CYBER RISK CONTROL ASSESSMENT WORKBOOK

Client: [Client Name]
Engagement: Annual Cyber Risk Assessment
Period: FY 2024
Prepared by: [Audit Team]
Date: [Assessment Date]
Version: 2.1

EXECUTIVE SUMMARY

Engagement Objective

To assess the effectiveness of cybersecurity controls and identify potential risk exposures across the organization's technology infrastructure, data management practices, and security governance framework.

Key Findings Summary

- **High Risk Items:** [X] findings requiring immediate attention
- **Medium Risk Items:** [X] findings requiring remediation within 90 days
- **Low Risk Items:** [X] findings for continuous improvement
- **Overall Risk Rating:** [To be determined based on assessment]

SECTION 1: GOVERNANCE & RISK MANAGEMENT

1.1 Cybersecurity Governance Framework

Control ID: GRC-001
Control Description: Board-level oversight of cybersecurity risks and strategy

Assessment Criteria	Rating	Evidence	Observations
Board receives quarterly cyber risk reports	☐ Effective ☐ Partially Effective ☐ Ineffective		
Cybersecurity strategy aligned with business objectives	☐ Effective ☐ Partially Effective ☐ Ineffective		
Clear roles and responsibilities defined	☐ Effective ☐ Partially Effective ☐ Ineffective		

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

1.2 Risk Assessment Process

Control ID: GRC-002

Control Description: Regular comprehensive cyber risk assessments

Assessment Criteria	Rating	Evidence	Observations
Annual risk assessments conducted	☐ Effective ☐ Partially Effective ☐ Ineffective		
Risk register maintained and updated	☐ Effective ☐ Partially Effective ☐ Ineffective		
Risk appetite clearly defined	☐ Effective ☐ Partially Effective ☐ Ineffective		

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

SECTION 2: ACCESS CONTROLS & IDENTITY MANAGEMENT

2.1 User Access Management

Control ID: IAM-001

Control Description: Proper user provisioning, modification, and deprovisioning processes

Assessment Criteria	Rating	Evidence	Observations
Formal access request/approval process	☐ Effective ☐ Partially Effective ☐ Ineffective		
Segregation of duties enforced	☐ Effective ☐ Partially Effective ☐ Ineffective		
Timely deprovisioning upon termination	☐ Effective ☐ Partially Effective ☐ Ineffective		
Regular access reviews performed	☐ Effective ☐ Partially Effective ☐ Ineffective		

Test Results:

- Sample size: [X] users
- Exceptions noted: [X]
- Exception rate: [X%]

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

2.2 Privileged Access Management

Control ID: IAM-002

Control Description: Controls over privileged and administrative accounts

Assessment Criteria	Rating	Evidence	Observations
Privileged accounts inventory maintained	☐ Effective ☐ Partially Effective ☐ Ineffective		
Multi-factor authentication required	☐ Effective ☐ Partially Effective ☐ Ineffective		
Session monitoring and logging	☐ Effective ☐ Partially Effective ☐ Ineffective		
Regular privileged access reviews	☐ Effective ☐ Partially Effective ☐ Ineffective		

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

SECTION 3: NETWORK & INFRASTRUCTURE SECURITY

3.1 Network Segmentation

Control ID: NET-001

Control Description: Proper network segmentation and zone isolation

Assessment Criteria	Rating	Evidence	Observations
Network architecture documented	☐ Effective ☐ Partially Effective ☐ Ineffective		
DMZ properly configured	☐ Effective ☐ Partially Effective ☐ Ineffective		
Internal network segmentation	☐ Effective ☐ Partially Effective ☐ Ineffective		
VLAN isolation implemented	☐ Effective ☐ Partially Effective ☐ Ineffective		

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

3.2 Firewall Management

Control ID: NET-002

Control Description: Firewall configuration and rule management

Security Tests Performed	Result	Notes
Firewall rule review	☐ Pass ☐ Fail	
Unused rules identification	☐ Pass ☐ Fail	
Change management process	☐ Pass ☐ Fail	
Default deny policy	☐ Pass ☐ Fail	

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

SECTION 4: DATA PROTECTION & ENCRYPTION

4.1 Data Classification & Handling

Control ID: DLP-001

Control Description: Data classification scheme and handling procedures

Assessment Criteria	Rating	Evidence	Observations
Data classification policy exists	☐ Effective ☐ Partially Effective ☐ Ineffective		
Data handling procedures documented	☐ Effective ☐ Partially Effective ☐ Ineffective		
Data retention policies enforced	☐ Effective ☐ Partially Effective ☐ Ineffective		
Secure data disposal procedures	☐ Effective ☐ Partially Effective ☐ Ineffective		

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

4.2 Encryption Controls

Control ID: ENC-001

Control Description: Encryption of data at rest and in transit

Encryption Assessment	Implementation Status	Standard Used	Notes
Database encryption	☐ Implemented ☐ Partial ☐ Not Implemented		
File system encryption	☐ Implemented ☐ Partial ☐ Not Implemented		
Email encryption	☐ Implemented ☐ Partial ☐ Not Implemented		
Web traffic (TLS/SSL)	☐ Implemented ☐ Partial ☐ Not Implemented		

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

SECTION 5: VULNERABILITY MANAGEMENT

5.1 Vulnerability Assessment Program

Control ID: VUL-001

Control Description: Regular vulnerability scanning and remediation

Assessment Criteria	Rating	Evidence	Observations
Regular vulnerability scans performed	☐ Effective ☐ Partially Effective ☐ Ineffective		
Vulnerability management process documented	☐ Effective ☐ Partially Effective ☐ Ineffective		
Risk-based remediation prioritization	☐ Effective ☐ Partially Effective ☐ Ineffective		
Tracking and reporting mechanisms	☐ Effective ☐ Partially Effective ☐ Ineffective		

Vulnerability Statistics:

- Critical vulnerabilities: [X]
- High vulnerabilities: [X]
- Medium vulnerabilities: [X]
- Average remediation time: [X] days

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

5.2 Patch Management

Control ID: VUL-002

Control Description: Timely application of security patches

System Category	Patch Compliance Rate	Target SLA	Notes
Critical systems	[X%]	72 hours	
Production servers	[X%]	30 days	
Workstations	[X%]	30 days	
Network devices	[X%]	60 days	

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

SECTION 6: INCIDENT RESPONSE & MONITORING

6.1 Security Operations Center (SOC)

Control ID: MON-001

Control Description: 24/7 security monitoring and alerting

Assessment Criteria	Rating	Evidence	Observations
SIEM solution implemented	☐ Effective ☐ Partially Effective ☐ Ineffective		
24/7 monitoring coverage	☐ Effective ☐ Partially Effective ☐ Ineffective		
Alert correlation and analysis	☐ Effective ☐ Partially Effective ☐ Ineffective		
Threat intelligence integration	☐ Effective ☐ Partially Effective ☐ Ineffective		

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

6.2 Incident Response Plan

Control ID: IRP-001

Control Description: Formal incident response procedures

Assessment Criteria	Rating	Evidence	Observations
Incident response plan documented	☐ Effective ☐ Partially Effective ☐ Ineffective		
Response team roles defined	☐ Effective ☐ Partially Effective ☐ Ineffective		
Regular tabletop exercises conducted	☐ Effective ☐ Partially Effective ☐ Ineffective		
External communication procedures	☐ Effective ☐ Partially Effective ☐ Ineffective		

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

SECTION 7: BUSINESS CONTINUITY & DISASTER RECOVERY

7.1 Business Continuity Planning

Control ID: BCP-001

Control Description: Business continuity and disaster recovery capabilities

Assessment Criteria	Rating	Evidence	Observations
BCP documented and approved	☐ Effective ☐ Partially Effective ☐ Ineffective		
Recovery objectives defined (RTO/RPO)	☐ Effective ☐ Partially Effective ☐ Ineffective		
Regular testing performed	☐ Effective ☐ Partially Effective ☐ Ineffective		
Plan maintenance and updates	☐ Effective ☐ Partially Effective ☐ Ineffective		

Recovery Objectives:

- Critical systems RTO: [X] hours
- Critical systems RPO: [X] hours
- Last DR test date: [Date]
- Test results: [Pass/Fail/Partial]

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

SECTION 8: THIRD-PARTY RISK MANAGEMENT

8.1 Vendor Risk Assessment

Control ID: TPR-001

Control Description: Third-party cybersecurity risk assessment and monitoring

Assessment Criteria	Rating	Evidence	Observations
Vendor risk assessment process	☐ Effective ☐ Partially Effective ☐ Ineffective		
Security requirements in contracts	☐ Effective ☐ Partially Effective ☐ Ineffective		
Regular vendor security reviews	☐ Effective ☐ Partially Effective ☐ Ineffective		
Vendor incident notification requirements	☐ Effective ☐ Partially Effective ☐ Ineffective		

High-Risk Vendors Identified: [X]

Vendors with access to sensitive data: [X]

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

SECTION 9: COMPLIANCE & REGULATORY REQUIREMENTS

9.1 Regulatory Compliance Assessment

Control ID: COM-001

Control Description: Compliance with applicable cybersecurity regulations

Regulation/Standard	Compliance Status	Gap Analysis	Remediation Plan
SOX IT Controls	☐ Compliant ☐ Partial ☐ Non-Compliant		
GDPR	☐ Compliant ☐ Partial ☐ Non-Compliant		
NIST Cybersecurity Framework	☐ Compliant ☐ Partial ☐ Non-Compliant		
ISO 27001	☐ Compliant ☐ Partial ☐ Non-Compliant		

Risk Rating: ☐ Low ☐ Medium ☐ High

Management Response: [To be completed]

Target Remediation Date: [Date]

SECTION 10: SECURITY AWARENESS & TRAINING

10.1 Security Awareness Program

Control ID: TRA-001

Control Description: Employee cybersecurity awareness and training

Assessment Criteria	Rating	Evidence	Observations
Annual security training program	☐ Effective ☐ Partially Effective ☐ Ineffective		
Phishing simulation exercises	☐ Effective ☐ Partially Effective ☐ Ineffective		
Role-based security training	☐ Effective ☐ Partially Effective ☐ Ineffective		
Training effectiveness measurement	☐ Effective ☐ Partially Effective ☐ Ineffective		

Training Metrics:

- Training completion rate: [X%]
- Phishing simulation click rate: [X%]
- Improvement trend: [Improving/Stable/Declining]

Risk Rating: ☐ Low ☐ Medium ☐ High
Management Response: [To be completed]
Target Remediation Date: [Date]

RISK RATING METHODOLOGY

Risk Assessment Criteria

High Risk:

- Control is ineffective or absent
- Significant likelihood of exploitation
- High potential business impact
- Regulatory compliance concern

Medium Risk:

- Control is partially effective
- Moderate likelihood of exploitation
- Medium potential business impact
- Minor compliance gaps

Low Risk:

- Control is generally effective
- Low likelihood of exploitation
- Minimal potential business impact

- No compliance concerns

MANAGEMENT ACTION PLAN

Priority 1 (High Risk) Items

Finding ID	Description	Target Date	Owner	Status

Priority 2 (Medium Risk) Items

Finding ID	Description	Target Date	Owner	Status

Priority 3 (Low Risk) Items

Finding ID	Description	Target Date	Owner	Status

APPENDICES

Appendix A: Testing Procedures

[Detailed testing procedures and methodologies used during the assessment]

Appendix B: System Inventory

[Complete inventory of systems assessed including versions, configurations, and criticality ratings]

Appendix C: Regulatory Requirements Matrix

[Detailed mapping of controls to applicable regulatory requirements]

Appendix D: Risk Register

[Comprehensive risk register with detailed risk scenarios and mitigations]

Document Control:

- **Classification:** Confidential
- **Distribution:** [List of authorized recipients]
- **Retention Period:** 7 years
- **Next Review Date:** [Date + 1 year]

This workbook template follows industry-standard cybersecurity frameworks including NIST CSF, ISO 27001, and COBIT for comprehensive cyber risk assessment coverage.