PHILOCYBERS
CONSULTING FIRM

IT SYSTEM RISK ASSESSMENT REPORT

PREPARED BY

OSWALD E.TOKU

SEPTEMBER 2025

Part 1: Risk Assessment Report for Microsoft Exchange Server

1.0 EXECUTIVE SUMMARY

This report presents a detailed risk assessment of the organization's on-premises Microsoft Exchange Server environment. The primary objective is to identify, analyze, and evaluate potential risks to this critical communication system and to propose actionable mitigation strategies. Microsoft Exchange Server is the central hub for all corporate email, calendaring, and collaboration, making its security paramount to business continuity and the protection of sensitive data. The assessment concludes that the on-premises Exchange Server presents a significant risk profile, primarily due to its public-facing nature and a history of high-impact vulnerabilities. A failure to manage these risks effectively could lead to a catastrophic loss of data confidentiality, integrity, and availability. The most pressing threats identified are from sophisticated, state-sponsored actors and financially motivated cybercriminal groups. This report strongly recommends a multi-layered approach to mitigation, focusing on a comprehensive patching and hardening strategy, with a strategic view toward a more secure, long-term solution.

2.0 ASSESSMENT OBJECTIVES AND SCOPE

This assessment was initiated to provide a structured, in-depth analysis of the security posture of the on-premises Microsoft Exchange Server. A systematic approach, a key component of effective risk management, was followed to ensure that all identified risks are thoroughly understood and effectively addressed.[1]

2.1 Assessment Objectives

The specific objectives of this assessment were as follows:

- To identify and document potential threats and vulnerabilities to the Microsoft Exchange Server system, with a focus on its core components and external dependencies.[1]

- To conduct a qualitative analysis of the likelihood and potential impact of these risks on the confidentiality, integrity, and availability (CIA) of the organization's data and operational mission.[2]
- To evaluate the overall risk level for each identified threat by applying a standardized qualitative risk matrix and scoring system.[4]
- To recommend and prioritize a series of mitigation strategies and controls to reduce the assessed risks to a level that is acceptable to the organization.[1]

2.2 Scope of Assessment

The scope of this risk assessment is focused on a live, on-premises deployment of Microsoft Exchange Server 2019.[6] The analysis includes an examination of its key services, such as the mailbox database, client access services, and transport services.[7] The assessment also covers the system's external dependencies, including required DNS records (MX, SPF), firewall configurations, and various client access methods (e.g., Outlook on the web, Exchange ActiveSync).[9] The threats considered include those from both external adversaries and potential internal sources, such as human error or malicious insiders.[10] This is a point-in-time assessment; while continuous monitoring and review are identified as a core recommendation, the implementation of those controls is outside the scope of this specific report.[1] The findings presented in this document may be used to inform higher-level risk assessments at the organizational or mission-specific level.[11]

2.3 Assessment Team and Resources

A successful risk assessment is a collaborative effort requiring a clearly defined team and the right tools and resources. An objective assessment team is essential for reviewing the system and its controls and reporting findings to leadership.[13]

Role	**Responsibilities**

Risk Owners / Leadership	Responsible for setting the organization's risk appetite, defining risk policies, and allocating a budget for mitigation activities.[14]
IT System Administrator / Owner	Responsible for implementing security controls, maintaining the system, and ensuring that mitigation strategies are carried out in accordance with documentation.[13]
Assessment Team / Auditors	Objectively review the system, document findings, and report to leadership to ensure the assessment is unbiased.[13]

Resource Category	**Examples**
Risk Assessment Tools	Standardized templates and checklists to identify risks.[1] Tools like the SRA Tool can be used by smaller organizations.[16]
Frameworks and Standards	Use established frameworks like NIST and ISO to guide the process and benchmark controls against best practices.[1]
Threat Intelligence	Monitor threat intelligence feeds and reports from organizations like NIST to stay informed of the latest vulnerabilities and threats.[1]

3.0 IDENTIFIED ASSETS

A core component of any risk assessment is the identification of all key assets that are part of or interact with the system being evaluated. This inventory is the foundation for understanding which

components are most critical and, therefore, most vulnerable to attack.[2] For the on-premises Microsoft Exchange Server, the following assets have been identified:

- **Hardware:** The physical Windows Server hardware on which the Exchange software is installed.[8]
- **Software:** The Microsoft Exchange Server application itself, the underlying Windows Server operating system, and client applications such as Outlook and Teams.[7]
- **Data:** All corporate data, including user emails, calendars, contacts, and other sensitive information stored on the server.[2]
- **Personnel:** System administrators who manage the server and all end-users who rely on its services for daily communication and collaboration.[10]
- **Network Components:** All associated network infrastructure and dependencies, including DNS records (MX, SPF), firewall rules, and communication protocols (SMTP, MAPI, IMAP, POP3, and Exchange ActiveSync).[8]
- **Services:** The public-facing services that enable client access, such as Outlook on the web (OWA), and Exchange ActiveSync for mobile devices.[8]

4.0 PURPOSE OF THE SYSTEM

4.1 Core Functionality

Microsoft Exchange Server is an enterprise-grade mail and calendaring server developed by Microsoft that runs on Windows Server operating systems.[8] Beyond its primary function as a mail server, it is a robust, centralized platform that supports a wide range of collaborative functions, including email hosting, shared calendars, contact management, and task organization.[7] It enables real-time synchronization of mailboxes and address books, ensuring that teams can collaborate efficiently across multiple devices and locations.[7] The system supports both proprietary protocols like MAPI for Outlook clients and standard protocols like POP3 and IMAP for other mail clients, with SMTP used for communication with other external mail servers.[8] This versatile functionality makes it the indispensable backbone of the organization's daily communication and collaboration.[7]

4.2 Business Criticality

The system's primary purpose is to ensure secure and efficient communication, which is vital for daily business operations. A compromise of the Exchange Server would severely disrupt core business functions and could lead to a catastrophic loss of data confidentiality and integrity.[2] For many organizations, the system is a critical asset whose compromise would lead to a significant degradation or total loss of mission capability.[3] Beyond communication, it acts as a central hub for storing, organizing, and securing sensitive user data, simplifying backup and recovery processes.[7] A disruption to or breach of this system would not only halt productivity but also likely result in severe financial, legal, and reputational damage.[3]

5.0 RISK IDENTIFICATION AND ANALYSIS (NIST SP 800-30 APPROACH)

This risk assessment was conducted following the guidelines of NIST SP 800-30, which provides a systematic approach for identifying, analyzing, and evaluating risks to information systems.[1] The process involves defining the context of the assessment, identifying potential threats and vulnerabilities, and then analyzing the likelihood and impact of each risk.

5.1 Risk Identification

The first step in the NIST approach is to identify what could go wrong by analyzing system assets, threats, vulnerabilities, and existing controls.

Threat #	Threat	Vulnerabilities	Predisposing Conditions	Potential Impacts	Existing Controls
1	Phishing attacks	Weak MFA enforcement; poor user awareness	High email volume; BYOD environment	Unauthorized mailbox access; credential theft	Basic spam filter & antivirus; security awareness training
2	Malware in attachments	Limited email sandboxing/ATP	High inbound email volume	Malware propagation; compromise of endpoints	Basic spam filter; endpoint antivirus

3	Zero-day exploits	Internet-exposed Exchange services with unpatched CVEs	Public-facing Exchange Server	Remote code execution; full server compromise	Patch management ; vulnerability scanning
4	Delayed patching / slow patch cycle	Manual patch process; insufficient testing resources	Resource constraints delaying patching	Exploitation of known vulnerabilities ; data breach	Monthly patch cycle & manual updates
5	Insider misuse (malicious or negligent)	Over-privileged admin accounts; weak monitoring	Limited separation of duties	Data exfiltration; unauthorized changes	RBAC for admins; logging and monitoring
6	Credential stuffing / brute-force on OWA	Weak password policy; lack of lockout thresholds	Many remote users using OWA	Account takeover; unauthorized access	Password policy (complexity enforced); conditional access
7	Denial-of-Service (DoS) against mail services	No rate limiting or DDoS protection	Public-facing OWA and SMTP endpoints	Email service outage; business disruption	Basic intrusion detection; firewall rules
8	Misconfigured mail flow rules (data leakage)	Mail flow rules not periodically reviewed	Decentralized rule management	Unintended forwarding of sensitive data externally	Annual transport rule review
9	Compromise of mobile devices syncing via ActiveSync	Lack of Mobile Device Management (MDM)	Personal/BYOD devices without corporate controls	Loss/theft of corporate data from mobiles	Manual device enrollment policy
10	Social engineering of IT staff (helpdesk/admins)	Lack of strict verification procedures	Helpdesk lacks identity verification scripts	Attacker gains privileged access via impersonation	Basic helpdesk call-back procedure for admin requests

5.2 Risk Analysis

The risk analysis stage evaluates the identified risks to determine their overall severity. This involves scoring each risk's likelihood of occurrence and its potential impact on the organization.

5.3 Evaluation Criteria

- **Likelihood:** The estimated probability of a risk event occurring was rated on a five-point scale.[4]
    - **1 - Rare:** The event is highly unlikely to happen.
    - **2 - Unlikely:** The event is possible but not probable.
    - **3 - Moderate:** The event is likely to occur sometime in the system's life.
    - **4 - Likely:** The event is probable and will likely occur multiple times.
    - **5 - Almost Certain:** The event is expected to occur frequently.
- **Impact:** The potential consequences of a risk event were rated on a five-point scale, considering the effect on the organization's mission, productivity, finances, legal standing, and reputation.[3]
    - **1 - Negligible:** The risk will have little to no consequences.
    - **2 - Minor:** The risk may cause some disruption, but mission-critical functions will be maintained.
    - **3 - Significant:** The risk will cause significant degradation of mission capability, requiring substantial effort to restore.
    - **4 - Major:** The risk will cause severe degradation or loss of mission capability.
    - **5 - Catastrophic:** The risk will cause a total loss of mission capability, resulting in severe financial, legal, and reputational damage.
- **Risk Rating:** The overall risk score for each threat was determined by multiplying the likelihood and impact values (Risk = Likelihood x Impact).[3]

5.4 Risk Matrix and Legend

The following table and matrix were used to visually represent and evaluate the risk landscape.

Likelihood	Qualitative Description	Impact	Qualitative Description
5	Almost Certain	5	Catastrophic
4	Likely	4	Major
3	Moderate	3	Significant
2	Unlikely	2	Minor
1	Rare	1	Negligible

IMPACT	LIKELIHOOD					
	LIKELIHOOD * IMPACT	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
	5 Catastrophic					
	4 Major					
	3 Significant					
	2 Minor					
	1 Negligible					

RISK RATING	1 - 5	6 - 10	11 - 15	16 - 25
QUALITY LEVEL	LOW	MEDIUM	HIGH	CRITICAL

5.5 Risk Analysis Table

Risk ID	Threat / Vulnerability	Likelihood (L)	Impact (I)	Risk Rating (L×I)	Risk Level (Legend)
EX-1	Phishing attacks + weak MFA	4 (Likely)	4 (Major)	16	Critical
EX-2	Malware in attachments (no sandbox)	4 (Likely)	3 (Significant)	12	High
EX-3	Zero-day exploits (public-facing service)	3 (Possible)	5 (Catastrophic)	15	High
EX-4	Delayed patching / slow patch cycle	4 (Likely)	4 (Major)	16	Critical
EX-5	Insider misuse (malicious or negligent)	3 (Possible)	4 (Major)	12	High
EX-6	Credential stuffing / brute-force on OWA	4 (Likely)	3 (Significant)	12	High
EX-7	Denial-of-Service (DoS) against mail services	3 (Possible)	3 (Significant)	9	Medium
EX-8	Misconfigured mail flow rules (data leakage)	3 (Possible)	3 (Significant)	9	Medium
EX-9	Compromise of mobile devices via ActiveSync	3 (Possible)	4 (Major)	12	High
EX-10	Social engineering of IT staff (helpdesk/admins)	4 (Likely)	4 (Major)	16	Critical

6.0 MITIGATION STRATEGIES AND RECOMMENDATIONS

The mitigation of risks to the Exchange Server requires a multi-layered approach involving technical, administrative, and physical controls.[2]

6.1 Technical Controls

- **Prioritize Patching:** The immediate and most critical action is to apply all available security updates, patches, and cumulative updates from Microsoft. This process should be automated where possible and regularly tested to ensure its effectiveness.[20] Continuous monitoring for new vulnerabilities and patching them promptly is the most effective way to reduce the attack surface.[17]
- **System Hardening:**
    - **Remove Unnecessary Services:** To reduce the attack surface, all non-essential services and components should be disabled or removed from the server.[24] This includes services that are not explicitly required for mission-critical functions.[25]
    - **Implement Least Privilege:** Access controls should be implemented based on the principle of least privilege, ensuring that users and administrators have only the permissions necessary to perform their duties.[21] This is especially important for administrative accounts and should be supported by a Privileged Access Management (PAM) solution.[21]
    - **Enforce Strong Authentication:** Implement and enforce a robust multi-factor authentication (MFA) policy for all remote access, especially for administrative and OWA access.[21]
    - **Network Segmentation:** The Exchange Server network should be logically segregated from the rest of the internal network using a firewall or other application-aware defenses. This containment strategy limits an attacker's ability to move laterally across the network if the server is compromised.[21]
- **Logging and Monitoring:**
    - **Centralized Logging:** All logs from the Exchange Server, including access and security logs, must be enabled and sent to a centralized Security Information and Event Management (SIEM) system.[25]
    - **Intrusion Detection:** Actively monitor for and investigate anomalous activities, such as the deployment of web shells or other suspicious processes.[17] Implement an Endpoint Detection and Response (EDR) solution on the server to provide additional threat-hunting capabilities.[21]

6.2 Administrative Controls

- **Policy and Procedure:** A formal patch management policy must be developed and enforced, with clear responsibilities, timelines, and a review process.[22] This policy should align with a repeatable risk management framework to ensure consistency.[27]
- **Security Awareness Training:** Mandatory and regular security awareness training must be provided to all employees to educate them on identifying phishing attempts and maintaining secure email and remote access practices.[2] This is a preventative control that helps to address human factors of security.[26]
- **Disaster Recovery Plan:** A comprehensive and regularly tested disaster recovery plan (DRP) must be in place. This plan should include a strategy for restoring data from encrypted, offsite, and offline backups to ensure business continuity in the event of a major incident like a ransomware attack.[21]

6.3 Physical Controls

- The Exchange server hardware must be physically secured within a locked, access-controlled data center or server room.[10] Physical controls are a tangible layer of protection against theft or unauthorized physical access to critical infrastructure.[28]

7.0 RISK REGISTER

This risk register lists the key risks identified for the organization's on-premises Microsoft Exchange Server 2019 environment. It summarizes the description of each risk, its source, consequences, likelihood, inherent and residual ratings, existing controls, planned treatments and responsible owners. The register is designed to track mitigation actions and review dates for continuous improvement.

Risk #	Date	Description of Risk	Risk Source	Risk Consequences	Likelihood Rating	Inherent Risk Rating	Existing Controls	Residual Risk Rating	Planned Treatments	Risk Owner	Treatment Due Date	Risk Review Date
EX-1	Sept 2025	Phishing with weak MFA leads to account compromise	External attackers (phishing emails)	Unauthorized mailbox access; data leakage; reputational damage	4 (Likely) x 4(Major)	16 (Critical)	Basic spam filter; endpoint antivirus; monthly patching cycle	8 (Medium)	Enforce robust MFA; phishing awareness training; advanced email filtering	IT Security	Oct 2025	Jan 2026
EX-2	Sept 2025	Malware in attachments (no sandboxing)	External attackers (email malware)	Malware infection; disruption of mail service; data breach	4 (Likely) x 3(Significant)	12 (High)	Basic spam filter	6 (Medium)	Deploy sandboxing; tighten attachment policies	IT Security	Oct 2025	Jan 2026
EX-3	Sept 2025	Zero-day exploit targeting Exchange	External attackers	Remote code execution; total compromise of server; data exfiltration	3 (Possible) x 5(Catastrophic)	15 (High)	Monthly patching; antivirus	15 (High)	Accelerate patch management; implement threat intelligence feeds; segment Exchange server	IT Security	Oct 2025	Jan 2026

									network			
EX-4	Sept 2025	Delayed patching of Exchange server	Internal processes (patch management)	Exploitation of known vulnerabilities; data breach	4 (Likely) x 4(Major)	16 (Critical)	Monthly patch cycle	8 (Medium)	Implement automated patch deployment; enforce patch SLAs	IT Operations	Nov 2025	Feb 2026
EX-5	Sept 2025	Insider misuse of admin credentials	Internal (malicious insider or error)	Unauthorized changes; mailbox data exfiltration	3 (Moderate) x 4(Major)	12 (High)	Basic logging	9 (Medium)	Implement PAM; stronger monitoring; least privilege	IT Security	Nov 2025	Feb 2026
EX-6	Sept 2025	Bring-Your-Own-Device (BYOD) introduces insecure endpoints	Internal (user devices)	Malware spread; credential theft	4 (Likely) x 3(Significant)	12(Medium)	Basic mobile policy	6 (Medium)	Implement mobile device management (MDM); enforce endpoint security	IT Security	Dec 2025	Mar 2026
EX-7	Sept 2025	Weak sandboxing of attachments	Technical configuration	Malicious code execution	3 (Moderate) x 3(Significant)	9 (Medium)	Spam filter	6 (Medium)	Deploy advanced attachment sandboxing	IT Security	Dec 2025	Mar 2026
EX-8	Sept 2025	Misconfigured mail rules lead to	Internal (misconfiguration)	Emails auto-forwarded externa	3 (Moderate) x 3(Significant)	9 (Medium)	Basic admin reviews	6 (Medium)	Implement DLP (data loss preven	IT Security	Dec 2025	Mar 2026

		data leakage		lly; data loss					tion); periodic rule reviews			
EX-9	Sept 2025	Lack of user security training	Internal (user awareness)	Susceptibility to phishing; accidental data leaks	3 (Moderate) x 4(Major)	12 (High)	Occasional awareness sessions	6 (Medium)	Mandatory quarterly security awareness training	HR/IT Security	Jan 2026	Apr 2026
EX-10	Sept 2025	Inadequate monitoring of Exchange logs	Internal (monitoring)	Delayed detection of attacks; prolonged compromise	4 (Likely) x 4(Major)	16 (Critical)	Basic logging only	6 (Medium)	Implement centralized SIEM; enable full audit logging	IT Security	Jan 2026	Apr 2026

8.0 CONCLUSION

The on-premises Microsoft Exchange Server, as a central communication hub, remains a high-risk asset. The primary risks are associated with sophisticated external threats from nation-state actors and cybercriminals, who are known to exploit critical vulnerabilities for both espionage and financial gain. The assessment found that the most significant weaknesses are a failure to apply timely security patches and insecure configurations. While the recommended mitigation strategies can significantly reduce these risks, the sheer number of attack vectors and the history of zero-day exploits necessitate a model of continuous vigilance.

Part 2: Risk Assessment Report for Oracle Database 19c

1.0 EXECUTIVE SUMMARY

This report presents a detailed risk assessment of the organization's Oracle Database 19c environment. The primary objective is to identify, analyze, and evaluate potential risks to this critical data management system and to propose actionable mitigation strategies. Oracle Database 19c is a powerful platform that manages both operational and analytical workloads, handling sensitive information such as financial and customer data for mission-critical applications across various industries.[29] The assessment concludes that the Oracle Database 19c presents a significant risk profile, primarily due to common vulnerabilities like SQL injection, unpatched software, and the abuse of excessive privileges. A failure to manage these risks effectively could lead to catastrophic data breach, regulatory fines, and operational disruption. This report recommends a multi-layered approach to mitigation, focusing on a comprehensive hardening and access control strategy.

2.0 ASSESSMENT OBJECTIVES AND SCOPE

This assessment was initiated to provide a structured, in-depth analysis of the security posture of the Oracle Database 19c environment. A systematic approach was followed to ensure that all identified risks are thoroughly understood and effectively addressed.[2]

2.1 Assessment Objectives

The specific objectives of this assessment were as follows:

- To identify and document potential threats and vulnerabilities to the Oracle Database 19c system, with a focus on its core components and external dependencies.[2]
- To conduct a qualitative analysis of the likelihood and potential impact of these risks on the confidentiality, integrity, and availability (CIA) of the organization's data and operational mission.[2]
- To evaluate the overall risk level for each identified threat by applying a standardized qualitative risk matrix and scoring system.[4]
- To recommend and prioritize a series of mitigation strategies and controls to reduce the assessed risks to a level that is acceptable to the organization.[1]

2.2 Scope of Assessment

The scope of this risk assessment is focused on a live, on-premises deployment of Oracle Database 19c. The analysis includes an examination of its key assets, such as production databases, backup files, and administrative accounts.[2] The threats considered include those from both external adversaries, such as SQL injection, and potential internal sources, like accidental misconfigurations or malicious insiders with excessive privileges.[31] This is a point-in-time assessment; while continuous monitoring and review are identified as a core recommendation, the implementation of those controls is outside the scope of this specific report.[1]

2.3 Assessment Team and Resources

The assessment of a critical network device like the Oracle Database 19c requires a specialized team and a structured approach. The team is responsible for managing the security posture of the device, with leadership providing strategic direction and auditors ensuring objectivity.[13]

Role	Responsibilities
Risk Owners / Leadership	Responsible for defining the acceptable level of risk and allocating a budget for security initiatives.[14]
Database Administrators (DBAs)	Responsible for implementing security controls, managing the database configuration, and applying patches and updates as they are released.[32]
Assessment Team / Auditors	An objective team is required to review the system, interview staff, and report findings to leadership to ensure an unbiased assessment.[13]

Resource Category	Examples
Risk Assessment Tools	Use checklists and templates to ensure a comprehensive identification of risks.[1] Tools like the SRA Tool are available for smaller organizations.[16]
Frameworks and Standards	Standardized frameworks such as NIST, ISO, and CIS Benchmarks can provide secure configuration guidelines for network devices.[33]
Threat Intelligence	Leverage threat intelligence feeds and security advisories from vendors like Oracle to stay informed about the latest threats and vulnerabilities affecting the database.[34]

3.0 IDENTIFIED ASSETS

The IT risk assessment process begins with a comprehensive review of the systems to be evaluated and a thorough inventory of the assets within them.[2] For the Oracle Database 19c, the following assets have been identified:

- **Databases:** The production databases containing critical business information, including customer data, financial records, and intellectual property.[31]
- **Accounts:** All user accounts, particularly privileged Database Administrator (DBA) accounts, which have extensive access to the system.[32]
- **Data Files:** All data files, including production data files and backup files, which are a common target for theft or encryption.[32]
- **Network Components:** The database listener and other network interfaces that allow applications and users to connect to the database.[32]

4.0 PURPOSE OF THE SYSTEM

4.1 Core Functionality

Oracle Database 19c is a comprehensive, multi-model enterprise-class database designed for both on-premises and cloud deployments.[30] It is a centralized platform that supports a wide range of operational and analytical workloads, including traditional transactions, real-time analytics, and data warehousing.[29] It provides advanced features such as automatic indexing, in-memory processing, and parallel execution to handle complex workloads efficiently.[29] The database is built to provide a high level of performance, scalability, and reliability, making it a foundation for many critical business processes.[30]

4.2 Business Criticality

The Oracle Database 19c is a core business asset for managing and protecting critical information. It is used across various industries, including banking for transaction processing and healthcare for electronic health records, where downtime or data loss would be catastrophic.[29] A compromise of the database would severely disrupt core business functions, leading to a loss of data confidentiality, integrity, and availability.[31] A breach of sensitive data, such as personally identifiable information (PII) or protected health information (PHI), could result in severe financial penalties, legal liabilities (e.g., GDPR, HIPAA), and irreparable reputational damage.[31]

5.0 RISK IDENTIFICATION AND ANALYSIS (NIST SP 800-30 APPROACH)

This risk assessment was conducted following the guidelines of NIST SP 800-30, which provides a systematic approach for identifying, analyzing, and evaluating risks to information systems.[1] The process involves defining the context of the assessment, identifying potential threats and vulnerabilities, and then analyzing the likelihood and impact of each risk.

5.1 Risk Identification

The first step in the NIST approach is to identify what could go wrong by analyzing system assets, threats, vulnerabilities, and existing controls.

Threat #	Threat	Vulnerabilities	Predisposing Conditions	Potential Impacts	Existing Controls
1	SQL Injection attacks	Lack of parameterized queries; insecure coding	Legacy applications interfacing with DB	Unauthorized data access; data modification	Web application firewall; developer secure coding training
2	Unpatched database vulnerabilities	Delayed application of Oracle Critical Patch Updates	Complex change management; large DBA team	Remote code execution; privilege escalation	Regular CPU patching schedule; vulnerability scanning
3	Insider misuse (DBAs)	Excessive DBA privileges; lack of monitoring	Large DBA team; limited segregation of duties	Data exfiltration; unauthorized changes	RBAC; audit trails enabled

4	Unencrypted backups stolen	Backups stored in plain text; weak access controls	Backups stored on shared drives; offsite without encryption	Data breach; regulatory fines	Encryption at rest; restricted backup access
5	Weak authentication to database	Weak password policy; no MFA	Multiple legacy apps; hard-coded credentials	Credential compromise; unauthorized access	Strong password policy; credential vaulting
6	Privilege escalation through vulnerable PL/SQL packages	Unpatched PL/SQL packages; unnecessary packages installed	Legacy packages remain enabled	Attackers gain DBA privileges	Periodic package review; patching
7	Denial-of-Service (DoS) attacks	No resource limits; lack of monitoring	Shared DB resources; external connections	DB unavailability; business disruption	Resource manager configured; network firewall
8	Data leakage through misconfigured roles	Overly broad role grants; no periodic review	Rapidly changing user base	Sensitive data exposure; compliance violation	Periodic role/privilege review; least privilege
9	Compromise via insecure database links	Database links to untrusted sources; no encryption	Multiple inter-database connections	Lateral movement between databases	Encryption of DB links; strict link policies
10	Social engineering of DBAs	Lack of strict verification procedures for DBA requests	Busy support team; remote work	Attackers gain privileged access	Helpdesk verification procedures; mandatory call-back

5.2 Risk Analysis

The risk analysis stage evaluates the identified risks to determine their overall severity. This involves scoring each risk's likelihood of occurrence and its potential impact on the organization.

5.3 Evaluation Criteria

- **Likelihood:** The estimated probability of a risk event occurring was rated on a five-point scale.[4]
    - **1 - Rare:** The event is highly unlikely to happen.
    - **2 - Unlikely:** The event is possible but not probable.
    - **3 - Moderate:** The event is likely to occur sometime in the system's life.
    - **4 - Likely:** The event is probable and will likely occur multiple times.
    - **5 - Almost Certain:** The event is expected to occur frequently.
- **Impact:** The potential consequences of a risk event were rated on a five-point scale, considering the effect on the organization's mission, productivity, finances, legal standing, and reputation.[3]
    - **1 - Negligible:** The risk will have little to no consequences.
    - **2 - Minor:** The risk may cause some disruption, but mission-critical functions will be maintained.
    - **3 - Significant:** The risk will cause significant degradation of mission capability, requiring substantial effort to restore.
    - **4 - Major:** The risk will cause severe degradation or loss of mission capability.
    - **5 - Catastrophic:** The risk will cause a total loss of mission capability, resulting in severe financial, legal, and reputational damage.
- **Risk Rating:** The overall risk score for each threat was determined by multiplying the likelihood and impact values (Risk = Likelihood x Impact).[3]

5.4 Risk Matrix and Legend

The following table and matrix were used to visually represent and evaluate the risk landscape.

Likelihood	Qualitative Description	Impact	Qualitative Description

5	Almost Certain	5	Catastrophic
4	Likely	4	Major
3	Moderate	3	Significant
2	Unlikely	2	Minor
1	Rare	1	Negligible

	LIKELIHOOD					
IMPACT	**LIKELIHOOD * IMPACT**	**1 Rare**	**2 Unlikely**	**3 Possible**	**4 Likely**	**5 Almost Certain**
	5 Catastrophic					
	4 Major					
	3 Significant					
	2 Minor					
	1 Negligible					

RISK RATING	1 - 5	6 - 10	11 - 15	16 - 25
QUALITY LEVEL	LOW	MEDIUM	HIGH	CRITICAL

5.5 Risk Analysis Table

Risk ID	Threat / Vulnerability	Likelihood (L)	Impact (I)	Risk Rating (L×I)	Risk Level (Legend)
DB-1	SQL Injection attacks	3 (Possible)	5 (Catastrophic)	15	High
DB-2	Unpatched database vulnerabilities	4 (Likely)	4 (Major)	16	Critical
DB-3	Insider misuse (DBAs)	3 (Possible)	4 (Major)	12	High
DB-4	Unencrypted backups stolen	3 (Possible)	5 (Catastrophic)	15	High
DB-5	Weak authentication to database	4 (Likely)	4 (Major)	16	Critical
DB-6	Privilege escalation through vulnerable PL/SQL packages	3 (Possible)	4 (Major)	12	High
DB-7	Denial-of-Service (DoS) attacks	3 (Possible)	3 (Significant)	9	Medium
DB-8	Data leakage through	3 (Possible)	3 (Significant)	9	Medium

	misconfigured roles				
DB-9	Compromise via insecure database links	3 (Possible)	4 (Major)	12	High
DB-10	Social engineering of DBAs	4 (Likely)	4 (Major)	16	Critical

6.0 MITIGATION STRATEGIES AND RECOMMENDATIONS

Mitigating the risks to the Oracle Database 19c requires a blend of immediate technical controls and a long-term strategic shift in security philosophy.

6.1 Technical Controls

- **Prioritize Patching:** A primary mitigation strategy is to apply all available patches and security updates from Oracle as soon as they are available.[32] Oracle releases Critical Patch Updates (CPUs) regularly and delaying these can leave systems vulnerable to known exploits.[34]
- **Database Hardening:**
    - **Enforce Strong Authentication:** Implement and enforce a robust password policy that includes complexity requirements and account lockout after multiple invalid attempts to prevent brute-force attacks.[32] Strong authentication methods like Kerberos or SSL should be used for remote access.[32]
    - **Implement Least Privilege:** Access controls should be implemented based on the principle of least privilege, ensuring that users and applications have only the permissions necessary to perform their duties.[31] Regular audits of privileged accounts and roles are essential to remove excessive or unnecessary access.[32]
    - **Database Firewalls and Activity Monitoring:** Use a database firewall to monitor and block suspicious queries, such as SQL injection attempts.[32] Deploy Database Activity Monitoring (DAM) tools to track and audit all activity on the database.[32]
- **Data Protection:**

- **Encrypt Data:** Data should be encrypted both at rest (in the database and backups) and in transit (across the network) to protect it from unauthorized access.[32]
- **Secure Backups:** Ensure all backups are encrypted, and the backup process is secured to prevent data from being stolen and used to exfiltrate sensitive information.[32]

6.2 Administrative Controls

- **Policy and Procedure:** A formal patch management policy must be developed and enforced, with clear responsibilities, timelines, and a review process.[22] A policy on data classification and data handling must be in place to ensure sensitive data is treated with extra care.[32]
- **Security Awareness Training:** Mandatory and regular security awareness training must be provided to all employees to educate them on identifying phishing attempts and maintaining secure email and remote access practices. DBAs and developers should be trained on secure coding practices, such as using parameterized queries to prevent SQL injection.[32]
- **Disaster Recovery Plan:** A comprehensive and regularly tested disaster recovery plan (DRP) must be in place. This plan should include a strategy for restoring data from encrypted, offsite, and offline backups to ensure business continuity in the event of a major incident like a ransomware attack.[21]

7.0 RISK RERGISTER

This risk register presents the main risks identified for the organization's Oracle Database 19c production instance. It records the description of each risk, its source, consequences, likelihood, inherent and residual ratings, existing controls, planned treatments and responsible owners. The register will be used to monitor and update risk treatments over time to ensure the database remains secure and resilient.

Risk #	Date	Description of Risk	Risk Source	Risk Consequences	Likelihood Rating	Inherent Risk Rating	Existing Controls	Residual Risk Rating	Planned Treatments	Risk Owner	Treatment Due Date	Risk Review Date

DB-1	Sept 2025	SQL Injection attacks	External attackers (web apps)	Unauthorized data access; data modification	3 (Possible) x 5(Catastrophic)	15 (High)	Web application firewall; developer secure coding training	9 (Medium)	Implement parameterized queries; code review; DB firewall	IT Security/Developers	Oct 2025	Jan 2026
DB-2	Sept 2025	Unpatched database vulnerabilities	External attackers	Remote code execution; privilege escalation	4 (Likely) x 4(Major)	16 (Critical)	Regular CPU patching schedule; vulnerability scanning	8 (Medium)	Accelerate patching; automated patch deployment	DBA Team	Oct 2025	Jan 2026
DB-3	Sept 2025	Insider misuse (DBAs)	Internal (DBAs)	Data exfiltration; unauthorized changes	3 (Possible) x 4(Major)	12 (High)	RBAC; audit trails enabled	9 (Medium)	Implement least privilege; PAM; stronger monitoring	IT Security	Nov 2025	Feb 2026
DB-4	Sept 2025	Unencrypted backups stolen	Internal/External theft	Data breach; regulatory fines	3 (Possible) x 5(Catastrophic)	15 (High)	Encryption at rest; restricted backup access	9 (Medium)	Encrypt backups offsite; tighten backup access	DBA Team	Nov 2025	Feb 2026

DB-5	Sept 2025	Weak authentication to database	Internal/External (credential theft)	Credential compromise; unauthorized access	4 (Likely) x 4(Major)	16 (Critical)	Strong password policy; credential vaulting	8 (Medium)	Enforce MFA for DBAs; rotate credentials; vault integration	IT Security	Dec 2025	Mar 2026
DB-6	Sept 2025	Privilege escalation through vulnerable PL/SQL packages	Internal/External	Attackers gain DBA privileges	3 (Possible) x 4(Major)	12 (High)	Periodic package review; patching	9 (Medium)	Disable unused packages; patch regularly	DBA Team	Dec 2025	Mar 2026
DB-7	Sept 2025	Denial-of-Service (DoS) attacks	External attackers	DB unavailability; business disruption	3 (Possible) x (Significant)	9 (Medium)	Resource manager configured; network firewall	6 (Medium)	Rate limiting; advanced firewall rules	IT Security	Dec 2025	Mar 2026
DB-8	Sept 2025	Data leakage through misconfigured roles	Internal (misconfiguration)	Sensitive data exposure; compliance violation	3 (Possible) x 3(Significant)	9 (Medium)	Periodic role/privilege review; least privilege	6 (Medium)	Automate privilege review; tighten grants	DBA Team	Jan 2026	Apr 2026
DB-9	Sept 20	Compromise via insecure datab	External/Internal lateral movement	Lateral movement betwe en	3 (Possible) x 4(Major)	12 (High)	Encryption of DB links; strict link	9 (Medium)	Remove unnecessary DB links;	DBA Team	Jan 2026	Apr 2026

	25	ase links		databases			policies		enforce encryption			
DB-10	Sept 2025	Social engineering of DBAs	External attackers (phishing)	Attackers gain privileged access	4 (Likely) x 4 (Major)	16 (Critical)	Help desk verification procedures; mandatory call-back	8 (Medium)	Mandatory security awareness for DBAs; strict verification	IT Security	Jan 2026	Apr 2026

8.0 CONCLUSION

The Oracle Database 19c, as a central repository for critical data, remains a high-risk asset. The primary risks are associated with sophisticated external threats from cybercriminals and internal threats from misconfigurations or misuse of privileged access. The assessment found that the most significant weaknesses are failure to apply timely security patches, insecure authentication, and improper access controls. While the recommended mitigation strategies can significantly reduce these risks, the sheer number of attack vectors and the history of zero-day exploits necessitate a model of continuous vigilance.

Works cited

1. Keys to Developing an Effective Risk Assessment Methodology - AuditBoard, accessed September 15, 2025, https://auditboard.com/blog/risk-assessment-methodology
2. A Comprehensive Guide to IT Risk Assessments | Omega Systems, accessed September 15, 2025, https://omegasystemscorp.com/insights/white-papers/a-comprehensive-guide-to-it-risk-assessments/

3. How to Rate Impact for Risk Assessments | Information Technology ..., accessed September 15, 2025, https://its.wsu.edu/information-security-services/policies-standards-and-guidelines/how-to-rate-impact-for-risk-assessments/
4. Risk Matrix Template: Assess Risk for Project Success [2025] - Asana, accessed September 15, 2025, https://asana.com/resources/risk-matrix-template
5. A Guide to Understanding 5x5 Risk Assessment Matrix - Safety Culture, accessed September 15, 2025, https://safetyculture.com/topics/risk-assessment/5x5-risk-matrix/
6. Exchange Server editions and versions | Microsoft Learn, accessed September 15, 2025, https://learn.microsoft.com/en-us/exchange/plan-and-deploy/deployment-ref/editions-and-versions
7. What is Microsoft Exchange Server? Key Features & Benefits - NetCom Learning, accessed September 15, 2025, https://www.netcomlearning.com/blog/5-microsoft-exchange-benefits-for-modern-day-enterprises
8. Microsoft Exchange Server - Wikipedia, accessed September 15, 2025, https://en.wikipedia.org/wiki/Microsoft_Exchange_Server
9. Configure Exchange server in on-premises ? what is requirement - Microsoft Learn, accessed September 15, 2025, https://learn.microsoft.com/en-us/answers/questions/1636202/configure-exchange-server-in-on-premises-what-is-r
10. 3 Examples Of IT Risk Assessments You Should Know - Interscale, accessed September 15, 2025, https://interscale.com.au/blog/it-risk-assessment-examples/
11. DCSA Risk Assessment Report (RAR) Template, accessed September 15, 2025, https://www.dcsa.mil/Portals/69/documents/io/rmf/Risk_Assessment_Report_Template_Nov17.docx
12. ISO 27005 | IT Governance USA, accessed September 15, 2025, https://www.itgovernanceusa.com/cyber-security-solutions/iso27001/iso-27005

13. 7 NIST Risk Management Framework (RMF) Steps Explained - IPKeys, accessed September 15, 2025, https://ipkeys.com/blog/rmf-steps/
14. Roles and Responsibilities of Board Members in IT Risk Assessment, accessed September 15, 2025, https://www.360factors.com/blog/roles-responsibilities-board-members-it-risk-assessment/
15. Risk Assessment Methodology for Information Security - ZenGRC, accessed September 15, 2025, https://www.zengrc.com/blog/risky-business-risk-assessments-101/
16. Security Risk Assessment Tool | HealthIT.gov, accessed September 15, 2025, https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
17. Stopping attacks against on-premises Exchange Server and SharePoint Server with AMSI | Microsoft Security Blog, accessed September 15, 2025, https://www.microsoft.com/en-us/security/blog/2025/04/09/stopping-attacks-against-on-premises-exchange-server-and-sharepoint-server-with-amsi/
18. Your guide to qualitative risk analysis for decision-making - Lumivero, accessed September 15, 2025, https://lumivero.com/resources/blog/qualitative-risk-analysis-guide/
19. Risk Assessment Matrix: How to Calculate & Use a Risk Matrix Effectively - Vector Solutions, accessed September 15, 2025, https://www.vectorsolutions.com/resources/blogs/risk-matrix-calculations-severity-probability-risk-assessment/
20. Alert - Active Exploitation of Microsoft Exchange Vulnerabilities - update 4, accessed September 15, 2025, https://www.cyber.gc.ca/en/alerts/active-exploitation-microsoft-exchange-vulnerabilities
21. NSA'S Top Ten Cybersecurity Mitigation Strategies, accessed September 15, 2025, https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf

22. 12 Tips for Mitigating Cyber Risk | JPMorgan Chase, accessed September 15, 2025, https://www.jpmorgan.com/insights/cybersecurity/ransomware/12-tips-for-mitigating-cyber-risk
23. Free Risk Register Template | Confluence - Atlassian, accessed September 15, 2025, https://www.atlassian.com/software/confluence/resources/guides/how-to/risk-register
24. Complete Guide to Systems Hardening [Checklist] - NinjaOne, accessed September 15, 2025, https://www.ninjaone.com/blog/complete-guide-to-systems-hardening/
25. System Hardening Checklist for Systems/Devices - International Trade Administration, accessed September 15, 2025, https://www.trade.gov/sites/default/files/2022-10/Cimcor%20Security%20Guide%20-%20System%20Hardening%20Checklist%20v2.pdf
26. What are the different types of security controls? - Scrut, accessed September 15, 2025, https://www.scrut.io/post/security-control-types
27. The Six Steps of the NIST Risk Management Framework (RMF), accessed September 15, 2025, https://www.micromindercs.com/blog/the-six-steps-of-the-nist-risk-management-framework
28. What Are Security Controls: Types, Functions, and 8 Frameworks to Know | CyCognito, accessed September 15, 2025, https://www.cycognito.com/learn/exposure-management/security-controls.php
29. Comprehensive Guide to Oracle Database 19c: Features, Benefits, and Business Value, accessed September 15, 2025, https://www.certlibrary.com/blog/comprehensive-guide-to-oracle-database-19c-features-benefits-and-business-value/
30. Oracle Database 19c Introduction and Overview, accessed September 15, 2025, https://www.oracle.com/a/tech/docs/database19c-wp.pdf

31. Oracle Database Security - A Technical Primer, accessed September 15, 2025, https://download.oracle.com/database/oracle-database-security-primer.pdf

32. Best Practices for Oracle Database Security - DataSunrise, accessed September 15, 2025, https://www.datasunrise.com/professional-info/oracle-db-security/

33. Checklist CIS Oracle Database 23ai Benchmark - NCP, accessed September 15, 2025, https://ncp.nist.gov/checklist/revision/6642

34. Critical Patch Updates, Security Alerts and Bulletins - Oracle, accessed September 15, 2025, https://www.oracle.com/security-alerts/