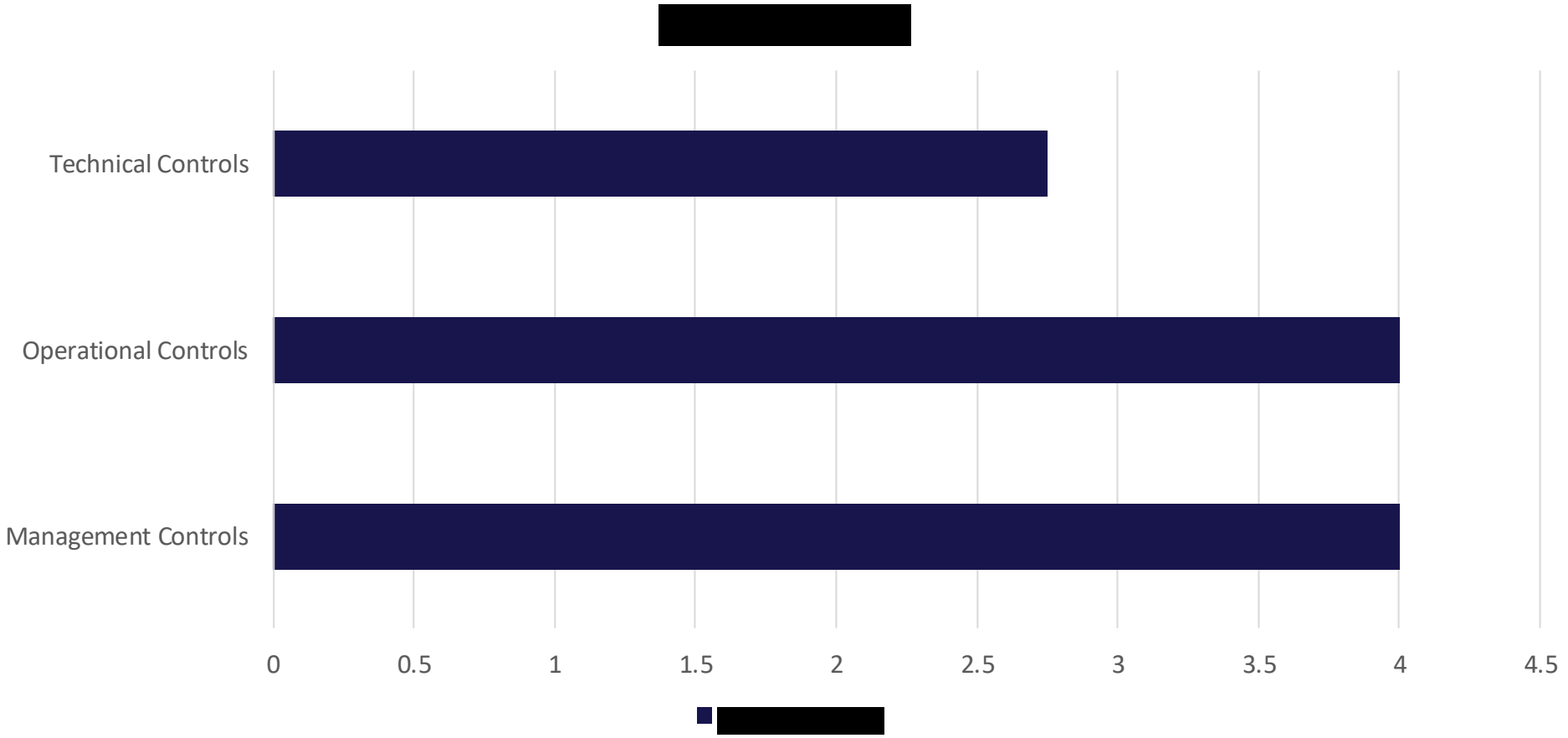
Recommendation: Implement Microsoft 365

- Considering the organization's size and work environment (many team members working remotely), it is Abacus Group's recommendation for Skyway Tower to implement the Microsoft 365 suite of tools. With a Business Premium license, which is $22 a month (if paid annually), [redacted] would have access to many of the tools and features of the Microsoft 365 ecosystem.
  - Entra ID, which can be used for identity management, authentication and access controls, and other user-based security controls.
  - Intune, which can be used for device management, device configuration control, and device compliance control.
  - Defender, which can be used for additional email security control hardening.
  - Purview, which can be used for Data Loss Prevention (DLP).
  - Tools such as Word, PowerPoint, Excel, and OneNote would also be available to the organization.



0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Executive Summary – [redacted] (2 of 2)



Management Controls – Management of the information technology security system and the management and acceptance of risk.

Operational Controls – Security methods focusing on mechanisms implemented and executed primarily by people, including media safeguards and inventory controls

Technical Controls – Hardware and software controls provide automated protection to the system or applications.

0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Assessed Overall Cybersecurity Grade: **B**

Executive Summary – [redacted] (1 of 2)

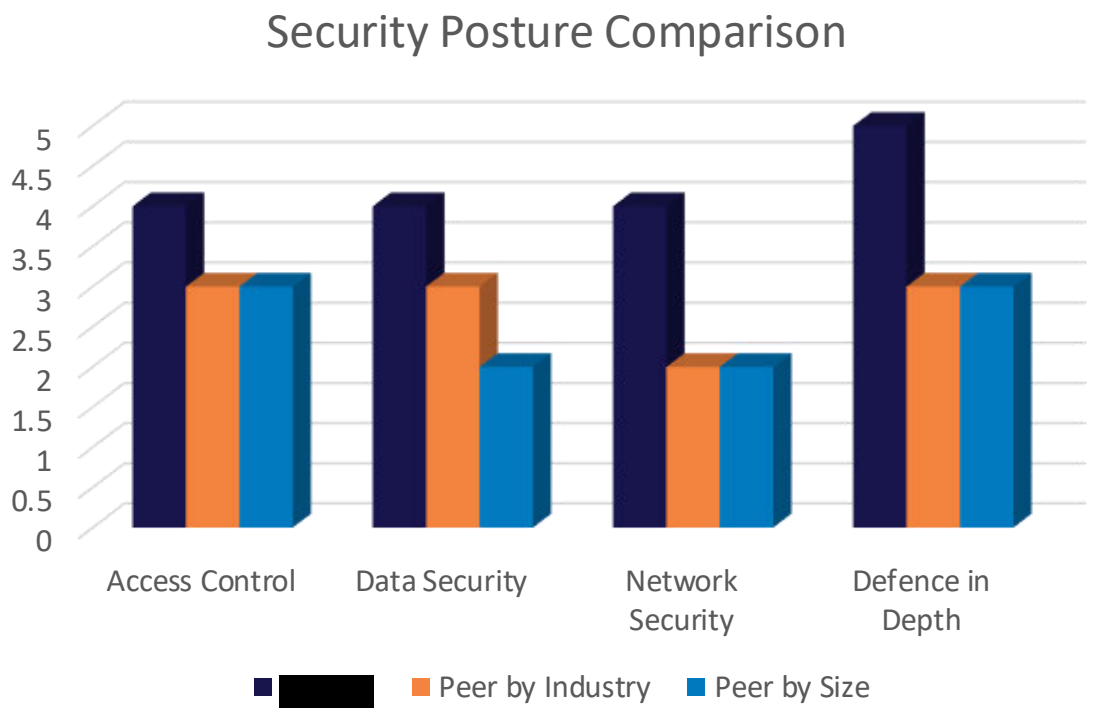
The observed cybersecurity posture for [redacted] is both operationally effective and highly secure. From Abacus Group's vantage point, [redacted] demonstrated robust and mature cybersecurity practices. This holds true even at the enterprise level.

Key Recommendations

Based on the results and the context identified during this assessment, Abacus Group's vCISO team recommends the following key initiative for 2025 and onward.

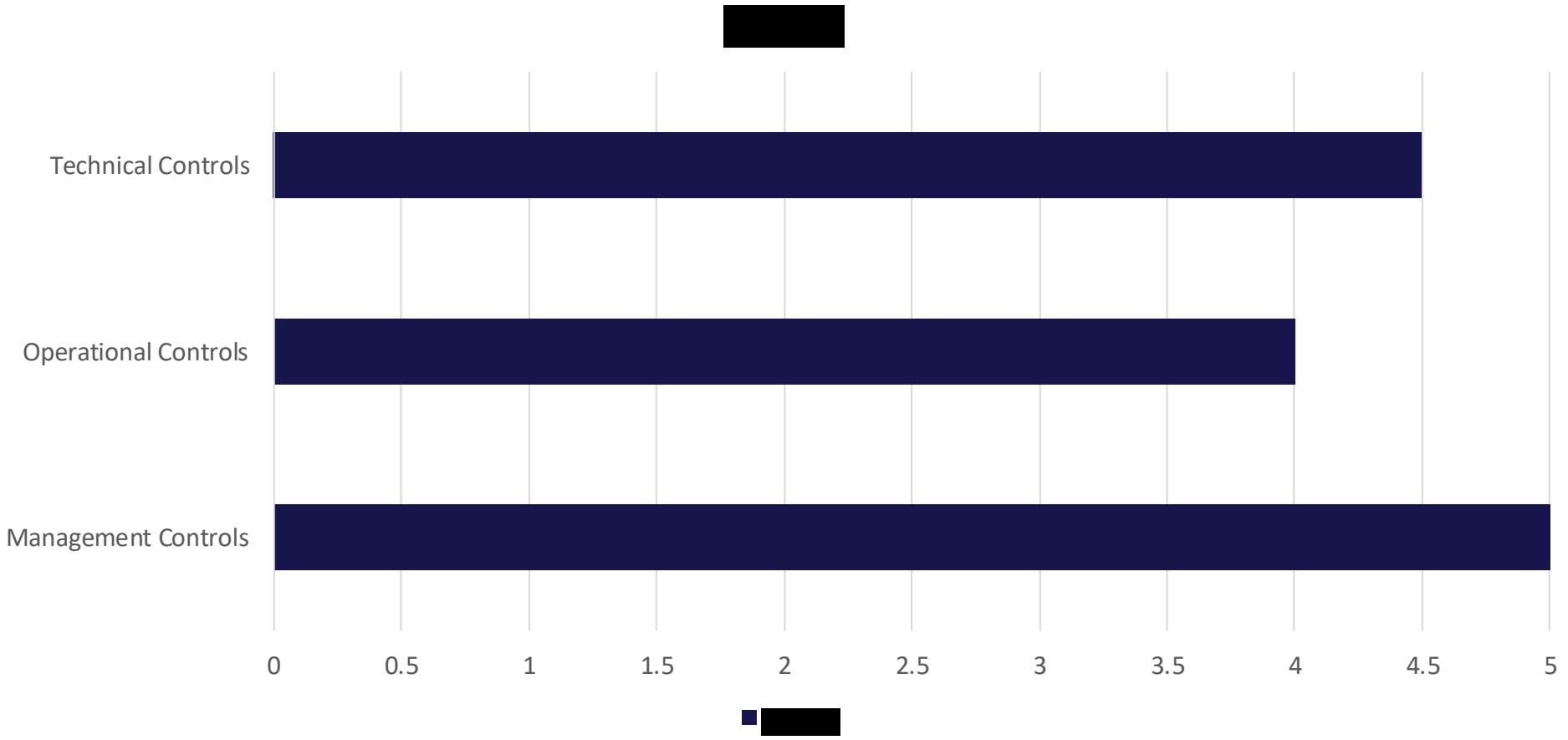
Recommendation: Implementation of a cross-functional cloud security and infrastructure team.

- During the review of Azure, Abacus Group security engineers were able to review specific resources, network groups, connections between resources, and high-level infrastructure configurations. However, though Abacus Group was able to execute an extensive review of Azure, Abacus Group lacks the nuanced understanding of how certain functions are built, maintained, and leveraged in the context of [redacted] operations. Therefore, a lot of the security recommendations were established with general best practice considerations.
- With this in mind, and of course with the consideration that there is not already a multi and cross-functional team already established, it is Abacus Group's recommendation to establish this team for cloud and infrastructure security. With such a team, [redacted] would benefit from routine audits of resources, increased understanding of the configurations, as the organizational context would be more readily available, and already established permissions and access to critical information and infrastructure.
- If a team already exists, then this recommendation can be foregone. If it is desired to outsource this team, which is perfectly acceptable, then it is recommended that this team be familiarized with [redacted] operations. This relationship should be established over many months for the best outcome. Abacus Group recognizes that this will likely incur much deliberation, especially funding and establishing such a team would need to be approved across many internal departments. This recommendation remains, as with [redacted] expansive cloud environment, a security incident could cause significant disruptions that may outweigh the costs and efforts associated with establishing and maintaining the aforementioned team. Finally, having such a team would give [redacted] the ability to reduce costs where possible and limit the attack surface by deprecating assets that are not needed.



0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Executive Summary – [redacted] (2 of 2)



Management Controls – Management of the information technology security system and the management and acceptance of risk.

Operational Controls – Security methods focusing on mechanisms implemented and executed primarily by people, including media safeguards and inventory controls

Technical Controls – Hardware and software controls provide automated protection to the system or applications.

0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Assessed Overall Cybersecurity Grade: **A**

Executive Summary – [redacted] (1 of 2)

The observed cybersecurity posture for [redacted] is both operationally effective and highly secure. From Abacus Group's vantage point, [redacted] demonstrated robust and mature cybersecurity practices.

Key Recommendations

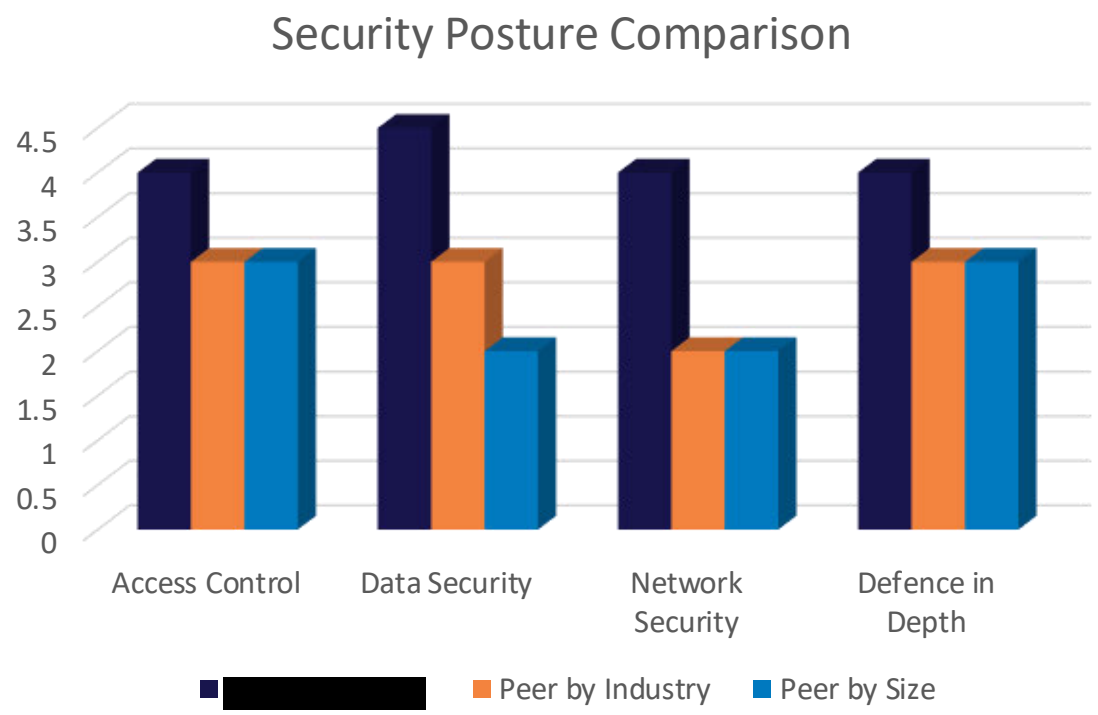
Based on the results and the context identified during this assessment, Abacus Group's vCISO team recommends the following key initiatives for 2025.

Recommendation: Implementation of a corporate password management solution.

- During the interview question portion of the cybersecurity risk assessment, Abacus Group discovered that there was no corporate password management solution in place for [redacted] However, immediate discussions were held regarding the importance of implementing one, and the Point of Contact (PoC) expressed intent to move forward with selecting and deploying a solution.
- The absence of a centralized password manager increases the risk of poor credential hygiene, such as password reuse, weak passwords, and insecure storage practices. Once a solution is selected, it should be rolled out organization-wide and made mandatory to ensure consistent, secure password practices across all teams and systems.

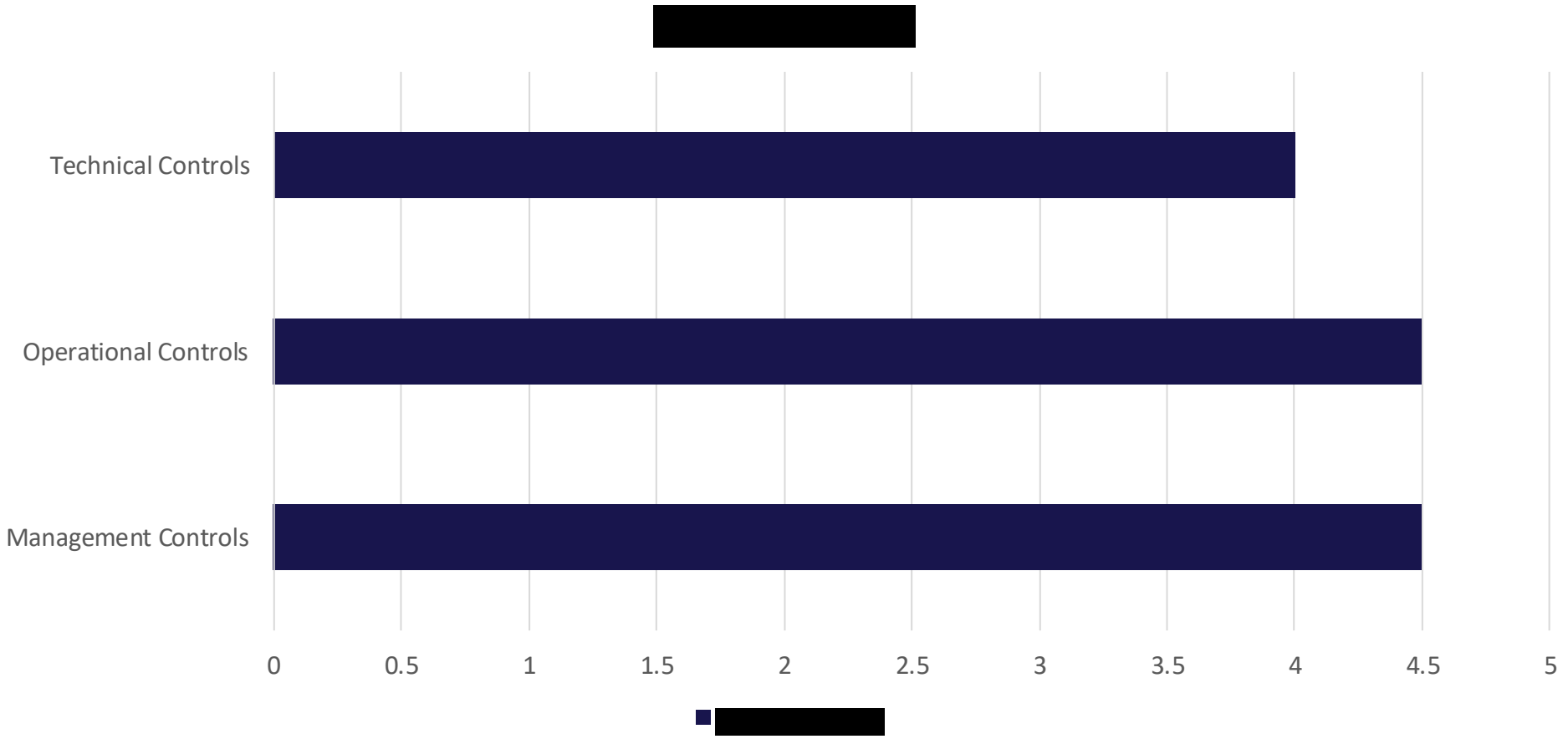
Recommendation: Centralized domain management.

- Abacus Group observed that [redacted] is currently operating across multiple domains for user identity and access across various systems. This fragmented structure introduces complexity in managing user accounts, enforcing consistent security policies, and maintaining visibility across the environment.
- To address this, Abacus Group recommends consolidating all users under a single, centralized domain. This approach would streamline identity management, simplify access control, and enable consistent enforcement of security measures such as Multi-Factor Authentication (MFA). Continuing to operate across multiple domains increases the risk of misconfigurations, inconsistent policy enforcement, and administrative overhead. A unified domain structure would support a cleaner, more secure, and more manageable environment organization-wide.



0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Executive Summary – [redacted] (2 of 2)



Management Controls – Management of the information technology security system and the management and acceptance of risk.

Operational Controls – Security methods focusing on mechanisms implemented and executed primarily by people, including media safeguards and inventory controls

Technical Controls – Hardware and software controls provide automated protection to the system or applications.

0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Assessed Overall Cybersecurity Grade: **A-**

Executive Summary – [redacted] (1 of 3)

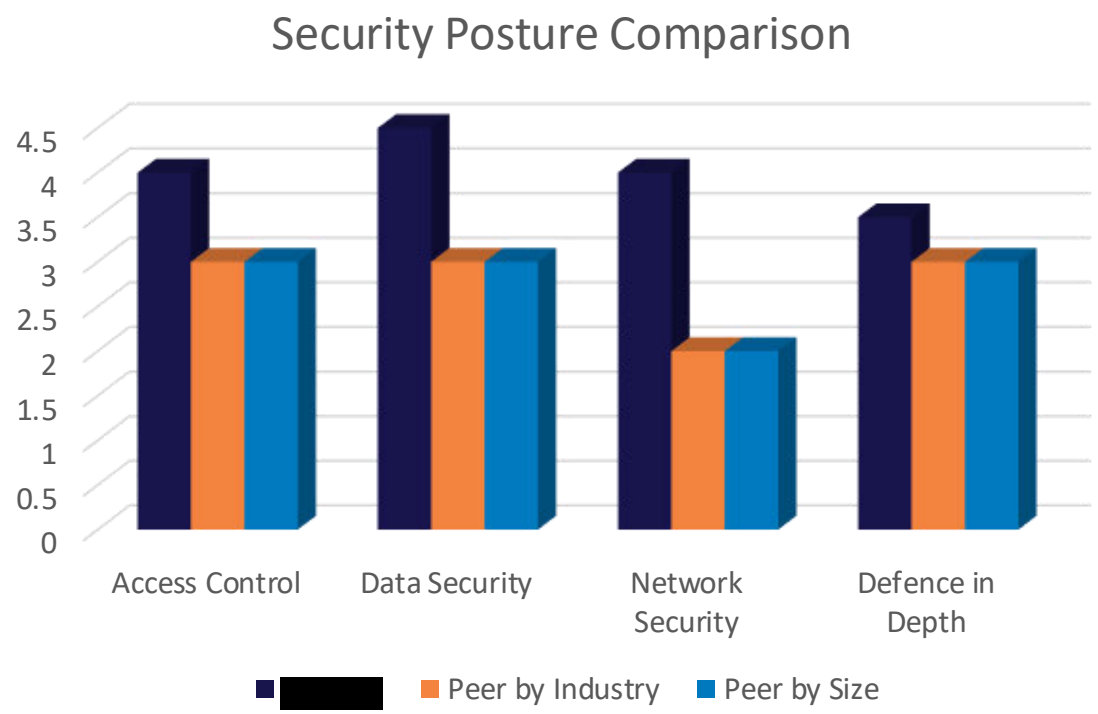
The observed cybersecurity posture for [redacted] is both operationally effective and secure. From Abacus Group's vantage point, [redacted] demonstrated robust and mature cybersecurity best practices.

Key Recommendations

Based on the results and the context identified during this assessment, Abacus Group's vCISO team recommends the following key initiatives for 2025 and onward.

Recommendation: Implement a routine audit and review of both devices and users (status and roles/permissions).

- During the analysis of Entra, Abacus Group identified well over 200 privileged role assignments. Additionally, through the review of Entra, Intune, SentinelOne, and even Duo Admin, Abacus Group identified discrepancies in device counts. While it is understood that device counts may fluctuate from platform to platform, especially when considering Duo Admin, Abacus Group again identified that corporate device counts were dissimilar.
- In such an environment, the combination of over-privileged users and device mismanagement presents a significant security risk. Without strong identity governance and endpoint hygiene, enterprises risk cascading failures across their infrastructure, especially in hybrid or cloud-connected environments where visibility and control are already complex.
- It is Abacus Group's recommendation to conduct an audit of both devices and users and ensure that this audit is done routinely. This will eliminate unnecessary permissions, remove inactive users, and properly manage all necessary endpoints.



0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Executive Summary – [redacted] (2 of 3)

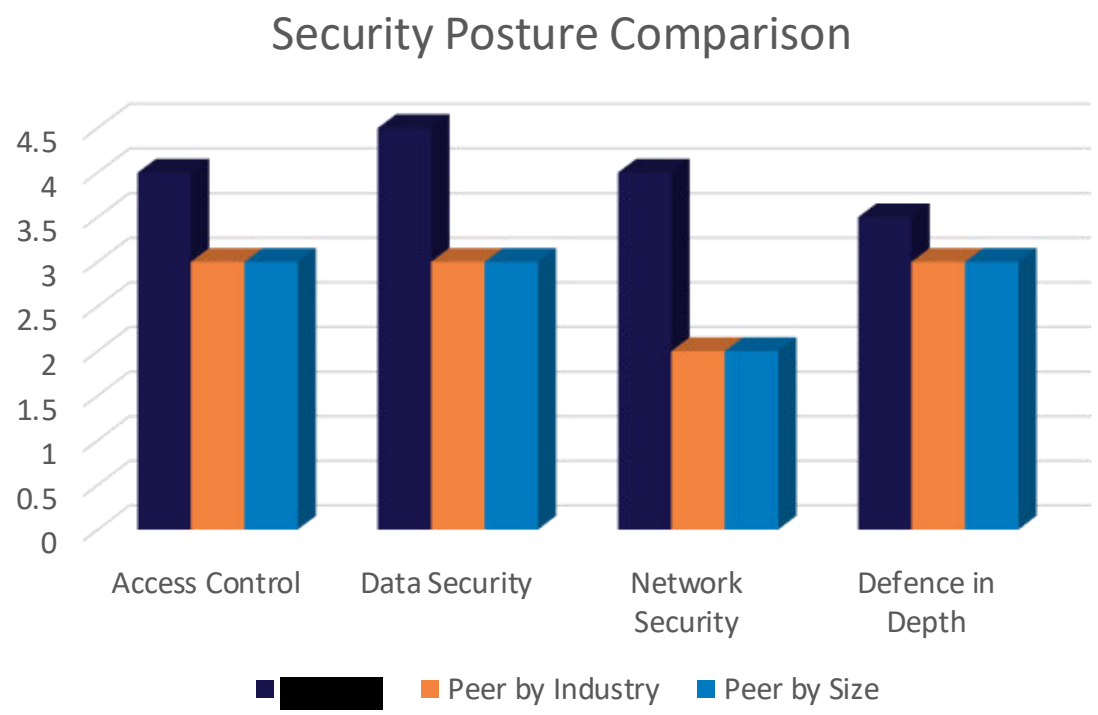
The observed cybersecurity posture for [redacted] is both operationally effective and secure. From Abacus Group's vantage point, [redacted] demonstrated robust and mature cybersecurity best practices.

Key Recommendations

Based on the results and the context identified during this assessment, Abacus Group's vCISO team recommends the following key initiatives for 2025 and onward.

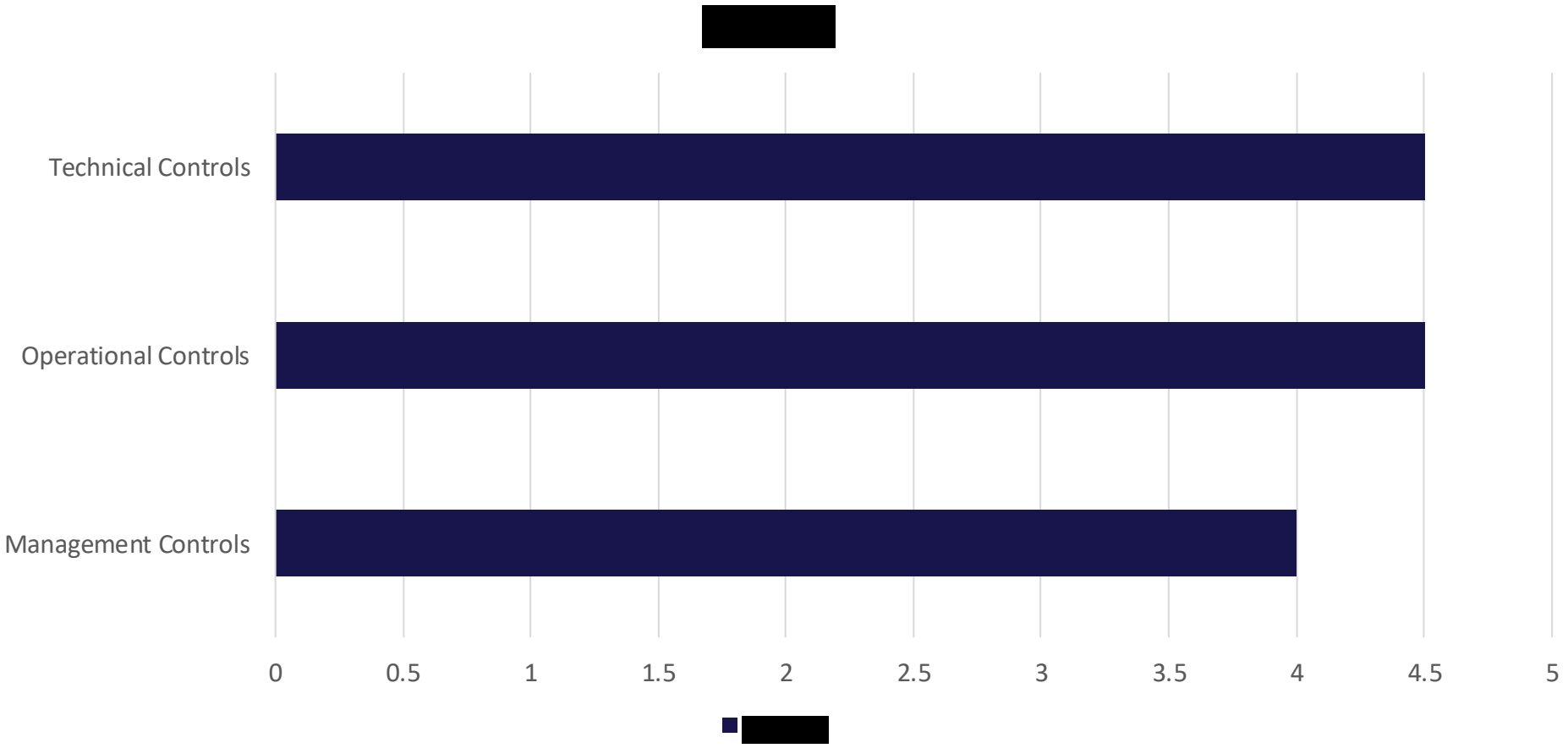
Recommendation: Identify areas for layered defense.

- During the review of Entra, Abacus Group identified few conditional access policies. Though the current configuration is acceptable, especially when considering the various authentication flows, it is Abacus Group's belief that additional protections could be layered onto the current slate of policies. Compliant devices and location-based policies would be especially helpful.
- The above is just used as an example to drive the point that layers of defense are critical for enterprise organizations with numerous endpoints and users. Some such layers do not even have to be integrated within the systems currently in place. One such example is domain monitoring, which could be employed to detect, track, and even remove domains that impersonate or misuse [redacted] brand.
- While layered security strategies come with upfront costs, they are often far less expensive than the fallout from a cyber breach. It is Abacus Group's general recommendation to explore additional protections, as the cost of prevention is almost always lower than the cost of recovery.



0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Executive Summary – [redacted] (3 of 3)



Management Controls – Management of the information technology security system and the management and acceptance of risk.

Operational Controls – Security methods focusing on mechanisms implemented and executed primarily by people, including media safeguards and inventory controls

Technical Controls – Hardware and software controls provide automated protection to the system or applications.

0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Assessed Overall Cybersecurity Grade: **B+**

Executive Summary – [redacted] (1 of 2)

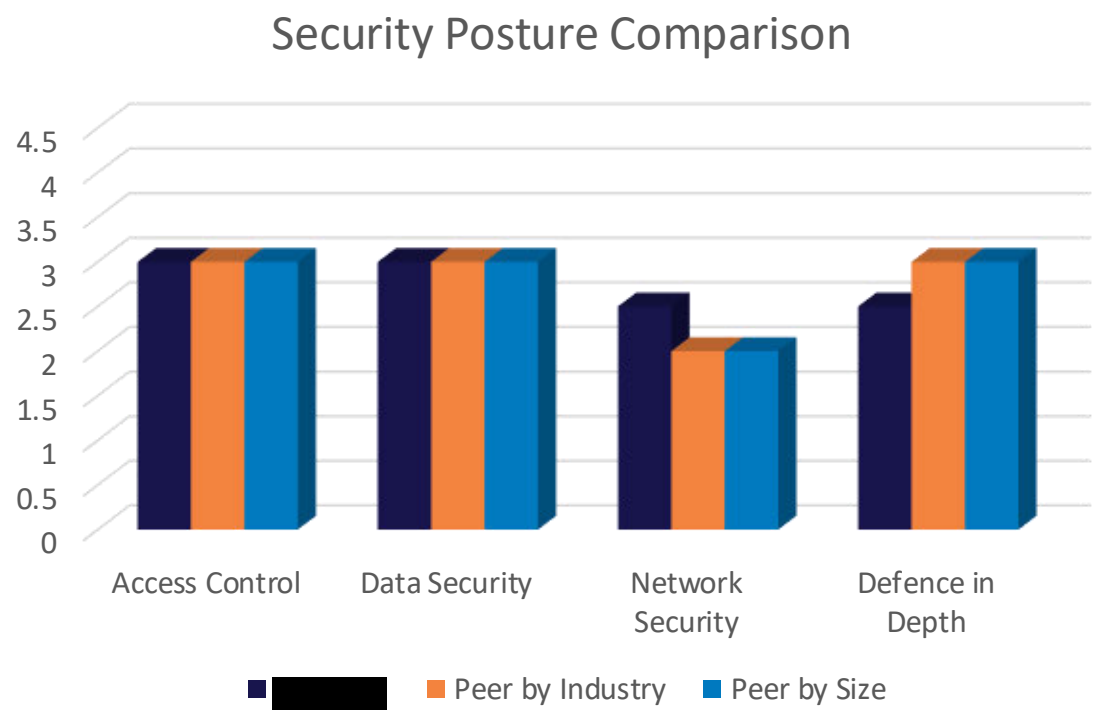
The observed cybersecurity posture for [redacted] could use improvement. From Abacus Group's vantage point, [redacted] demonstrated moderately effective security practices.

Key Recommendations

Based on the results and the context identified during this assessment, Abacus Group's vCISO team recommends the following key initiatives for 2025 and onward.

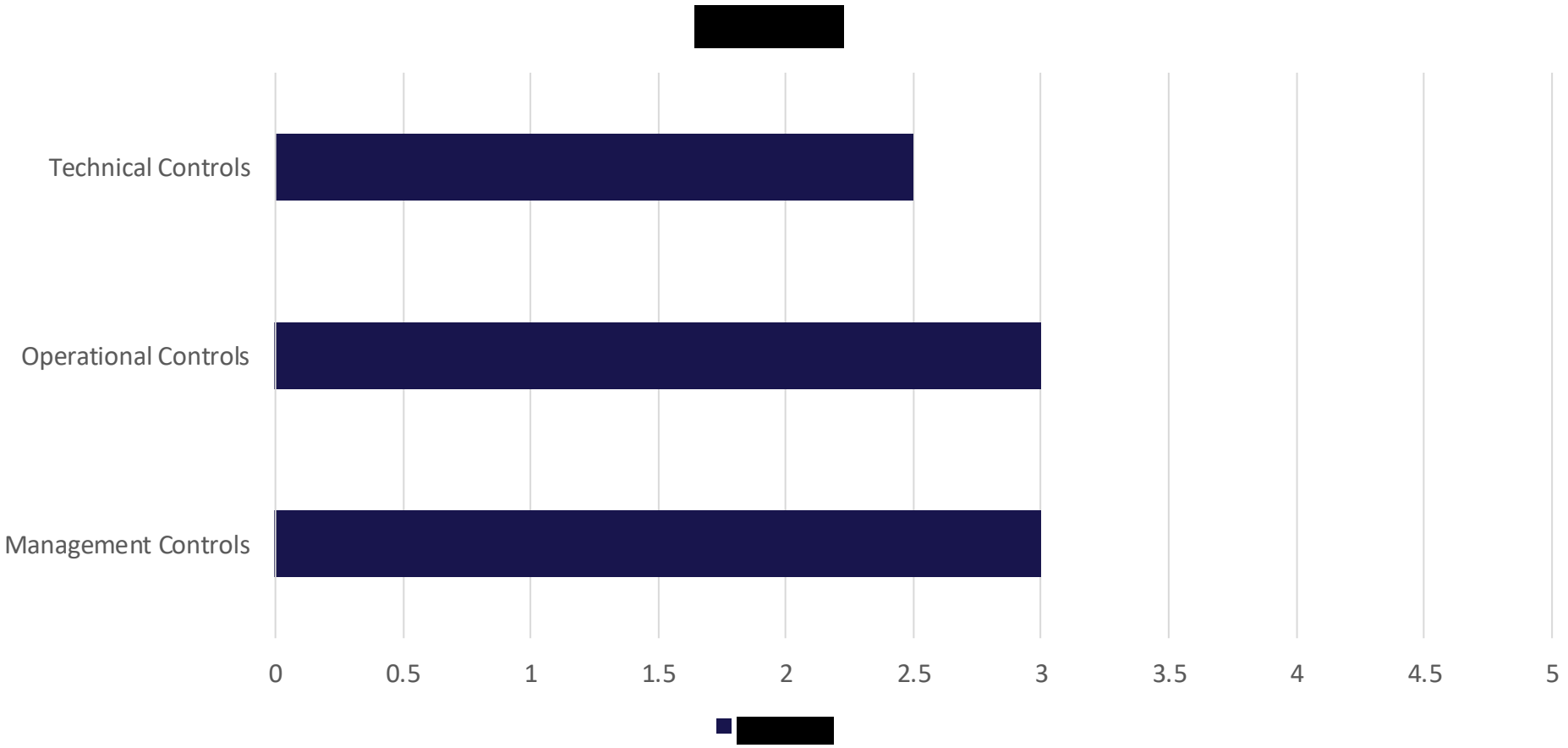
Recommendation: Implement Routine Testing and Analysis

- Based on the information that Abacus Group was able to review, the client's overall risk posture appears to be generally acceptable, though there are clear opportunities for improvement. Strengthening internal processes, improving visibility into key systems, and ensuring timely responsiveness to future assessments would contribute meaningfully to a more robust security posture.
- Notably, one high-risk finding was identified during the assessment. The client has indicated that this issue has been resolved; however, Abacus Group was not provided with sufficient evidence to independently verify remediation. Abacus Group documented the resolution as reported by the client, though the finding was referenced within the narrative of the report.
- Considering the above, it is Abacus Group's recommendation that [redacted] be required to have routine security testing that not only includes what would generally be reviewed in a cybersecurity risk assessment, but also would extend to internal systems and even organizational personnel (social engineering).
    - These assessments (external and internal network penetration testing, social engineering, cybersecurity risk assessments, and even compliance-based assessments, like an Incident Response Table-Top) should also be on an enforced schedule.
- Finally, [redacted] should implement ongoing monitoring and reporting expectations to ensure the organization's systems, infrastructure, and processes are secure.



0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Executive Summary – [redacted] (2 of 2)



Management Controls – Management of the information technology security system and the management and acceptance of risk.

Operational Controls – Security methods focusing on mechanisms implemented and executed primarily by people, including media safeguards and inventory controls

Technical Controls – Hardware and software controls provide automated protection to the system or applications.

0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Assessed Overall Cybersecurity Grade: **C**

Executive Summary – [redacted] (1 of 2)

The observed cybersecurity posture for [redacted] is both operationally effective and highly secure. From Abacus Group's vantage point, [redacted] demonstrated robust and mature cybersecurity practices.

Key Recommendations

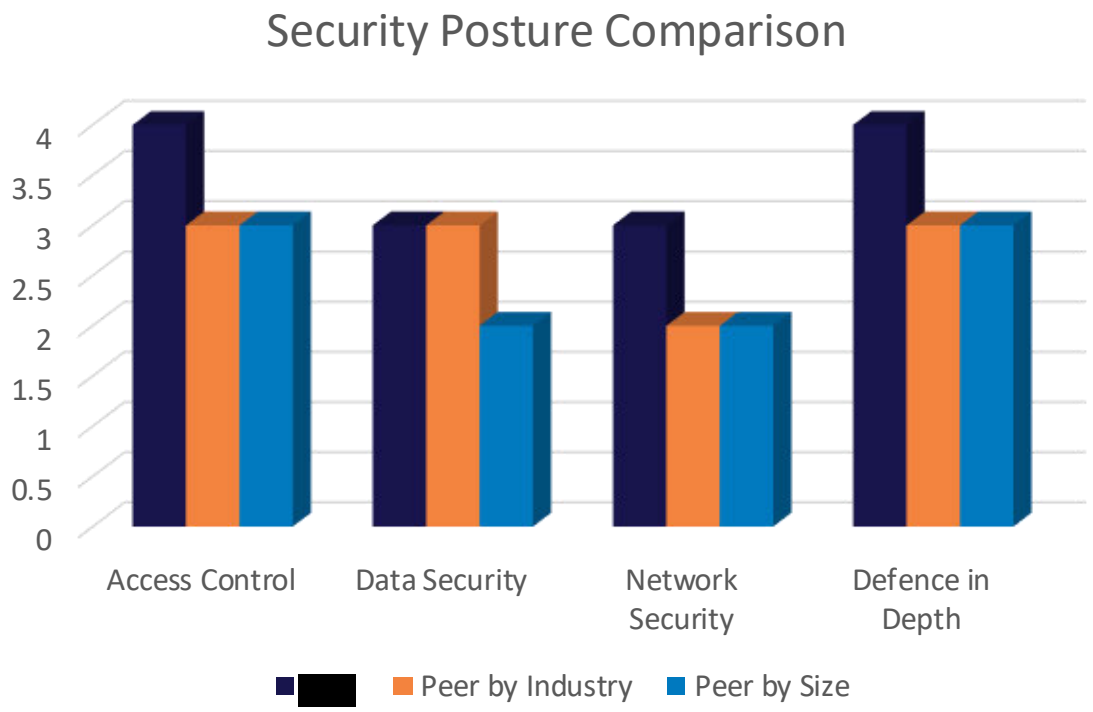
Based on the results and the context identified during this assessment, Abacus Group's vCISO team recommends the following key initiatives for 2025.

Recommendation: Implementation of a Written Information Security Program.

- During the interview question portion of the cybersecurity risk assessment, Abacus Group discovered that there was no Written Information Security Program (WISP) in place for [redacted]
- In the absence of a WISP, security practices tend to be ad-hoc, increasing the likelihood of control gaps, misconfigurations, regulatory non-compliance, and heightened legal and financial exposure. A WISP also serves as a foundational component of incident readiness by defining roles, responsibilities, and required procedures during security events. Without this structure, incident response efforts may be delayed or uncoordinated, amplifying the impact of potential breaches.

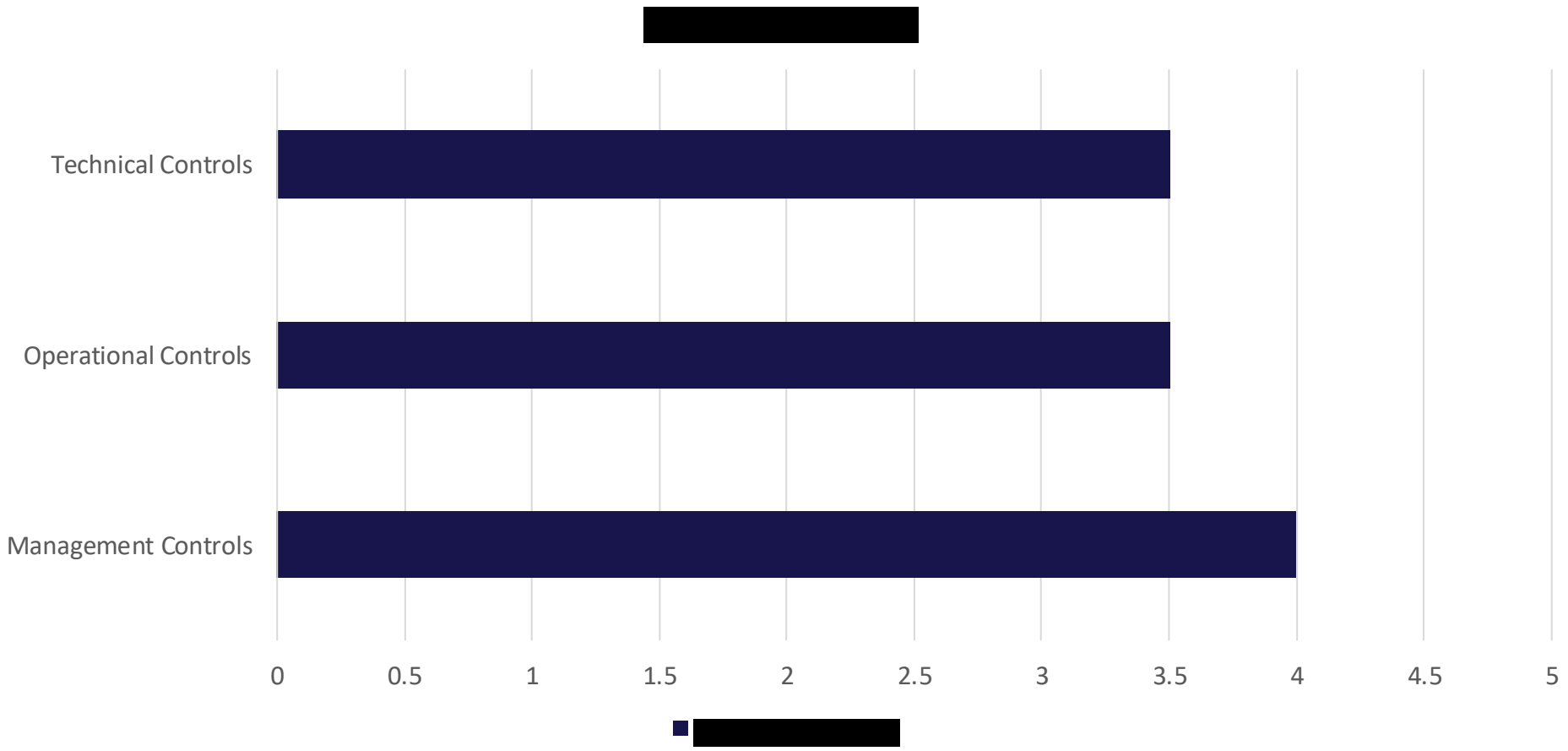
Recommendation: Implementation of a Vulnerability Management as a Service (VMaaS) solution.

- During the interview question portion of the cybersecurity risk assessment, Abacus Group discovered that there was no VMaaS solution in place for [redacted] Implementing VMaaS is essential for ensuring continuous identification, assessment, and remediation of vulnerabilities across the [redacted] infrastructure. A dedicated VMaaS program provides consistent scanning, analysis, and prioritized remediation guidance, capabilities that are difficult to maintain internally without specialized resources.



0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Executive Summary – [redacted] (2 of 2)



Management Controls – Management of the information technology security system and the management and acceptance of risk.

Operational Controls – Security methods focusing on mechanisms implemented and executed primarily by people, including media safeguards and inventory controls

Technical Controls – Hardware and software controls provide automated protection to the system or applications.

0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Assessed Overall Cybersecurity Grade: **A-**

Executive Summary – [redacted] (1 of 2)

It is clear from the assessment that [redacted] are in the early stages of developing a more mature cybersecurity program. From Abacus Group's perspective, primary concerns identified include general endpoint hardening deficiencies, the absence of Microsoft 365 licensing that supports advanced security capabilities, insufficient separation of privileges, and a lack of formalized policies and procedures.

Key Recommendations

Based on the results and the context identified during this assessment, Abacus Group's vCISO team recommends the following key initiatives for 2026.

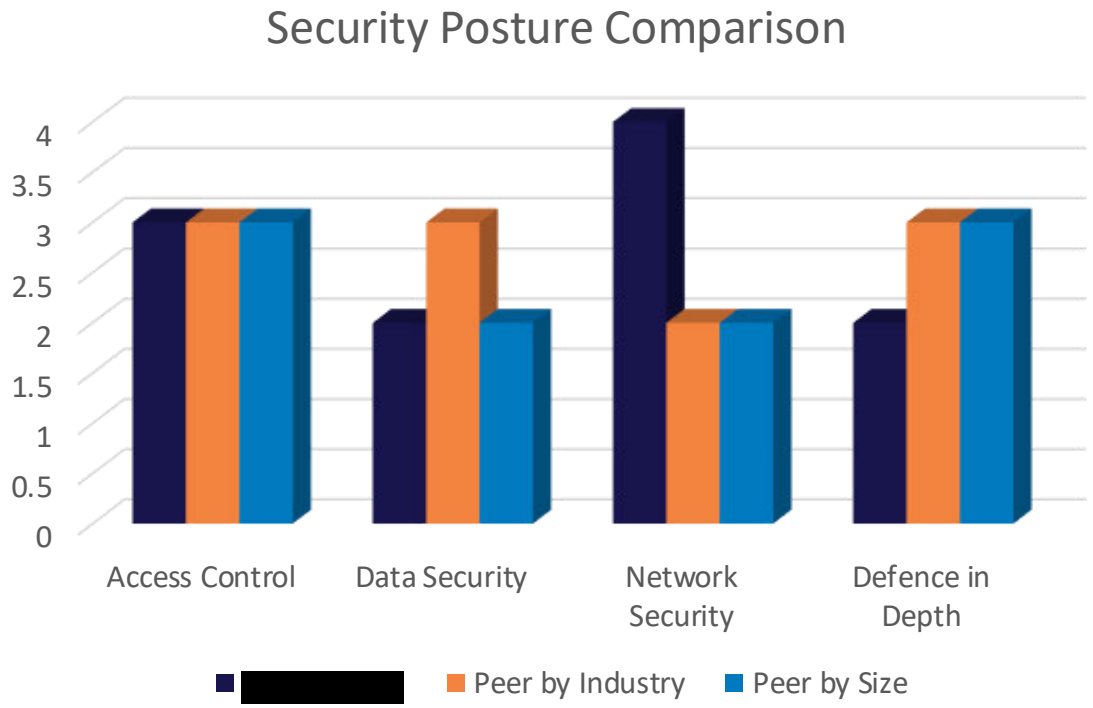
Recommendation: Implement improved device hardening controls across all company endpoints.

- During the assessment of an endpoint through the VMaaS dashboard, Abacus Group identified that numerous recommended Windows security configuration controls, such as strong Kerberos encryption, autorun disabling, and BitLocker encryption, were not implemented. Whilst Abacus Group only had visibility into a single device, and given that this device was configured with the current standard [redacted] controls, it has been assumed that the issue is widespread.

- In such an environment, the lack of consistent device hardening increases the risk of malware propagation, credential compromise, and unauthorized access. Unprotected or misconfigured endpoints can serve as an initial attack vector, potentially enabling attackers to move laterally across the network or exfiltrate sensitive data.

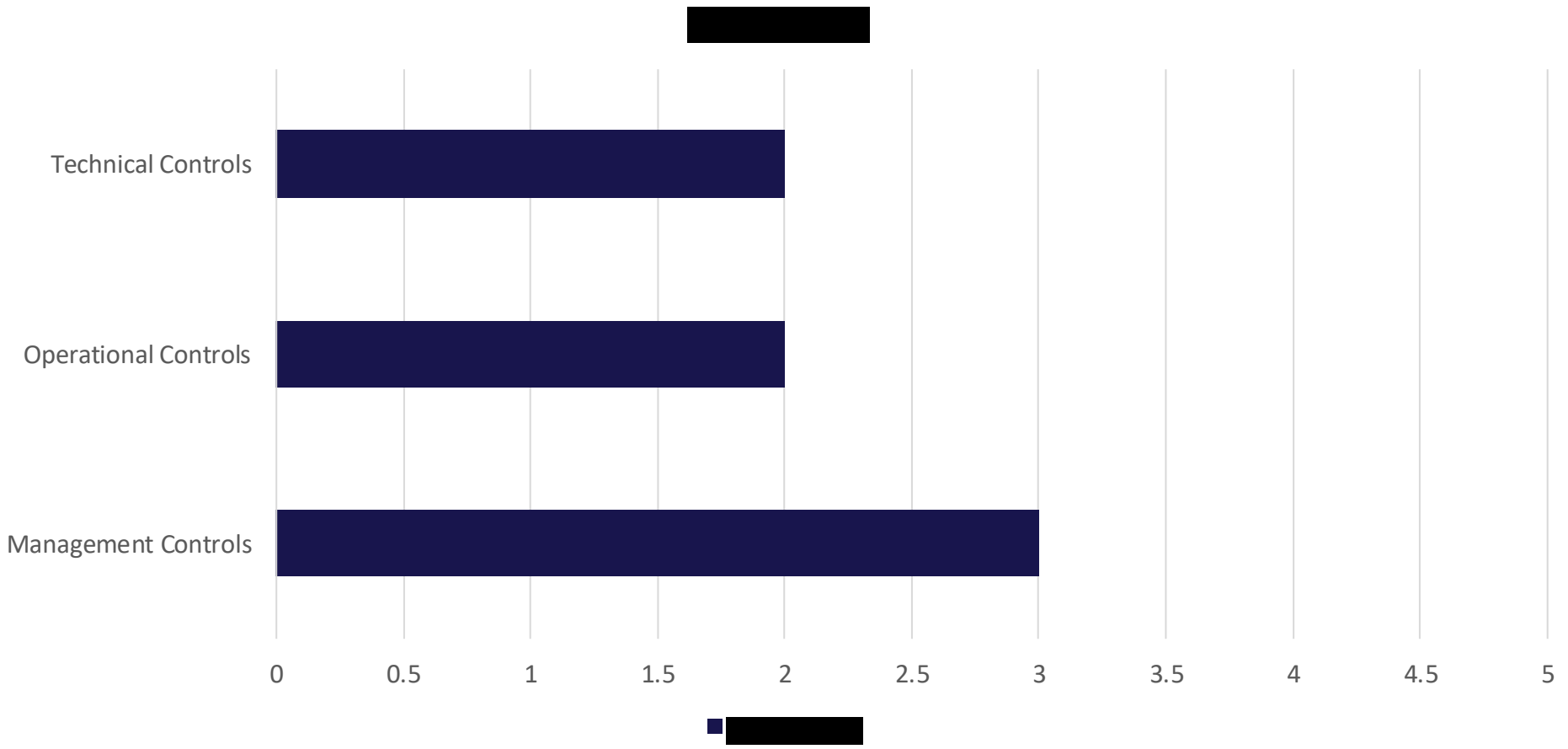
Recommendation: Upgrade Microsoft 365 licensing to unlock additional security features.

- During the review of Microsoft 365, Abacus Group identified that the organization is licensed at Microsoft 365 Business Standard, which does not include security features such as Microsoft Intune and data loss prevention policies within Microsoft Purview.



0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Executive Summary – [redacted] (2 of 2)



Management Controls – Management of the information technology security system and the management and acceptance of risk.

Operational Controls – Security methods focusing on mechanisms implemented and executed primarily by people, including media safeguards and inventory controls

Technical Controls – Hardware and software controls provide automated protection to the system or applications.

0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Assessed Overall Cybersecurity Grade: **C**

Executive Summary – Integrated Materials Solutions (1 of 2)

Integrated Materials Solutions' ([redacted] security posture reflects a strong foundation, with several components of a defense-in-depth architecture implemented with sound configurations around threat detection and baseline identity protections. These controls provide a solid security configuration and reduce exposure to common threat vectors.

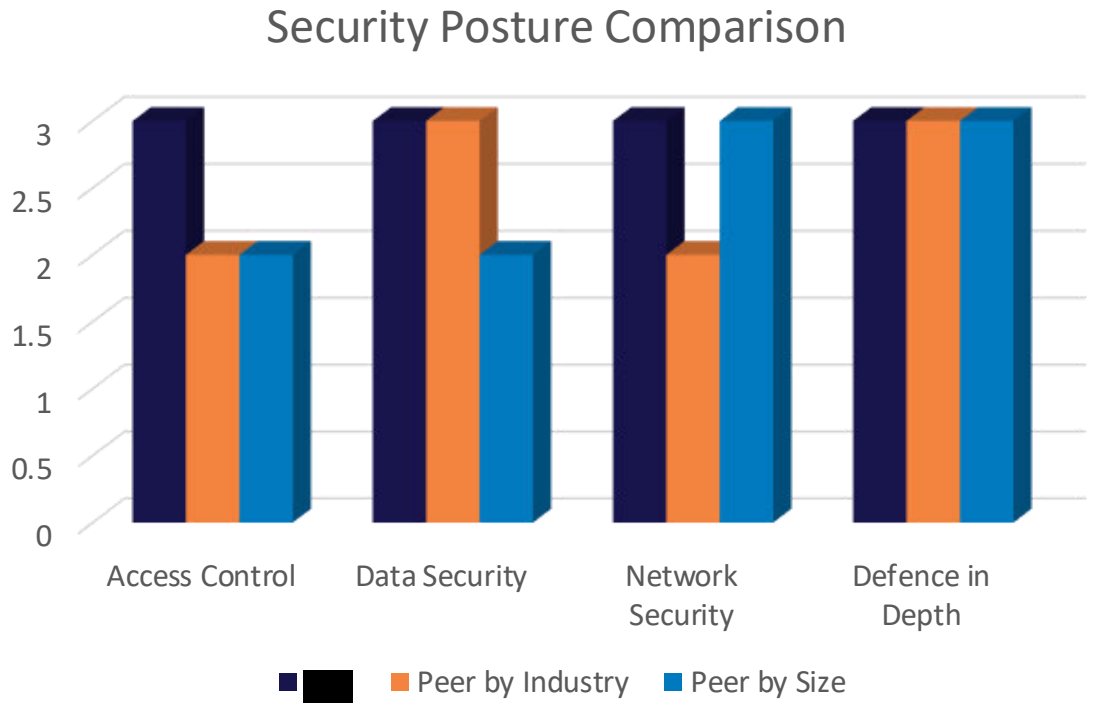
Key Recommendations
Based on the results and the context identified during this assessment, Abacus's vCISO team recommends the following key initiatives for 2026 and onward.

Recommendation: Implementation of a Corporate Password Management Solution.

- During the interview question portion, Abacus identified the absence of a corporate password management solution, increasing the risk of weak or reused credentials and insecure storage practices. Implementing a mandatory, organization-wide solution would significantly improve credential hygiene.

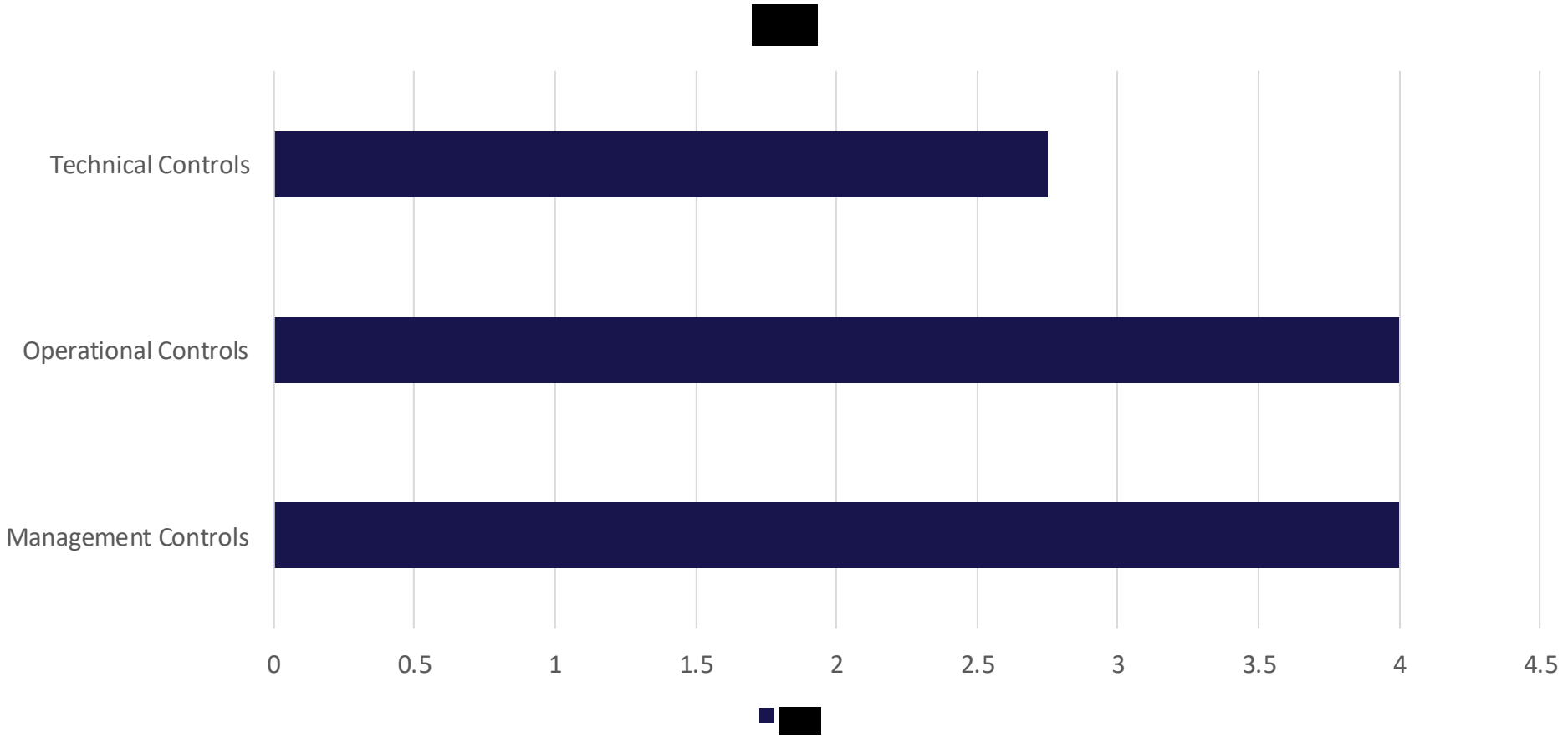
Recommendation: Implement Data Loss Prevention Controls, Additional Conditional Access Policies, and Adjustment of Standard Users Settings

- During the Microsoft Entra review, Abacus identified that [redacted] has not implemented formal Data Loss Prevention (DLP) controls within Microsoft 365. The absence of DLP controls increases the risk of unauthorized or accidental exposure of sensitive financial, personal, and proprietary data. Implementing DLP aligned to [redacted] data classification would improve data handling consistency, reduce data leakage risk, and strengthen regulatory and contractual compliance.
- Abacus also identified that while [redacted] has implemented several strong and robust Conditional Access policies, additional critical policies were missing or disabled at the time of assessment. The lack of enforced restrictions for high-privilege accounts and legacy authentication weakens the identity security posture and increases the attack surface, creating additional opportunities for credential-based attacks such as phishing or password spraying.
- Additionally, Abacus observed that standard users can create Microsoft 365 security groups, which weakens identity governance and increases the risk of privilege misuse or persistence. Restricting security group creation to administrators would enforce least privilege, improve visibility into access assignments, and reduce the risk of abuse or misconfiguration.
- Collectively, these observations show that Microsoft 365 is a critical platform and a concentrated point of risk for [redacted] Core functions such as identity, email, collaboration, and document management depend heavily on M365, so a compromise would have major impact. Abacus recommends prioritizing as mission-critical infrastructure to reduce enterprise risk and improve resilience.



0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Executive Summary – Integrated Materials Solutions (2 of 2)



Management Controls – Management of the information technology security system and the management and acceptance of risk.

Operational Controls – Security methods focusing on mechanisms implemented and executed primarily by people, including media safeguards and inventory controls

Technical Controls – Hardware and software controls provide automated protection to the system or applications.

0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Assessed Overall Cybersecurity Grade: B

Executive Summary – [redacted] (1 of 2)

The observed cybersecurity posture for [redacted] is both operationally effective and highly secure. From Abacus's vantage point, [redacted] demonstrated robust and mature cybersecurity practices. [redacted] also communicated that the organization is aware of its security posture, with the majority of risks already being known with applied considerations for risk acceptance and remediation.

Key Recommendations

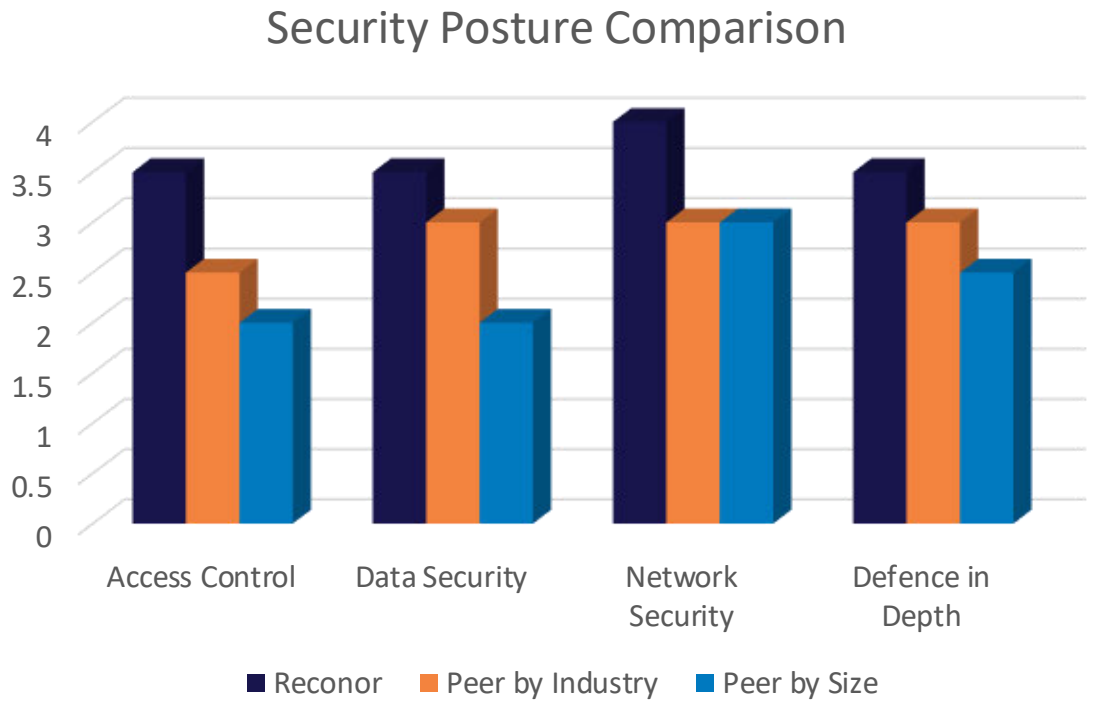
Based on the results and the context identified during this assessment, Abacus's vCISO team recommends the following key initiatives for 2026 and onward.

Recommendation: Improve the overall hygiene of Active Directory and Entra ID

- [redacted] should continue to mature identity security by tightening privileged role assignments, enforcing stronger authentication controls (including MFA and risk based access), and reducing over privileged or stale administrative access across on premises Active Directory and Entra ID.
- Several identity services and configurations present opportunities for hardening, including legacy authentication methods, directory service protections, and identity related services running on critical infrastructure. Addressing these areas will materially reduce exposure to identity based attacks commonly leveraged for lateral movement and privilege escalation.
- Identity hygiene should be treated as an ongoing operational discipline, incorporating regular review of privileged access, credential lifecycle management, and guest or external account governance to ensure identity controls remain aligned with organizational needs over time.

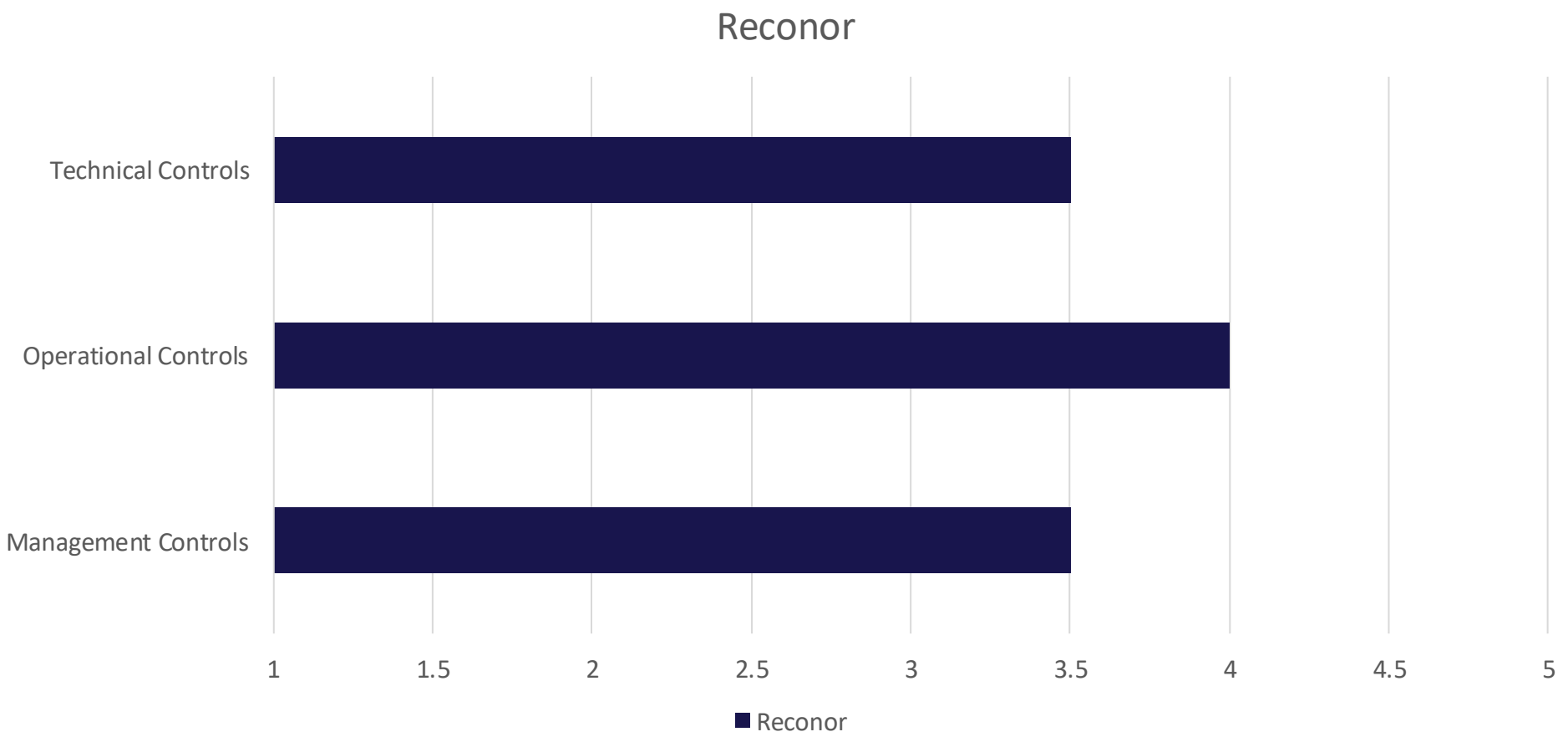
Recommendation: Align Identity Remediation with Migration and Modernization Goals

- [redacted] should assess identity related remediation activities within the context of planned modernization or migration initiatives, such as changes to hybrid identity models, directory consolidation, or cloud first identity adoption, to ensure remediation efforts align with long term architectural objectives.
- Where legacy identity components or configurations are expected to be replaced, consolidated, or deprecated, certain remediation actions may be more effectively addressed as part of those initiatives rather than implemented as standalone fixes.
- Security improvements that reduce immediate identity risk, such as strengthening authentication controls, reducing excessive privilege, and improving visibility, should remain a priority regardless of migration timelines, as these measures provide sustained security value.



0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Executive Summary – [redacted] (2 of 2)



Management Controls – Management of the information technology security system and the management and acceptance of risk.

Operational Controls – Security methods focusing on mechanisms implemented and executed primarily by people, including media safeguards and inventory controls

Technical Controls – Hardware and software controls provide automated protection to the system or applications.

0 – No Controls	(Critical Risk)
1 – Immature Controls	(High Risk)
2 – Minimal Controls	(Medium – High Risk)
3 – Industry Standard	(Medium Risk)
4 – Mature Security Controls	(Low Risk)
5 – Operational Excellence	(Minimal Risk)

Assessed Overall Cybersecurity Grade: B