SCOPE Framework: Cloud & Emerging Technologies Security 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 Cloud & Emerging Technologies Security domain addresses the unique security requirements, operational risks, and architectural challenges introduced by modern cloud platforms and rapidly evolving technologies. This domain ensures that cloud environments are continuously monitored and aligned with secure configurations and novel technologies such as AI/ML, quantum computing, IoT, blockchain, and smart city infrastructure are secured with tailored, forward-looking controls. By embedding security into the design, deployment, and operation of these technologies, the organization enables innovation while maintaining trust, resilience, and regulatory alignment across digital transformation efforts.

Section 1. Cloud Security Posture Management (CSP)

As organizations increasingly adopt cloud services across multi-cloud and hybrid-cloud environments, maintaining a continuous and resilient security posture becomes paramount. The Cloud Security Posture Management (CSP) control family focuses on the automated and programmatic enforcement, visibility, and remediation of security misconfigurations, policy violations, and drift within cloud infrastructure. These controls ensure cloud environments remain aligned with enterprise security baselines, compliance requirements, and evolving threat landscapes.

1.1 CSP-01: Cloud Configuration Baseline Enforcement

Organizations shall define, document, and enforce cloud service configuration baselines for each provider and service in use, using standardized templates and validated industry benchmarks (e.g., CIS, CSA).

1.2 CSP-02: Continuous Configuration Monitoring

Automated tools shall be deployed to continuously monitor for unauthorized changes, misconfigurations, or deviations from approved cloud configuration baselines.

1.3 CSP-03: Asset Discovery and Inventory

Cloud-native and third-party tools shall be implemented to maintain a real-time inventory of all cloud assets, including compute, storage, network, and serverless resources across accounts and providers.

1.4 CSP-04: Identity & Entitlement Visibility

Organizations shall maintain centralized visibility into all cloud identities, roles, and entitlements, and ensure permissions are regularly reviewed for alignment with least privilege principles.

1.5 CSP-05: Policy-as-Code Implementation

Security and compliance policies shall be codified and version-controlled using Policy-as-Code frameworks (e.g., Open Policy Agent, Sentinel), with enforcement embedded in CI/CD and runtime pipelines.

1.6 CSP-06: Automated Remediation Workflows

Cloud misconfigurations and violations of policy shall trigger automated remediation workflows where feasible, with escalation paths defined for high-risk findings requiring manual intervention.

1.7 CSP-07: Multi-Cloud Posture Standardization

Security posture standards shall be normalized across multiple cloud service providers to ensure consistent enforcement regardless of platform-specific implementations.

1.8 CSP-08: Cloud Account Onboarding Control

Procedures shall be established for securely onboarding new cloud accounts or subscriptions, including enforcement of default security controls and monitoring integration prior to go-live.

1.9 CSP-09: Data Residency and Sovereignty Checks

Cloud posture assessments shall verify that data storage and processing align with jurisdictional, regulatory, and organizational data residency requirements.

1.10 CSP-10: Misconfiguration Detection for PaaS/SaaS

Security tooling shall extend beyond IaaS to detect configuration drift and exposure within PaaS and SaaS platforms, including storage buckets, APIs, and collaboration tools.

1.11 CSP-11: Encryption Configuration Validation

Posture tools shall validate that encryption-at-rest and in-transit is configured and enforced for all applicable cloud services and storage mechanisms.

1.12 CSP-12: Public Exposure Identification

Automated controls shall flag and report resources with public accessibility and validate alignment with approved access policies.

1.13 CSP-13: Anomaly Detection in Configuration Drift

Machine learning and behavior-based tools shall be used to detect unusual configuration changes or drifts that may signal insider threats or compromise.

1.14 CSP-14: Role & Policy Drift Detection

Controls shall be in place to detect and report on unauthorized changes to IAM roles, policies, or trust relationships that deviate from the established baseline.

1.15 CSP-15: Tagging Compliance Enforcement

All cloud assets shall be required to follow tagging standards, and posture tools shall identify assets that lack mandatory tags related to ownership, environment, and data classification.

1.16 CSP-16: Integration with CI/CD Pipelines

Cloud posture assessments shall be integrated into DevOps pipelines to validate infrastructure-as-code templates prior to deployment, blocking those with critical misconfigurations.

1.17 CSP-17: Risk Scoring & Prioritization

Detected posture violations shall be risk-scored based on asset criticality, exposure level, and threat intelligence to guide remediation prioritization.

1.18 CSP-18: Reporting & Dashboarding Capabilities

Organizations shall maintain dashboards that provide stakeholders with real-time and historical visibility into cloud security posture, violations, trends, and remediation status.

1.19 CSP-19: API & Infrastructure Drift Monitoring

Posture management tools shall monitor API-driven changes to cloud infrastructure to detect unauthorized or undocumented changes made outside of change management procedures.

1.20 CSP-20: Regulatory & Compliance Alignment Mapping

Cloud posture controls shall be mapped to applicable regulatory and compliance frameworks, with reporting capabilities to support audits.

1.21 CSP-21: Third-Party Integration Security Validation

All third-party services and tools integrated into cloud environments shall be evaluated for posture impact, with continuous monitoring of their privileges, data access, and compliance with cloud security policies.

1.22 CSP-22: Credential and Access Token Exposure Scanning

Automated scanning shall detect exposed access keys, credentials, or tokens in storage repositories, logs, or IaC, triggering immediate remediation protocols.

Section 2. AI/ML & Quantum Security (AQS)

The AI/ML & Quantum Security (AQS) control family addresses the emerging and rapidly evolving risks introduced by artificial intelligence, machine learning systems, and quantum computing. These controls focus on ensuring trust, integrity, and transparency in AI/ML pipelines, while preparing cryptographic systems and enterprise architectures for the disruptive potential of quantum computing. AQS safeguards both traditional environments integrating AI/ML capabilities and organizations anticipating the post-quantum era.

2.1 AQS-01: AI Model Provenance & Lineage Tracking

Organizations shall maintain detailed lineage tracking of AI/ML models, including data sources, algorithmic logic, training parameters, and versioning metadata to ensure traceability and reproducibility.

2.2 AQS-02: Model Poisoning & Data Drift Detection

Controls shall be implemented to detect poisoning attacks on training datasets and monitor for data drift that may degrade model performance or introduce unintentional bias over time.

2.3 AQS-03: Explainability & Interpretability Enforcement

All deployed AI/ML models shall include mechanisms for explainability to ensure decisions can be understood and challenged by human reviewers, especially in regulated or high-risk use cases.

2.4 AQS-04: Training Dataset Integrity Validation

Data used for training AI/ML models shall be validated for completeness, labeling accuracy, and freedom from adversarial manipulation or tampering.

2.5 AQS-05: Adversarial Input Defense Mechanisms

AI/ML applications shall include safeguards against adversarial inputs designed to manipulate outputs or cause unintended behavior, especially in computer vision and NLP models.

2.6 AQS-06: AI Model Repository Access Control

Access to AI model repositories shall be restricted through identity-based access controls, with change tracking and deployment approvals enforced for all updates.

2.7 AQS-07: Quantum-Resistant Cryptographic Planning

Organizations shall assess current cryptographic dependencies and develop roadmaps for transitioning to quantum-resistant algorithms in alignment with NIST PQC standards.

2.8 AQS-08: Post-Quantum Risk Assessments

Annual assessments shall be conducted to identify enterprise systems at risk of future quantum-based cryptographic compromise, including key exchange mechanisms and digital signatures.

2.9 AQS-09: Algorithmic Bias Testing & Remediation

AI/ML models shall be tested for algorithmic bias against protected classes and sensitive variables, with defined procedures to retrain or adjust models as needed.

2.10 AQS-10: AI-Specific Threat Modeling

Threat modeling exercises shall be performed on AI/ML pipelines to identify risks unique to data ingestion, model training, deployment, and feedback loops.

2.11 AQS-11: AI Output Monitoring for Anomalies

Automated monitoring shall be established to detect anomalies in AI output, such as hallucinations, outlier recommendations, or logic errors due to unforeseen inputs.

2.12 AQS-12: ML Pipeline Segmentation & Isolation

Critical components of the ML lifecycle—such as training environments, inference engines, and data pipelines—shall be logically segmented and monitored for unauthorized interaction.

2.13 AQS-13: Model Confidentiality Protections

Deployed AI/ML models shall be protected from extraction attacks through methods such as differential privacy, watermarking, or obfuscation to prevent reverse engineering.

2.14 AQS-14: Synthetic Data Security Controls

Synthetic data generated for model training or testing shall be reviewed to ensure it does not unintentionally replicate sensitive or regulated data patterns.

2.15 AQS-15: Autonomous System Override Controls

AI-enabled autonomous systems shall include manual override mechanisms and defined escalation paths to human operators for safety, ethics, and legal accountability.

2.16 AQS-16: Model Deployment Approval Governance

All production deployments of AI/ML models shall undergo a formal approval process that includes peer review, security validation, and business alignment.

2.17 AQS-17: Quantum Cryptanalysis Monitoring

Organizations shall monitor academic, government, and industry advancements in quantum cryptanalysis to anticipate breakthroughs impacting existing cryptographic safeguards.

2.18 AQS-18: Edge AI Security Protections

AI models deployed to edge devices (e.g., IoT, mobile, robotics) shall include runtime tamper protections, encrypted storage of model files, and remote revocation capabilities.

2.19 AQS-19: AI Ethics & Use Case Review Board

A cross-functional review board shall evaluate proposed AI use cases for ethical implications, misuse potential, and adherence to organizational values and legal constraints.

2.20 AQS-20: External Model & API Vetting

Any externally acquired AI models or third-party AI APIs shall undergo security reviews to assess data handling practices, model behavior, and exposure to malicious inference.

2.21 AQS-21: PQC Transition Testing in Lab Environments

Pilot testing of post-quantum cryptographic libraries and protocols shall be conducted in lab or simulation environments to evaluate performance, interoperability, and migration readiness.

2.22 AQS-22: Regulatory Alignment for AI & Quantum

AI/ML and quantum preparedness efforts shall be mapped to applicable laws, standards, and emerging regulatory frameworks (e.g., EU AI Act, NIST AI RMF, EO 14028) to ensure compliance.

Section 3. IoT & OT Security (IOT)

The IoT & OT Security (IOT) control family establishes the baseline security expectations and operational safeguards necessary to protect environments leveraging Internet of Things (IoT) and Operational Technology (OT) assets. These systems, which often bridge physical and digital infrastructure, pose unique challenges due to constrained devices, legacy protocols, and real-time operational demands. IOT controls are tailored to address lifecycle management, network segregation, secure firmware practices, and real-world risk mitigation specific to IoT and OT ecosystems.

3.1 IOT-01: Asset Classification & Inventory for IoT/OT Devices

Organizations shall maintain a continuously updated and categorized inventory of all IoT and OT devices, including make, model, firmware version, physical location, and assigned function.

3.2 IOT-02: Network Segmentation for IoT/OT Systems

IoT and OT environments shall be logically segmented from enterprise and internet-facing networks using VLANs, firewalls, and unidirectional gateways where appropriate.

3.3 IOT-03: Protocol Whitelisting for OT Communications

Only explicitly approved protocols (e.g., Modbus, DNP3, OPC-UA) shall be permitted within OT zones, and all traffic shall be logged and monitored for anomalies.

3.4 IOT-04: Secure Device Onboarding Process

A formalized onboarding process shall be used for IoT/OT device deployment, which includes identity verification, initial configuration hardening, and secure provisioning.

3.5 IOT-05: Default Credential Elimination

All default credentials on IoT and OT devices shall be changed during provisioning, and password complexity policies shall be enforced where device capability allows.

3.6 IOT-06: Firmware Validation and Signing

All firmware updates shall be cryptographically signed, verified upon installation, and sourced from authenticated and trusted channels only.

3.7 IOT-07: Physical Tamper Resistance & Detection

IoT and OT devices located in uncontrolled or semi-controlled environments shall include tamper-evident features and detection mechanisms that alert on physical access or manipulation.

3.8 IOT-08: Wireless Protocol Security Controls

Wireless communications used by IoT devices (e.g., Zigbee, BLE, LoRaWAN) shall be encrypted and authenticated using the strongest supported standards, with key rotation enforced.

3.9 IOT-09: Legacy OT System Hardening

Legacy OT systems without native security controls shall be hardened using compensating controls such as protocol break proxies, secure enclaves, or access mediation gateways.

3.10 IOT-10: Device Function Restriction by Role

IoT/OT device functionality shall be configured to operate only in alignment with its designated role, disabling unused ports, services, and administrative interfaces.

3.11 IOT-11: Time Synchronization with Trusted Sources

All IoT/OT devices shall synchronize time with approved NTP sources to support log integrity, operational consistency, and forensic traceability.

3.12 IOT-12: Logging & Audit Capabilities in Resource-Constrained Devices

Where device limitations exist, centralized log collection agents or lightweight logging proxies shall be used to ensure operational visibility and event correlation.

3.13 IOT-13: Remote Management Access Control

Remote access to IoT/OT devices shall be restricted to authorized administrators through encrypted channels, with session logging and time-bound access policies enforced.

3.14 IOT-14: Operational Safety Interlocks

IoT/OT systems interfacing with physical equipment or human safety mechanisms shall implement safety interlocks to prevent unintended or unsafe actions resulting from compromise.

3.15 IOT-15: Patch Applicability & Risk-Based Scheduling

Patching for IoT and OT devices shall be evaluated for operational impact, and applied using risk-based schedules, prioritizing vulnerabilities with active exploitation or safety implications.

3.16 IOT-16: Traffic Behavior Baselines

Behavioral baselining of IoT/OT device traffic shall be established and used to detect deviations that may indicate compromise, lateral movement, or malfunction.

3.17 IOT-17: OT System Remote Firmware Rollback Capability

Firmware rollback functionality shall be tested and available for OT systems in the event that a new firmware introduces instability or unanticipated behavior.

3.18 IOT-18: Procurement Security Requirements for Devices

Security requirements—including secure boot, update capabilities, and end-of-life support policies—shall be included in procurement criteria for all IoT and OT device acquisitions.

3.19 IOT-19: Maintenance & Field Technician Identity Validation

All field technician access to IoT/OT systems shall require strong identity verification and time-based authorization controls to prevent unauthorized servicing or modification.

3.20 IOT-20: End-of-Life Device Decommissioning Procedure

IoT/OT devices that reach end-of-life shall be securely decommissioned using processes that remove all data, cryptographic keys, and network credentials from memory and storage.

3.21 IOT-21: Insider Threat Controls for Critical OT Infrastructure

Insider threat detection and mitigation measures shall be extended to personnel with access to OT environments, including behavior analytics, background checks, and access reviews.

3.22 IOT-22: Safety & Control System Redundancy

Critical OT safety systems shall be designed with physical and logical redundancy to preserve integrity and availability during security events, malfunctions, or targeted disruptions.

Section 4. Blockchain Security (BCS)

The Blockchain Security (BCS) control family establishes safeguards for the secure design, deployment, and operation of blockchain-based technologies—whether public, private, or consortium-based. These controls address the decentralized nature of blockchain systems, smart contract integrity, consensus mechanism trust, and the proper handling of cryptographic elements inherent to distributed ledger technologies. BCS ensures that blockchain integrations do not introduce systemic risk, data compromise, or operational instability to the broader enterprise ecosystem.

4.1 BCS-01: Node Identity & Trust Establishment

All participating nodes in a blockchain network shall be authenticated using unique cryptographic identities, with trust established through pre-defined onboarding policies or consensus governance.

4.2 BCS-02: Smart Contract Security Review

All smart contracts shall undergo manual and automated security reviews prior to deployment, including checks for logic flaws, gas limit abuse, reentrancy, and oracle manipulation.

4.3 BCS-03: Blockchain Consensus Integrity Monitoring

Organizations shall monitor the consensus process for anomalies such as double-signing, stale block propagation, or unusual fork behavior that may indicate manipulation or failure.

4.4 BCS-04: Immutable Ledger Access Control

Read and write access to blockchain interfaces shall be controlled via cryptographically enforced permissions, and unauthorized access attempts shall be logged and alertable.

4.5 BCS-05: On-Chain Data Classification & Minimization

Only non-sensitive, non-personal data shall be written to public or consortium blockchains unless regulatory exemptions and encryption protections are explicitly in place.

4.6 BCS-06: Private Key Custody & Protection

All private keys used for signing transactions, managing smart contracts, or operating nodes shall be secured using hardware security modules (HSMs) or equivalent vaulting technologies.

4.7 BCS-07: Blockchain Network Partition Detection

Mechanisms shall be in place to detect and alert on partitioned blockchain networks (e.g., network splits or eclipse attacks) that may cause inconsistent ledgers or transaction fraud.

4.8 BCS-08: Gas & Resource Abuse Limiting

Smart contract platforms shall enforce transaction limits, gas ceilings, and execution timeouts to prevent denial-of-service conditions or unintended resource exhaustion.

4.9 BCS-09: Smart Contract Versioning & Governance

Version control and formal governance processes shall be implemented to manage updates, upgrades, and deprecations of deployed smart contracts in a controlled manner.

4.10 BCS-10: Off-Chain Computation Integrity Controls

Where blockchain logic relies on off-chain computation or oracles, controls shall ensure authenticity, accuracy, and resistance to manipulation of those external data sources.

4.11 BCS-11: Transaction Anomaly Detection

Automated systems shall monitor blockchain transactions for anomalies such as batch minting, flash loan attacks, or signature forgeries indicative of compromise or abuse.

4.12 BCS-12: Blockchain Fork Response Strategy

Organizations shall maintain procedures for responding to unplanned hard forks, chain reorganizations, or network consensus failures, including impact assessments and rollback readiness.

4.13 BCS-13: Token & Asset Control Policy Enforcement

For blockchain systems that include tokenized assets, policies shall define ownership verification, transfer rules, revocation conditions, and recovery mechanisms for lost or stolen assets.

4.14 BCS-14: Smart Contract Kill Switch Capability

Smart contracts that perform financial, physical, or irreversible functions shall include administrative controls (e.g., pause, disable, or self-destruct) for emergency intervention.

4.15 BCS-15: Blockchain Interoperability Gateway Security

Interfaces between different blockchains (e.g., bridges, pegs, relays) shall be secured with authentication, access control, and transaction integrity checks to prevent cross-chain attacks.

4.16 BCS-16: Multi-Signature Requirements for Critical Functions

Blockchain-based operations with high impact—such as treasury withdrawals, contract upgrades, or validator rotation—shall require multi-signature approvals to reduce single points of failure.

4.17 BCS-17: Node Software Hardening & Update Controls

All blockchain node software shall be securely configured, kept up to date with validated patches, and monitored for tampering or version drift.

4.18 BCS-18: Regulatory Compliance of Blockchain Use Cases

Blockchain implementations shall be evaluated for compliance with applicable laws, including KYC/AML regulations, financial transaction reporting, and digital identity standards.

4.19 BCS-19: Encryption for Layer-2 and Off-Chain Storage

Any off-chain data referenced by blockchain transactions shall be encrypted at rest and in transit, with tamper detection and access control equivalent to on-chain protections.

4.20 BCS-20: Governance Model Transparency

Organizations shall document and make transparent the governance structures controlling blockchain network rules, upgrade procedures, node admission, and dispute resolution processes.

4.21 BCS-21: Smart Contract Deployment Environment Isolation

Smart contracts shall be developed and tested in isolated environments that mirror production conditions, with enforcement of promotion workflows through staging gates and peer validation.

4.22 BCS-22: Blockchain-Specific Incident Response Plan

Incident response plans shall include procedures specific to blockchain scenarios such as smart contract compromise, consensus attack, key leakage, or governance disputes.

Section 5. Smart Cities & Critical Infrastructure Protection (SCI)

The Smart Cities & Critical Infrastructure Protection (SCI) control family provides security controls tailored to the interconnected, data-driven ecosystems that define modern urban infrastructure. These environments blend civic services, industrial control systems (ICS), public-private data exchanges, and real-time digital infrastructure across domains such as transportation, utilities, and public safety. SCI controls address systemic resilience, cross-sector interdependencies, cyber-physical security integration, and governance mechanisms for critical systems operating at urban scale.

5.1 SCI-01: Urban System Dependency Mapping

Organizations shall document and maintain current maps of interdependencies across critical infrastructure systems (e.g., power, water, transportation, emergency services) to identify systemic risks and cascading failure paths.

5.2 SCI-02: Cross-Domain Data Exchange Governance

All data exchanges between city departments, private vendors, and infrastructure systems shall follow documented governance models ensuring integrity, consent, accountability, and lawful use of shared data.

5.3 SCI-03: Real-Time Sensor Data Integrity Verification

Controls shall validate the authenticity and consistency of sensor data used in real-time decision-making systems (e.g., traffic control, utilities monitoring), with alerts on out-of-band data or spoofing attempts.

5.4 SCI-04: Autonomous System Risk Mitigation

Critical infrastructure utilizing autonomous control systems (e.g., driverless transit, smart grids) shall implement safeguards to detect and contain unsafe or unexpected autonomous behavior.

5.5 SCI-05: Smart Infrastructure Cyber-Physical Resilience Testing

Routine resilience testing shall be conducted to evaluate cyber-physical systems' ability to maintain safety and operability under cyberattack scenarios, including loss of connectivity or data corruption.

5.6 SCI-06: Integrated Security for Public Service Platforms

Smart city platforms delivering services (e.g., e-voting, public Wi-Fi, license renewals) shall be secured using multi-layered access control, input validation, and end-to-end encryption.

5.7 SCI-07: Emergency System Redundancy Planning

Redundant communication and control systems shall be deployed for emergency infrastructure (e.g., 911, fire response, EMS dispatch) to ensure survivability under disruption or cyberattack.

5.8 SCI-08: Industrial IoT Device Security Zoning

Critical industrial IoT (IIoT) components within smart city systems (e.g., power meters, valves, grid control units) shall be deployed in logically zoned network segments with controlled cross-zone access.

5.9 SCI-09: Vendor Ecosystem Criticality Assessments

Third-party providers of smart city platforms or infrastructure services shall be assessed for their criticality, and higher-tier providers shall be subject to stricter cybersecurity and operational continuity requirements.

5.10 SCI-10: Operational Technology Incident Escalation Protocols

City infrastructure systems using OT components shall define escalation paths and command handoff procedures in the event of detected cyber events or operational anomalies.

5.11 SCI-11: Secure Firmware Lifecycle for Field-Deployed Assets

All field-deployed smart infrastructure (e.g., traffic lights, street sensors, SCADA endpoints) shall follow a secure firmware lifecycle including authenticated updates, rollback support, and update auditability.

5.12 SCI-12: Environmental Resilience Controls

Smart city systems shall implement environmental safeguards (e.g., temperature, humidity, vibration sensors) to detect and respond to conditions that could degrade the integrity or availability of critical hardware.

5.13 SCI-13: Geospatial System Access Restrictions

Geospatial and GIS systems shall be protected from unauthorized access and manipulation, particularly when used to inform emergency response, zoning, or transportation routing.

5.14 SCI-14: Physical-Cyber Coordination Plans

Incident response plans shall integrate physical and cyber considerations for city assets such as smart traffic controls, utility substations, or public surveillance systems.

5.15 SCI-15: Public-Facing Interface Security Controls

All public-facing smart city interfaces (e.g., kiosks, mobile apps, digital signage) shall be hardened against tampering, malware injection, and exploitation of embedded operating systems.

5.16 SCI-16: Time Synchronization Across Critical Infrastructure

All components of critical smart infrastructure shall use authenticated, tamper-resistant time sources to ensure synchronization for event correlation, audit trails, and safety operations.

5.17 SCI-17: Citizen Data Usage Transparency Controls

Data collected from citizens through smart infrastructure (e.g., smart meters, city apps, public transport systems) shall include explicit use notices, opt-out mechanisms, and retention policies.

5.18 SCI-18: Autonomous Public Safety System Supervision

Systems such as AI-assisted surveillance, gunshot detection, or predictive policing analytics shall include manual override capabilities and human-in-the-loop supervision.

5.19 SCI-19: Legacy Infrastructure Integration Safeguards

Controls shall be implemented to isolate and protect legacy systems (e.g., water treatment ICS, legacy rail controls) when integrated into modern smart city environments.

5.20 SCI-20: Threat Intelligence Sharing with Civic Partners

Smart city governance bodies shall participate in local, regional, and national threat intelligence sharing programs to enhance preparedness and resilience across the broader urban ecosystem.

5.21 SCI-21: Inter-Agency Cyber Crisis Simulation Exercises

Cities shall conduct regular cyber crisis simulations involving all relevant agencies, departments, and infrastructure operators to validate coordinated response capabilities and recovery procedures.

5.22 SCI-22: Critical Infrastructure Resource Prioritization Matrix

A prioritization matrix shall be maintained to identify which assets or services receive resource preference during emergency conditions or cyber-induced operational degradation.