SCOPE Framework: Cybersecurity Governance & Risk Management Control Domain

Table of Contents

Originating Component	SCOPE Framework Governance Committee
Releasability	Cleared for public distribution. Available in the SCOPE Framework Hub at [https://timtiptonjr.com/scope-hub].

Purpose: The Governance & Risk Management domain establishes the foundational framework for managing security governance, enterprise risk, third-party risk, security policies, business continuity, and cybersecurity awareness. This domain ensures that security is embedded into organizational strategy, risk is proactively identified and mitigated, policies are structured and enforceable, business resilience is maintained, and personnel are trained to recognize and respond to security threats. By integrating these disciplines, the organization strengthens its overall security posture, regulatory compliance, and operational resilience against evolving risks.

Section 1. Governance, Risk, and Compliance (GRC)

The Governance, Risk, & Compliance (GRC) control family provides a structured framework for aligning security, risk, and compliance efforts with organizational objectives. It ensures that security governance is well-defined, risk management is integrated into decision-making, and compliance obligations are continuously met. This control family facilitates accountability, transparency, and executive oversight in managing security and risk across the enterprise.

1.1 GRC-01: Governance Framework Establishment

The organization shall establish a governance framework that defines the roles, responsibilities, and decision-making authorities for security and risk management. The framework shall be documented, reviewed, and approved by senior leadership to ensure alignment with business objectives and regulatory requirements.

1.2 GRC-02: Security Governance Oversight

The organization shall designate a senior executive or governing body responsible for overseeing the implementation of security and risk management practices, ensuring alignment with enterprise strategy and regulatory obligations.

1.3 GRC-03: Security and Risk Management Roles and Responsibilities

The organization shall define, document, and communicate security and risk management roles and responsibilities for all personnel. This includes executive leadership, security officers, risk managers, compliance officers, and key stakeholders.

1.4 GRC-04: Security and Compliance Governance Committee

The organization shall establish a Security and Compliance Governance Committee that meets periodically to review security risks, compliance status, and overall governance effectiveness. The committee shall include representatives from key business units and risk functions.

1.5 GRC-05: Security and Compliance Risk Integration

The organization shall integrate security and compliance considerations into business strategy, enterprise risk management (ERM), and corporate governance structures to ensure a holistic approach to risk mitigation.

1.6 GRC-06: Compliance Program Implementation

The organization shall develop and implement a compliance program that ensures adherence to applicable legal, regulatory, and industry requirements. The program shall include monitoring, reporting, and remediation mechanisms for compliance violations.

1.7 GRC-07: Regulatory and Legal Obligations Management

The organization shall maintain a process for identifying, assessing, and addressing legal, regulatory, and contractual obligations related to security and privacy. Compliance shall be continuously monitored and updated as regulatory landscapes evolve.

1.8 GRC-08: Risk-Based Decision-Making Framework

The organization shall implement a risk-based decision-making framework that aligns security investment and operational decisions with business risk tolerance, legal requirements, and compliance obligations.

1.9 GRC-09: Risk Governance Accountability

The organization shall establish accountability structures for managing security risks, including documented risk ownership, escalation pathways, and resolution mechanisms.

1.10 GRC-10: Control Framework Alignment

The organization shall align its security control framework with industry best practices to ensure consistency and effectiveness in governance, risk, and compliance practices.

1.11 GRC-11: Security Policy and Standardization Governance

The organization shall implement governance processes for the creation, approval, dissemination, and enforcement of security policies and standards across all operational units.

1.12 GRC-12: Policy Exception Management

The organization shall establish a formal process for requesting, reviewing, and approving exceptions to security policies and controls. Exceptions shall be documented, risk-assessed, and subject to periodic review.

1.13 GRC-13: Ethics and Compliance Reporting Mechanism

The organization shall implement a mechanism for employees, contractors, and stakeholders to report ethics and compliance concerns anonymously and without fear of retaliation.

1.14 GRC-14: Security Awareness and Cultural Integration

The organization shall foster a culture of security awareness by integrating security governance principles into corporate culture, leadership messaging, and employee engagement initiatives.

1.15 GRC-15: Metrics and Continuous Improvement

The organization shall define and track governance, risk, and compliance metrics to measure program effectiveness. Metrics shall be reviewed periodically, and improvements shall be made based on analysis and industry benchmarking.

1.16 GRC-16: Internal and External Audit Coordination

The organization shall establish coordination mechanisms between security governance teams and internal/external auditors to facilitate transparent assessments, regulatory compliance, and risk mitigation efforts.

1.17 GRC-17: Communication and Stakeholder Engagement

The organization shall develop a structured communication plan for engaging internal and external stakeholders in governance, risk, and compliance activities. The plan shall include periodic reporting, escalation procedures, and advisory sessions.

1.18 GRC-18: Governance for Emerging Risks and Technologies

The organization shall periodically assess and update governance structures to address emerging risks, such as cloud security, artificial intelligence, quantum computing, and evolving regulatory requirements.

1.19 GRC-19: Governance for Mergers, Acquisitions, and Divestitures

The organization shall implement governance controls for assessing security risks and compliance implications in mergers, acquisitions, and divestiture activities, ensuring seamless integration and risk mitigation.

1.20 GRC-20: Third-Party Governance Integration

The organization shall ensure that governance, risk, and compliance expectations extend to third-party service providers, partners, and vendors through formalized contracts, assessments, and monitoring mechanisms.

Section 2. Enterprise Risk Management (ERM)

The ERM control family enables the organization to identify, assess, prioritize, and manage risks that could impact business operations, financial performance, regulatory compliance, and strategic objectives. It ensures a structured, risk-based approach to decision-making, integrating risk tolerance and mitigation strategies across all business functions to enhance resilience and adaptability.

2.1 ERM-01: Enterprise Risk Management Framework

The organization shall establish and maintain an enterprise risk management (ERM) framework that integrates risk identification, assessment, response, and monitoring across all business functions.

2.2 ERM-02: Risk Appetite and Tolerance Definition

The organization shall define and document its risk appetite and tolerance levels to guide decision-making and risk acceptance criteria. These shall be reviewed and approved by executive leadership and integrated into operational risk management processes.

2.3 ERM-03: Risk Governance Structure

The organization shall implement a structured risk governance model that assigns risk ownership, establishes escalation pathways, and defines accountability for risk-related decisions.

2.4 ERM-04: Enterprise Risk Identification Process

The organization shall implement a formalized process for identifying risks across all operational, financial, regulatory, and technological domains. Risk identification shall be continuous and include internal and external threat considerations.

2.5 ERM-05: Risk Assessment and Prioritization

The organization shall conduct qualitative and quantitative risk assessments based on impact, likelihood, and business context. Risk prioritization shall be data-driven and support resource allocation for risk treatment.

2.6 ERM-06: Risk Treatment and Mitigation Strategies

The organization shall establish risk treatment plans that outline mitigation, transfer, acceptance, or avoidance strategies. Risk treatments shall be documented and continuously evaluated for effectiveness.

2.7 ERM-07: Risk Aggregation and Reporting

The organization shall develop a centralized risk aggregation and reporting mechanism that consolidates risks across departments, providing executive leadership with a comprehensive view of enterprise risks.

2.8 ERM-08: Continuous Risk Monitoring and Reassessment

The organization shall establish continuous risk monitoring mechanisms to detect emerging threats and changing risk conditions. Risk assessments shall be reassessed periodically or when significant changes occur.

2.9 ERM-09: Key Risk Indicators (KRIs) Implementation

The organization shall define and monitor Key Risk Indicators (KRIs) to provide early warnings of potential risk events. KRIs shall be aligned with enterprise objectives and reviewed regularly for relevance.

2.10 ERM-10: Risk-Based Decision-Making Integration

The organization shall integrate risk considerations into strategic planning, investment decisions, and operational processes, ensuring that risk exposure is factored into decision-making.

2.11 ERM-11: Scenario Analysis and Stress Testing

The organization shall conduct scenario-based risk analysis and stress testing exercises to evaluate the resilience of business operations under adverse conditions.

2.12 ERM-12: Risk Communication and Awareness

The organization shall implement structured communication protocols for informing stakeholders about enterprise risks, mitigation plans, and response strategies.

2.13 ERM-13: Third-Party and Supply Chain Risk Management

The organization shall assess and manage risks associated with third-party vendors, suppliers, and partners, ensuring that enterprise risk exposure is minimized through contractual agreements and continuous monitoring.

2.14 ERM-14: Regulatory and Compliance Risk Management

The organization shall monitor and assess regulatory and compliance risks to ensure adherence to evolving legal, industry, and contractual obligations.

2.15 ERM-15: Risk Escalation and Exception Handling

The organization shall establish a formal process for escalating high-priority risks to executive leadership and managing exceptions to risk policies through documented justifications and compensating controls.

2.16 ERM-16: Enterprise Risk Management Maturity Evaluation

The organization shall periodically assess and benchmark its ERM program against industry best practices to ensure continuous improvement and maturity progression.

2.17 ERM-17: Risk Integration in Mergers, Acquisitions, and Divestitures

The organization shall conduct risk assessments during mergers, acquisitions, and divestitures to evaluate security, financial, and operational risks associated with business transitions.

2.18 ERM-18: Emerging Risk Identification and Adaptation

The organization shall establish processes to identify, analyze, and adapt to emerging risks, including geopolitical, economic, technological, and environmental threats.

2.19 ERM-19: Cyber Risk Management Alignment

The organization shall integrate cybersecurity risk management within the broader ERM framework, ensuring cyber threats and vulnerabilities are assessed and addressed at the enterprise level.

2.20 ERM-20: Business Impact Analysis (BIA) Integration

The organization shall incorporate business impact analysis (BIA) findings into enterprise risk management activities to align risk prioritization with business continuity objectives.

Section 3. Third-Party Risk Management (TPR)

The TPR control family governs the assessment, monitoring, and mitigation of risks associated with third-party relationships, including vendors, suppliers, and service providers. It ensures that external entities adhere to security requirements, contractual obligations, and regulatory standards, reducing the risk exposure from supply chain vulnerabilities and outsourced services.

3.1 TPR-01: Third-Party Risk Management Program Establishment

The organization shall establish a formal Third-Party Risk Management (TPRM) program to assess, monitor, and mitigate risks associated with vendors, suppliers, contractors, and partners.

3.2 TPR-02: Third-Party Classification and Tiering

The organization shall implement a classification and tiering methodology to categorize third parties based on their risk impact, access to sensitive data, and business criticality.

3.3 TPR-03: Due Diligence and Vendor Pre-Screening

The organization shall conduct comprehensive due diligence before engaging third parties, including security assessments, financial stability reviews, regulatory compliance checks, and background verification.

3.4 TPR-04: Contractual Security and Compliance Requirements

The organization shall require all third parties to adhere to security, compliance, and risk management standards through legally binding contracts, including service-level agreements (SLAs), data protection clauses, and audit rights.

3.5 TPR-05: Continuous Vendor Risk Monitoring

The organization shall implement a process for continuously monitoring third-party security posture, compliance status, and operational risks throughout the vendor lifecycle.

3.6 TPR-06: Third-Party Access Control and Least Privilege Enforcement

The organization shall enforce least privilege access controls for third parties, ensuring they only have access to systems, data, and assets necessary for their contractual obligations.

3.7 TPR-07: Vendor Security Assessments and Audits

The organization shall conduct periodic security assessments and audits of high-risk third parties to validate compliance with security policies, industry regulations, and contractual obligations.

3.8 TPR-08: Incident Response and Notification Requirements for Third Parties

The organization shall require third parties to have an incident response plan in place and promptly report security incidents, data breaches, or compliance violations affecting the organization.

3.9 TPR-09: Supply Chain Security and Risk Mitigation

The organization shall evaluate and mitigate risks related to supply chain dependencies, including risks from fourth parties (subcontractors, downstream suppliers) and geopolitical factors.

3.10 TPR-10: Data Protection and Privacy Obligations for Third Parties

The organization shall ensure that third parties handling sensitive data implement appropriate data protection, encryption, and privacy controls in accordance with legal and regulatory requirements.

3.11 TPR-11: Third-Party Risk Metrics and Reporting

The organization shall define key risk indicators (KRIs) and performance metrics for third-party risk management, ensuring leadership visibility into vendor-related risks and trends.

3.12 TPR-12: Offboarding and Contract Termination Controls

The organization shall implement a structured offboarding process for third parties, ensuring proper data sanitization, access revocation, and risk reassessment upon contract termination.

3.13 TPR-13: Critical Vendor Contingency Planning

The organization shall require critical third parties to maintain business continuity and disaster recovery plans, ensuring resilience and service availability in the event of disruptions.

3.14 TPR-14: Cloud and Managed Service Provider Risk Management

The organization shall assess and govern risks associated with cloud service providers (CSPs), managed security service providers (MSSPs), and other technology outsourcing vendors.

3.15 TPR-15: Third-Party Security Awareness and Training Requirements

The organization shall mandate that third parties handling sensitive data or critical systems participate in security awareness and compliance training programs.

3.16 TPR-16: Vendor Risk Exception Handling

The organization shall establish a formalized process for evaluating and approving risk exceptions for third parties, including documented justifications, risk assessments, and compensating controls.

3.17 TPR-17: Legal and Compliance Review of Third-Party Contracts

The organization shall require legal and compliance teams to review third-party agreements to ensure risk, security, and regulatory obligations are properly addressed.

3.18 TPR-18: Secure Development and Code Review for Software Vendors

The organization shall require third-party software vendors to adhere to secure coding practices, undergo code reviews, and provide a Software Bill of Materials (SBOM) where applicable.

3.19 TPR-19: Insider Threat Risk Mitigation for Third-Party Personnel

The organization shall assess insider threat risks associated with third-party personnel, ensuring background checks, monitoring controls, and access reviews are in place.

Section 4. Security Policy & Standards Development (SPS)

The SPS control family ensures the organization establishes, maintains, and enforces security policies, standards, and guidelines that govern cybersecurity practices. It provides a structured approach to defining security expectations, aligning policies with regulatory requirements, and ensuring consistency in control implementation across the enterprise.

4.1 SPS-01: Security Policy Framework Development

The organization shall establish a structured security policy framework that defines security objectives, principles, and mandatory requirements aligned with business needs and regulatory obligations.

4.2 SPS-02: Policy Governance and Ownership

The organization shall assign ownership of security policies to designated personnel or committees, ensuring accountability for policy development, updates, and enforcement.

4.3 SPS-03: Policy Review and Approval Process

The organization shall implement a formalized process for drafting, reviewing, approving, and disseminating security policies, ensuring alignment with risk management strategies and business priorities.

4.4 SPS-04: Standards and Baseline Development

The organization shall develop security standards and baselines to support the enforcement of security policies, ensuring consistent implementation of security controls across all systems and environments.

4.5 SPS-05: Policy Harmonization and Regulatory Mapping

The organization shall ensure that security policies align with applicable laws, regulations, industry frameworks, and contractual obligations through a structured mapping and harmonization process.

4.6 SPS-06: Security Policy Exceptions and Waiver Management

The organization shall define a formal process for requesting, evaluating, and approving exceptions to security policies. Exceptions shall include risk assessments, documented compensating controls, and periodic reviews.

4.7 SPS-07: Policy Dissemination and Accessibility

The organization shall ensure that security policies and standards are easily accessible to all relevant personnel through centralized documentation repositories, training programs, and internal communication channels.

4.8 SPS-08: Security Policy Change Management

The organization shall implement a change management process for security policies, ensuring that updates are assessed for impact, communicated effectively, and implemented in a controlled manner.

4.9 SPS-09: Policy Awareness and Enforcement Mechanisms

The organization shall establish mechanisms to ensure personnel acknowledge security policies and understand their enforcement, including mandatory attestation and disciplinary actions for non-compliance.

4.10 SPS-10: Technical Standards for Security Control Implementation

The organization shall define technical security standards that prescribe minimum security configurations, hardening guidelines, and control implementations for infrastructure, applications, and cloud environments.

4.11 SPS-11: Secure Configuration Management Standards

The organization shall establish and maintain secure configuration standards for operating systems, network devices, databases, and applications to minimize security vulnerabilities.

4.12 SPS-12: Policy Integration into IT and Business Processes

The organization shall integrate security policies and standards into IT management, software development, procurement, and operational business processes to ensure security by design.

4.13 SPS-13: Policy Enforcement and Compliance Audits

The organization shall conduct periodic compliance audits to validate adherence to security policies and standards, identify policy violations, and implement corrective actions.

4.14 SPS-14: Security Guidelines for Emerging Technologies

The organization shall develop and update security policies and guidelines addressing emerging technologies such as cloud computing, AI/ML, quantum security, and IoT.

4.15 SPS-15: Secure Data Handling and Classification Standards

The organization shall define data classification standards and security policies governing the handling, storage, transmission, and disposal of sensitive and regulated data.

4.16 SPS-16: Cryptographic Standards and Key Management Policies

The organization shall establish cryptographic standards, including encryption protocols, hashing algorithms, and key management policies, ensuring compliance with industry best practices.

4.17 SPS-17: Access and Identity Management Policy Development

The organization shall develop policies governing identity lifecycle management, authentication, authorization, privileged access, and account review requirements.

4.18 SPS-18: Endpoint and Mobile Security Policy Development

The organization shall define security policies governing endpoint devices, mobile device management (MDM), remote work security, and acceptable use of corporate assets.

4.19 SPS-19: Security Policy Metrics and Performance Evaluation

The organization shall establish metrics to evaluate the effectiveness of security policies, track policy compliance, and support continuous improvement efforts.

4.20 SPS-20: Vendor and Third-Party Security Policy Requirements

The organization shall develop security policy requirements that third-party vendors, suppliers, and service providers must adhere to, ensuring alignment with enterprise security standards.

Section 5. Business Continuity & Disaster Recovery (BCM)

The BCM control family ensures the organization can maintain critical operations and recover from disruptive events, including cyber incidents, natural disasters, and system failures. It establishes business continuity planning, disaster recovery strategies, and resilience measures to minimize operational downtime and financial loss.

5.1 BCM-01: Business Continuity Management Program Establishment

The organization shall establish and maintain a Business Continuity Management (BCM) program that ensures operational resilience, continuity of critical services, and effective disaster recovery planning.

5.2 BCM-02: Business Impact Analysis (BIA) Execution

The organization shall conduct and regularly update a Business Impact Analysis (BIA) to identify mission-critical processes, assess potential disruptions, and define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

5.3 BCM-03: Risk Assessment for Business Disruptions

The organization shall perform risk assessments to identify threats that could impact business operations, including natural disasters, cyber incidents, supply chain disruptions, and geopolitical risks.

5.4 BCM-04: Business Continuity Plan (BCP) Development

The organization shall develop, document, and maintain a Business Continuity Plan (BCP) that outlines strategies, procedures, and resources required to sustain critical business functions during a disruption.

5.5 BCM-05: Disaster Recovery Plan (DRP) Development

The organization shall establish a Disaster Recovery Plan (DRP) that includes technical recovery procedures for IT systems, networks, applications, and data to ensure timely restoration following an incident.

5.6 BCM-06: Incident Escalation and Crisis Management Protocols

The organization shall define and implement escalation procedures for business disruptions, including crisis communication strategies, decision-making hierarchies, and emergency response coordination.

5.7 BCM-07: Redundancy and High Availability Requirements

The organization shall implement redundancy and high-availability measures for critical infrastructure, applications, and data to minimize service disruptions and ensure continuous operations.

5.8 BCM-08: Backup and Data Recovery Procedures

The organization shall establish backup policies and data recovery procedures that ensure regular, secure, and tested backups of critical business data, applications, and configurations.

5.9 BCM-09: Alternate Site and Work Location Strategies

The organization shall define and maintain alternate site strategies, including data center failover, remote work enablement, and offsite operational continuity solutions.

5.10 BCM-10: Business Continuity and Disaster Recovery Testing

The organization shall conduct regular testing of BCP and DRP plans, including tabletop exercises, full-scale simulations, and failover drills to validate effectiveness and identify gaps.

5.11 BCM-11: Supply Chain and Vendor Continuity Planning

The organization shall ensure that key vendors and suppliers maintain business continuity plans, disaster recovery capabilities, and contractual obligations to support operational resilience.

5.12 BCM-12: Employee Training and Awareness on Continuity Planning

The organization shall provide business continuity and disaster recovery training to employees, ensuring personnel understand roles, responsibilities, and response procedures during disruptions.

5.13 BCM-13: Emergency Communications and Notification Systems

The organization shall establish and maintain an emergency communication plan, ensuring stakeholders receive timely and accurate information regarding disruptions, recovery status, and contingency actions.

5.14 BCM-14: Legal, Regulatory, and Compliance Considerations in Continuity Planning

The organization shall ensure BCP and DRP activities comply with relevant legal, regulatory, and contractual requirements, including industry-specific continuity and resilience mandates.

5.15 BCM-15: Remote Work and Telecommuting Resilience

The organization shall develop policies and technological capabilities to support remote work continuity, ensuring secure access, collaboration, and operational functionality during disruptions.

5.16 BCM-16: Resilience Metrics and Performance Monitoring

The organization shall define key performance indicators (KPIs) and resilience metrics to measure the effectiveness of business continuity and disaster recovery strategies.

5.17 BCM-17: Financial Resilience and Contingency Planning

The organization shall develop financial contingency plans, including liquidity reserves, insurance coverage, and alternative funding strategies to sustain operations during prolonged disruptions.

5.18 BCM-18: Cyber Resilience Integration into Business Continuity

The organization shall incorporate cybersecurity incident scenarios into business continuity planning, ensuring preparedness for ransomware attacks, data breaches, and denial-of-service (DoS) events.

5.19 BCM-19: Post-Incident Review and Continuous Improvement

The organization shall conduct post-incident reviews following disruptions, identifying lessons learned, process improvements, and remediation actions to enhance future resilience.

5.20 BCM-20: Executive and Board-Level Oversight of Business Continuity

The organization shall ensure that business continuity and disaster recovery programs receive executive and board-level oversight, with periodic reporting on program effectiveness and strategic risks.

Section 6. Cybersecurity Awareness & Training (CAT)

The CAT control family fosters a security-conscious culture by equipping employees, contractors, and stakeholders with the knowledge and skills to identify and respond to security threats. It ensures that personnel receive role-specific security training, reinforcing best practices and reducing human-related security risks across the organization.

6.1 CAT-01: Cybersecurity Awareness Program Establishment

The organization shall develop and maintain a cybersecurity awareness program that educates employees, contractors, and stakeholders on security risks, best practices, and compliance obligations.

6.2 CAT-02: Role-Based Security Training

The organization shall implement tailored cybersecurity training based on roles and responsibilities, ensuring personnel in high-risk roles (e.g., IT administrators, executives, developers) receive specialized security education.

6.3 CAT-03: Phishing and Social Engineering Awareness Training

The organization shall conduct periodic phishing simulations and social engineering awareness training to educate employees on recognizing and reporting fraudulent activities.

6.4 CAT-04: Secure Behavior Reinforcement Mechanisms

The organization shall implement reinforcement mechanisms such as periodic security reminders, gamification, reward systems, and mandatory refresher training to sustain secure behavior.

6.5 CAT-05: Secure Coding and Development Training

The organization shall require developers and software engineers to complete secure coding training aligned with industry standards (e.g., OWASP, NIST) to mitigate vulnerabilities in applications.

6.6 CAT-06: Cyber Hygiene and Endpoint Security Training

The organization shall train personnel on fundamental cyber hygiene practices, including password management, device security, software updates, and safe browsing habits.

6.7 CAT-07: Security Awareness for Executives and Leadership

The organization shall provide cybersecurity awareness sessions for executives and board members, focusing on strategic risks, compliance requirements, and governance responsibilities.

6.8 CAT-08: Incident Response and Reporting Training

The organization shall train employees on identifying security incidents and following established reporting procedures to ensure timely response and containment of threats.

6.9 CAT-09: Compliance and Regulatory Security Training

The organization shall provide training on compliance obligations relevant to the workforce, including data protection laws, industry standards, and organizational security policies.

6.10 CAT-10: Third-Party and Vendor Security Awareness

The organization shall extend security awareness training requirements to third-party vendors, contractors, and partners handling sensitive data or accessing critical systems.

6.11 CAT-11: Secure Remote Work and BYOD Training

The organization shall provide security awareness training for employees working remotely or using personal devices (BYOD), covering topics such as VPN usage, endpoint security, and data protection.

6.12 CAT-12: Insider Threat Awareness Training

The organization shall educate employees on identifying insider threat indicators, emphasizing the importance of reporting suspicious behavior and safeguarding sensitive information.

6.13 CAT-13: Cybersecurity Training for Non-Technical Employees

The organization shall offer cybersecurity awareness training for non-technical employees, ensuring all personnel understand their role in protecting corporate assets and data.

6.14 CAT-14: Threat Landscape and Emerging Risk Education

The organization shall periodically update training content to reflect evolving cybersecurity threats, attack techniques, and risk trends relevant to the organization’s industry.

6.15 CAT-15: Security Awareness Metrics and Performance Tracking

The organization shall measure the effectiveness of cybersecurity awareness programs through testing, assessments, participation rates, and behavior analysis to improve training content.

6.16 CAT-16: Security Awareness Integration into Onboarding

The organization shall incorporate cybersecurity awareness training into the new hire onboarding process, ensuring employees understand security policies and best practices from day one.

6.17 CAT-17: Crisis Simulation and Tabletop Exercises

The organization shall conduct cybersecurity tabletop exercises and crisis simulations for leadership, security teams, and business units to enhance incident response preparedness.

6.18 CAT-18: Public-Facing Cybersecurity Awareness Initiatives

The organization shall engage in public cybersecurity awareness efforts, such as community outreach, customer security education, and partnerships with industry groups to promote cybersecurity best practices.

6.19 CAT-19: Cybersecurity Awareness Policy and Accountability

The organization shall define a policy requiring mandatory security training participation, with accountability measures for non-compliance, including potential disciplinary actions.

6.20 CAT-20: Continuous Learning and Advanced Security Training

The organization shall offer continuous learning opportunities, including access to cybersecurity certifications, industry conferences, and advanced security workshops for personnel seeking to enhance their expertise.