FedRAMP 20x Security Scan Results Summary

Generated on: August 18, 2025 at 02:01 PM  
Scan ID: 1755482304878  
Timestamp: 2025-08-17T00:00:00.000Z

Executive Summary

This report summarizes the results of automated security scans performed across 51 Key Security Indicators (KSIs)   
for the FedRAMP 20x pilot program. A total of 284 security checks were executed, with an overall   
pass rate of 43.3%.  
  
Key findings:  
• 0 KSIs passed all security checks  
• 49 KSIs had partial compliance (some checks passed, some failed)  
• 0 KSIs failed all security checks  
• 1 warnings were identified requiring attention

Summary Statistics

|  |  |
| --- | --- |
| **Metric** | **Value** |
| Total KSIs Evaluated | 51 |
| Total Security Checks | 284 |
| Checks Passed | 123 |
| Checks Failed | 160 |
| Warnings | 1 |
| Overall Pass Rate | 43.3% |
| KSIs - All Checks Passed | 0 |
| KSIs - Partial Pass | 49 |
| KSIs - All Checks Failed | 0 |

Results by Category

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **KSIs** | **Total Checks** | **Passed** | **Failed** |
| CED - Configuration & Environment Documentation | 2 | 12 | 4 | 8 |
| CMT - Change Management & Testing | 5 | 32 | 15 | 17 |
| CNA - Cloud Native Architecture | 7 | 27 | 17 | 9 |
| IAM - Identity & Access Management | 6 | 41 | 15 | 26 |
| INR - Infrastructure & Reliability | 3 | 17 | 8 | 9 |
| MLA - Monitoring, Logging & Auditing | 6 | 39 | 16 | 23 |
| PIY - Privacy & Information Handling | 7 | 32 | 13 | 19 |
| RPL - Risk & Policy Management | 4 | 22 | 9 | 13 |
| SVC - Service Operations | 7 | 38 | 16 | 22 |
| TPR - Third Party & Resource Management | 4 | 24 | 10 | 14 |

Detailed Results by Category

CED - Configuration & Environment Documentation

KSI-CED-01

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Securityawarenesstraining Checks:**

* **✅ PASS** | HIGH | Employee Training Enrollment Coverage
* Description: All employees should be enrolled in mandatory security awareness training programs
* **✅ PASS** | MEDIUM | Training Completion Tracking and Analytics
* Description: Security awareness training completion should be systematically tracked with analytics and reporting
* **❌ FAIL** | MEDIUM | Incomplete Training Content Coverage
* Description: Security awareness training lacks comprehensive coverage of critical cybersecurity topics
* **❌ FAIL** | MEDIUM | Inadequate Training Frequency and Reinforcement
* Description: Security awareness training lacks sufficient frequency and ongoing reinforcement mechanisms
* **❌ FAIL** | LOW | Limited Training Customization and Personalization
* Description: Security awareness training lacks customization for different roles, departments, and risk profiles
* **❌ FAIL** | MEDIUM | Insufficient Training Effectiveness Measurement
* Description: Security awareness training lacks comprehensive effectiveness measurement and outcome validation

KSI-CED-02

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Rolespecifictraining Checks:**

* **✅ PASS** | HIGH | Privileged User Training Coverage
* Description: Users with privileged access should receive specialized security training appropriate to their access levels
* **✅ PASS** | MEDIUM | High-Risk Role Training Matrix
* Description: High-risk roles should be systematically identified with appropriate specialized training requirements
* **❌ FAIL** | HIGH | Incomplete Developer Security Training
* Description: Development team lacks comprehensive secure coding and DevSecOps training coverage
* **❌ FAIL** | HIGH | Missing Incident Response Team Training
* Description: Incident response team lacks comprehensive specialized training for security incident handling
* **❌ FAIL** | MEDIUM | Inadequate Third-Party Vendor Training Requirements
* Description: Third-party vendors and contractors lack standardized security training requirements and verification
* **❌ FAIL** | LOW | Insufficient Training for Emerging Technologies
* Description: High-risk roles lack specialized training for emerging technologies and evolving threat landscapes

CMT - Change Management & Testing

KSI-CMT-01

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 3 | Failed: 3

**Systemmodificationmonitoring Checks:**

* **✅ PASS** | HIGH | Azure Activity Log Comprehensive Configuration
* Description: Azure Activity Log should capture all system modifications and configuration changes across the subscription
* **✅ PASS** | MEDIUM | Infrastructure as Code Change Tracking
* Description: Infrastructure changes should be tracked through version control and deployment automation
* **✅ PASS** | HIGH | Application and Database Change Auditing
* Description: Application deployments and database schema changes should be comprehensively logged and monitored
* **❌ FAIL** | HIGH | Incomplete Container and Kubernetes Change Tracking
* Description: Container deployments and Kubernetes configuration changes lack comprehensive monitoring and audit trails
* **❌ FAIL** | MEDIUM | Inadequate Network Configuration Change Monitoring
* Description: Network configuration changes lack comprehensive monitoring and real-time alerting capabilities
* **❌ FAIL** | LOW | Missing Third-Party System Change Integration
* Description: Third-party systems and external service changes are not integrated with central change monitoring

KSI-CMT-02

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 4 | Failed: 3

**Immutableinfrastructure Checks:**

* **✅ PASS** | HIGH | Infrastructure as Code Immutable Deployment
* Description: Infrastructure deployments should use immutable patterns with version-controlled templates
* **✅ PASS** | HIGH | Container Image Immutability
* Description: Container deployments should use immutable images with proper versioning and security scanning
* **✅ PASS** | MEDIUM | Application Deployment Immutability
* Description: Application deployments should follow immutable patterns with blue-green or canary deployment strategies
* **✅ PASS** | HIGH | Database Schema Immutability
* Description: Database schema changes should be executed through version-controlled migration scripts with rollback capabilities
* **❌ FAIL** | HIGH | Incomplete Server Configuration Immutability
* Description: Server configurations are modified directly rather than through immutable infrastructure patterns
* **❌ FAIL** | MEDIUM | Inadequate Application Configuration Immutability
* Description: Application configurations are modified in-place rather than through externalized configuration management
* **❌ FAIL** | LOW | Limited Infrastructure Rollback Capabilities
* Description: Infrastructure rollback procedures lack automation and comprehensive testing validation

KSI-CMT-03

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 3 | Failed: 3

**Automatedtestingvalidation Checks:**

* **✅ PASS** | HIGH | Comprehensive CI/CD Pipeline Testing
* Description: CI/CD pipelines should implement comprehensive automated testing including unit, integration, and security tests
* **✅ PASS** | HIGH | Infrastructure as Code Validation
* Description: Infrastructure as Code templates should undergo comprehensive validation and testing before deployment
* **✅ PASS** | MEDIUM | Database Change Testing and Validation
* Description: Database schema changes should undergo comprehensive testing including data integrity and performance validation
* **❌ FAIL** | HIGH | Insufficient Performance Testing Coverage
* Description: Performance testing lacks comprehensive coverage across all application tiers and realistic load scenarios
* **❌ FAIL** | HIGH | Inadequate Security Testing Integration
* Description: Security testing lacks comprehensive integration with development workflows and automated vulnerability detection
* **❌ FAIL** | MEDIUM | Limited Test Environment Management
* Description: Test environment management lacks automation and consistent configuration across development lifecycle

KSI-CMT-04

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Changemanagementprocedure Checks:**

* **✅ PASS** | HIGH | Comprehensive Change Management Policy Framework
* Description: Organization should have a comprehensive change management policy framework with clear procedures and governance
* **✅ PASS** | HIGH | ServiceNow Change Management Implementation
* Description: Change management procedures should be implemented through enterprise change management platforms with workflow automation
* **❌ FAIL** | HIGH | Incomplete Change Risk Assessment Procedures
* Description: Change risk assessment procedures lack comprehensive risk analysis and impact evaluation frameworks
* **❌ FAIL** | HIGH | Inadequate Emergency Change Procedures
* Description: Emergency change procedures lack comprehensive documentation and post-implementation review processes
* **❌ FAIL** | MEDIUM | Limited Change Management Training and Awareness
* Description: Change management training and awareness programs lack comprehensive coverage and effectiveness measurement
* **❌ FAIL** | LOW | Insufficient Change Management Metrics and Reporting
* Description: Change management metrics and reporting lack comprehensive KPIs and stakeholder-specific dashboards

KSI-CMT-05

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 3 | Failed: 4

**Changeriskimpactevaluation Checks:**

* **✅ PASS** | HIGH | Comprehensive Change Risk Assessment Framework
* Description: Organization should have a comprehensive change risk assessment framework for evaluating potential risks and impacts of proposed changes
* **✅ PASS** | HIGH | Integrated Change Impact Analysis Tools
* Description: Change impact analysis should be supported by integrated tools for dependency mapping, impact simulation, and automated risk evaluation
* **✅ PASS** | HIGH | Structured Change Review and Approval Process
* Description: Changes should undergo structured review and approval processes based on risk assessment outcomes and impact evaluation results
* **❌ FAIL** | HIGH | Incomplete Post-Implementation Risk Validation
* Description: Post-implementation risk validation processes lack systematic validation of pre-change risk assessments and impact predictions
* **❌ FAIL** | HIGH | Limited Business Impact Quantification Methods
* Description: Business impact quantification methods lack comprehensive financial modeling and stakeholder impact assessment capabilities
* **❌ FAIL** | MEDIUM | Insufficient Change Risk Communication Framework
* Description: Change risk communication framework lacks comprehensive stakeholder engagement and risk transparency mechanisms
* **❌ FAIL** | LOW | Basic Change Success Metrics and Evaluation
* Description: Change success metrics and evaluation processes lack comprehensive outcome measurement and continuous improvement integration

CNA - Cloud Native Architecture

KSI-CNA-01

**Status:** ⚠️ PARTIAL | Total Checks: 8 | Passed: 4 | Failed: 3 | Warnings: 1

**Containersecurity Checks:**

* **✅ PASS** | HIGH | Container Image Vulnerability Scan
* Description: Container images must be scanned for vulnerabilities
* **❌ FAIL** | HIGH | Container Base Image Security
* Description: Container base images must use approved secure base images
* **✅ PASS** | MEDIUM | Container Runtime Security
* Description: Containers must not run as root user
* **❌ FAIL** | HIGH | Container Network Security
* Description: Container network policies must restrict traffic
* **✅ PASS** | MEDIUM | Container Resource Limits
* Description: Containers must have CPU and memory limits defined
* **❌ FAIL** | HIGH | Container Image Signing
* Description: Container images must be digitally signed
* **✅ PASS** | HIGH | Container Secrets Management
* Description: Container secrets must be stored securely
* **⚠️ WARNING** | MEDIUM | Container Logging and Monitoring
* Description: Container logs must be centrally collected and monitored

KSI-CNA-02

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 5 | Failed: 1

**Permission Checks:**

* **✅ PASS** | HIGH | Service Principal Role Assignment Review
* Description: Service principals should have minimal required permissions
* **✅ PASS** | MEDIUM | Managed Identity Permission Analysis
* Description: Managed identities should not have overly broad permissions
* **✅ PASS** | HIGH | Container Registry Access Control
* Description: Container registry access should be restricted to authorized users only
* **✅ PASS** | HIGH | Key Vault Access Policy Review
* Description: Key Vault access should follow principle of least privilege
* **✅ PASS** | MEDIUM | Storage Account Permission Analysis
* Description: Storage account access should be minimal and scoped appropriately
* **❌ FAIL** | HIGH | Application Service Principal Excessive Permissions
* Description: Service principal has overly broad permissions that violate least privilege

KSI-CNA-03

**Status:** ⚠️ PARTIAL | Total Checks: 2 | Passed: 1 | Failed: 1

**Trafficflowcontrols Checks:**

* **✅ PASS** | HIGH | Application Gateway Traffic Flow Validation
* Description: Validate that traffic flows through proper security controls and WAF
* **❌ FAIL** | HIGH | Container Network Policy Enforcement
* Description: Validate that container-to-container traffic is properly controlled

KSI-CNA-04

**Status:** ⚠️ PARTIAL | Total Checks: 3 | Passed: 2 | Failed: 1

**Immutability Checks:**

* **✅ PASS** | HIGH | Container Image Immutability Validation
* Description: Container images should be immutable and not allow runtime modifications
* **✅ PASS** | MEDIUM | Infrastructure as Code Immutability
* Description: Infrastructure should be deployed through immutable IaC templates
* **❌ FAIL** | HIGH | Storage Account Configuration Mutability
* Description: Storage accounts should have immutable blob storage enabled for compliance data

KSI-CNA-05

**Status:** ⚠️ PARTIAL | Total Checks: 2 | Passed: 1 | Failed: 1

**Dosprotection Checks:**

* **✅ PASS** | HIGH | Application Gateway DDoS Protection Validation
* Description: Application Gateway should be properly configured with DDoS protection and rate limiting
* **❌ FAIL** | HIGH | Container Instance Resource Limits and DoS Protection
* Description: Container instances should have proper resource limits and DoS protection configured

KSI-CNA-06

**Status:** ⚠️ PARTIAL | Total Checks: 2 | Passed: 1 | Failed: 1

**Highavailability Checks:**

* **✅ PASS** | HIGH | App Service High Availability Configuration
* Description: App Service should be configured for high availability with proper scaling and disaster recovery
* **❌ FAIL** | HIGH | Storage Account Redundancy and Recovery Configuration
* Description: Storage accounts should be configured with appropriate redundancy and disaster recovery options

KSI-CNA-07

**Status:** ⚠️ PARTIAL | Total Checks: 4 | Passed: 3 | Failed: 1

**Cloudnativeresource Checks:**

* **✅ PASS** | HIGH | Azure Cosmos DB Best Practices Implementation
* Description: Cosmos DB should follow cloud-native best practices for security, performance, and cost optimization
* **✅ PASS** | MEDIUM | Azure Service Bus Enterprise Messaging Best Practices
* Description: Service Bus should implement cloud-native messaging patterns with proper security and reliability
* **✅ PASS** | HIGH | Azure Key Vault Secrets Management Best Practices
* Description: Key Vault should follow cloud-native security best practices for secrets, keys, and certificates
* **❌ FAIL** | HIGH | Azure SQL Database Configuration Issues
* Description: SQL Database should follow cloud-native best practices for security, performance, and cost optimization

IAM - Identity & Access Management

KSI-IAM-01

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 3 | Failed: 4

**Mfaenforcement Checks:**

* **✅ PASS** | CRITICAL | Azure AD Conditional Access MFA Policies
* Description: All users should have MFA enforced through Conditional Access policies
* **✅ PASS** | CRITICAL | Privileged Identity Management MFA Requirements
* Description: PIM role activations should require MFA verification
* **✅ PASS** | HIGH | Azure Resource Manager MFA Protection
* Description: Azure management operations should require MFA verification
* **❌ FAIL** | CRITICAL | Legacy Authentication Protocol Gaps
* Description: Legacy authentication protocols bypass MFA requirements
* **❌ FAIL** | HIGH | Service Account MFA Exemption Issues
* Description: Service accounts lack proper MFA alternatives and monitoring
* **❌ FAIL** | HIGH | Guest User MFA Enforcement Gaps
* Description: Guest users have inconsistent MFA enforcement and monitoring
* **❌ FAIL** | MEDIUM | Mobile Device MFA Bypass Vulnerabilities
* Description: Mobile applications and devices show MFA bypass possibilities

KSI-IAM-02

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Passwordlessandpasswordpolicy Checks:**

* **✅ PASS** | HIGH | Windows Hello for Business Implementation
* Description: Windows devices should use Windows Hello for Business for passwordless authentication
* **✅ PASS** | MEDIUM | FIDO2 Security Key Implementation
* Description: High-privilege users should have FIDO2 security keys for passwordless authentication
* **❌ FAIL** | HIGH | Weak Password Policy Configuration
* Description: Password policies do not meet security requirements and lack modern protections
* **❌ FAIL** | MEDIUM | Incomplete Passwordless Migration
* Description: Organizations has not fully migrated to passwordless authentication where feasible
* **❌ FAIL** | HIGH | Service Account Password Management Issues
* Description: Service accounts use weak passwords and lack proper rotation policies
* **❌ FAIL** | MEDIUM | Mobile Application Authentication Weaknesses
* Description: Mobile applications use weak authentication methods and lack passwordless options

KSI-IAM-03

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Nonuseraccountsecurity Checks:**

* **✅ PASS** | HIGH | Managed Identity Implementation
* Description: Azure resources should use managed identities instead of service accounts where possible
* **✅ PASS** | HIGH | Service Principal Security Configuration
* Description: Service principals should have proper security controls and monitoring
* **❌ FAIL** | CRITICAL | Legacy Service Account Security Gaps
* Description: Legacy service accounts lack proper security controls and management
* **❌ FAIL** | HIGH | Shared Account Usage Violations
* Description: Shared accounts are used inappropriately without proper controls
* **❌ FAIL** | HIGH | Application Account Security Weaknesses
* Description: Application accounts lack proper security configuration and lifecycle management
* **❌ FAIL** | MEDIUM | Emergency Access Account Management Issues
* Description: Emergency break-glass accounts lack proper controls and monitoring

KSI-IAM-04

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 3 | Failed: 4

**Leastprivilegerbacjit Checks:**

* **✅ PASS** | HIGH | Azure RBAC Least Privilege Implementation
* Description: Azure RBAC roles should follow least privilege principle with appropriate scope assignments
* **✅ PASS** | CRITICAL | Privileged Identity Management (PIM) Configuration
* Description: Azure PIM should be configured for all privileged roles with appropriate access policies
* **✅ PASS** | HIGH | Azure Resource JIT VM Access
* Description: Virtual machines should have just-in-time access configured to minimize attack surface
* **❌ FAIL** | HIGH | Over-Privileged Role Assignments
* Description: Multiple users have excessive privileges beyond their job requirements
* **❌ FAIL** | HIGH | Missing JIT Access Controls
* Description: Critical systems lack just-in-time access controls exposing permanent administrative access
* **❌ FAIL** | MEDIUM | Inadequate Access Review Processes
* Description: Access review processes lack automation and regular execution for privilege verification
* **❌ FAIL** | CRITICAL | Privilege Escalation Vulnerabilities
* Description: System configurations allow unauthorized privilege escalation through various attack vectors

KSI-IAM-05

**Status:** ⚠️ PARTIAL | Total Checks: 8 | Passed: 3 | Failed: 5

**Zerotrustdesignprinciples Checks:**

* **✅ PASS** | CRITICAL | Identity as Security Perimeter Implementation
* Description: Identity-based security controls should replace traditional network perimeter security
* **✅ PASS** | HIGH | Never Trust Always Verify Implementation
* Description: All access requests should be verified regardless of location or previous trust
* **✅ PASS** | HIGH | Micro-Segmentation and Least Privilege Network Access
* Description: Network access should be micro-segmented with least privilege principles applied
* **❌ FAIL** | HIGH | Legacy Trust Model Dependencies
* Description: Systems still rely on legacy network trust models rather than zero trust principles
* **❌ FAIL** | HIGH | Inadequate Context-Aware Access Controls
* Description: Access controls lack contextual awareness for risk-based decision making
* **❌ FAIL** | HIGH | Insufficient Data-Centric Security
* Description: Data protection lacks zero trust principles with inadequate classification and access controls
* **❌ FAIL** | MEDIUM | Limited Continuous Verification and Monitoring
* Description: Continuous verification and monitoring capabilities are insufficient for zero trust implementation
* **❌ FAIL** | MEDIUM | Application Integration Zero Trust Gaps
* Description: Applications lack proper zero trust integration with insufficient security controls

KSI-IAM-06

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 2 | Failed: 5

**Suspiciousbehavioraccountdisabling Checks:**

* **✅ PASS** | CRITICAL | Automated Risk-Based Account Protection
* Description: Azure Identity Protection should automatically respond to high-risk user activities
* **✅ PASS** | HIGH | Behavioral Analytics and Anomaly Detection
* Description: User and entity behavior analytics should detect suspicious patterns and trigger automated responses
* **❌ FAIL** | HIGH | Incomplete Suspicious Activity Detection
* Description: Suspicious activity detection coverage has significant gaps and limited automation
* **❌ FAIL** | HIGH | Manual Account Disabling Processes
* Description: Account disabling relies heavily on manual processes leading to delays and inconsistencies
* **❌ FAIL** | MEDIUM | Insufficient Threat Intelligence Integration
* Description: Threat intelligence integration lacks comprehensiveness and real-time application to account security
* **❌ FAIL** | MEDIUM | Limited Forensic and Investigation Capabilities
* Description: Forensic capabilities are insufficient for thorough investigation of suspicious account activities
* **❌ FAIL** | MEDIUM | Inadequate Incident Response Integration
* Description: Account disabling is not properly integrated with broader incident response procedures

INR - Infrastructure & Reliability

KSI-INR-01

**Status:** ⚠️ PARTIAL | Total Checks: 5 | Passed: 3 | Failed: 2

**Incidentreporting Checks:**

* **✅ PASS** | CRITICAL | FedRAMP Incident Reporting Compliance
* Description: Incidents should be reported according to FedRAMP requirements within mandated timeframes
* **✅ PASS** | HIGH | Cloud Service Provider Policy Compliance
* Description: Incident reporting should comply with internal cloud service provider policies and procedures
* **✅ PASS** | HIGH | Automated Incident Detection and Reporting Integration
* Description: Incident detection systems should be integrated with automated reporting capabilities for rapid response
* **❌ FAIL** | MEDIUM | Incomplete Customer and Stakeholder Notification
* Description: Customer and stakeholder notification processes lack automation and consistent execution for incident communication
* **❌ FAIL** | MEDIUM | Insufficient Incident Reporting Analytics and Metrics
* Description: Incident reporting lacks comprehensive analytics and metrics for performance measurement and continuous improvement

KSI-INR-02

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 3 | Failed: 3

**Incidentlogmaintenance Checks:**

* **✅ PASS** | HIGH | Comprehensive Incident Log Management
* Description: Incident logs should be maintained with comprehensive data retention and integrity protection
* **✅ PASS** | HIGH | Automated Pattern Analysis and Trend Identification
* Description: Incident logs should be analyzed for patterns, trends, and vulnerabilities using automated capabilities
* **✅ PASS** | MEDIUM | Incident Review Schedule and Process Automation
* Description: Incident logs should be reviewed periodically according to a defined schedule with automated process management
* **❌ FAIL** | MEDIUM | Limited Historical Data Analysis and Correlation
* Description: Historical incident data analysis lacks depth and correlation capabilities for comprehensive pattern identification
* **❌ FAIL** | HIGH | Insufficient Vulnerability Pattern Integration
* Description: Incident logs lack comprehensive integration with vulnerability management for pattern identification and remediation tracking
* **❌ FAIL** | MEDIUM | Missing Incident Lifecycle Analytics
* Description: Incident logs lack comprehensive lifecycle analytics for response effectiveness measurement and process optimization

KSI-INR-03

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Afteractionreports Checks:**

* **✅ PASS** | HIGH | After Action Report Generation and Documentation
* Description: After action reports should be generated for significant incidents with comprehensive documentation and analysis
* **✅ PASS** | HIGH | Lessons Learned Capture and Documentation
* Description: Lessons learned should be systematically captured, documented, and made accessible for organizational learning
* **❌ FAIL** | HIGH | Limited Operational Process Integration
* Description: Lessons learned lack comprehensive integration into operational processes for effective implementation and improvement
* **❌ FAIL** | MEDIUM | Insufficient Training and Knowledge Transfer
* Description: Lessons learned lack effective integration into training programs and knowledge transfer processes
* **❌ FAIL** | MEDIUM | Missing Automation and Technology Integration
* Description: Lessons learned processes lack automation and technology integration for efficient implementation and tracking
* **❌ FAIL** | LOW | Limited External Learning and Benchmarking
* Description: Lessons learned processes lack integration with external learning sources and industry benchmarking for comprehensive improvement

MLA - Monitoring, Logging & Auditing

KSI-MLA-01

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 3 | Failed: 4

**Siemsystemoperation Checks:**

* **✅ PASS** | CRITICAL | Azure Sentinel SIEM Deployment and Configuration
* Description: Azure Sentinel should be deployed as the primary SIEM with comprehensive data connector integration
* **✅ PASS** | HIGH | Centralized Log Management and Correlation
* Description: All critical systems should send logs to centralized SIEM with proper correlation capabilities
* **✅ PASS** | HIGH | Security Operations Center (SOC) Integration
* Description: SIEM should be integrated with SOC processes and staffed for 24x7 monitoring
* **❌ FAIL** | HIGH | Incomplete Log Source Coverage
* Description: Critical systems and applications lack comprehensive logging integration with SIEM
* **❌ FAIL** | MEDIUM | Inadequate Event Correlation and Analytics
* Description: Event correlation capabilities lack sophistication and miss complex attack patterns
* **❌ FAIL** | MEDIUM | Insufficient Backup and Disaster Recovery for SIEM
* Description: SIEM infrastructure lacks comprehensive backup and disaster recovery capabilities
* **❌ FAIL** | LOW | Limited Integration with External Security Tools
* Description: SIEM lacks comprehensive integration with external security tools and threat intelligence sources

KSI-MLA-02

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Logreviewaudit Checks:**

* **✅ PASS** | HIGH | Automated Log Analysis and Review Workflows
* Description: Automated systems should continuously analyze logs for security events and compliance violations
* **✅ PASS** | MEDIUM | Scheduled Audit Review Processes
* Description: Regular scheduled audit reviews should be conducted by qualified personnel with documented findings
* **❌ FAIL** | HIGH | Inadequate Manual Review Coverage
* Description: Manual review processes fail to cover critical log sources and security events adequately
* **❌ FAIL** | MEDIUM | Delayed Review Response Times
* Description: Log review processes experience significant delays in identifying and responding to security events
* **❌ FAIL** | MEDIUM | Insufficient Audit Trail Documentation
* Description: Audit review activities lack comprehensive documentation and evidence retention
* **❌ FAIL** | LOW | Limited Trend Analysis and Reporting
* Description: Log review processes lack comprehensive trend analysis and strategic reporting capabilities

KSI-MLA-03

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 3 | Failed: 4

**Vulnerabilitydetectionremediation Checks:**

* **✅ PASS** | HIGH | Automated Vulnerability Scanning Coverage
* Description: Comprehensive automated vulnerability scanning should cover all system components and infrastructure
* **✅ PASS** | MEDIUM | Vulnerability Intelligence and Threat Feeds
* Description: Current threat intelligence should be integrated with vulnerability management processes
* **✅ PASS** | CRITICAL | Rapid Patch Management and Deployment
* Description: Critical security patches should be deployed rapidly with proper testing and rollback capabilities
* **❌ FAIL** | HIGH | Delayed Vulnerability Remediation
* Description: Critical and high-severity vulnerabilities are not being remediated within acceptable timeframes
* **❌ FAIL** | MEDIUM | Inadequate Vulnerability Scanning Coverage
* Description: Vulnerability scanning does not adequately cover all system components and attack vectors
* **❌ FAIL** | MEDIUM | Missing Threat Intelligence Integration
* Description: Vulnerability management lacks integration with current threat intelligence and attack trends
* **❌ FAIL** | LOW | Limited Remediation Automation
* Description: Vulnerability remediation processes lack automation leading to slower response times and inconsistent execution

KSI-MLA-04

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Authenticatedscanning Checks:**

* **✅ PASS** | HIGH | Authenticated Windows System Scanning
* Description: Windows systems should have comprehensive authenticated vulnerability scanning with appropriate credentials
* **✅ PASS** | CRITICAL | Database Security Assessment
* Description: Database systems should undergo authenticated security assessments with appropriate database-specific scanning
* **❌ FAIL** | HIGH | Insufficient Linux System Authenticated Scanning
* Description: Linux systems lack comprehensive authenticated vulnerability scanning coverage
* **❌ FAIL** | MEDIUM | Missing Network Device Authentication
* Description: Network infrastructure devices lack authenticated vulnerability scanning and security assessment
* **❌ FAIL** | HIGH | Inadequate Container and Kubernetes Scanning
* Description: Container images and Kubernetes environments lack comprehensive authenticated vulnerability scanning
* **❌ FAIL** | MEDIUM | Limited Cloud Service Configuration Scanning
* Description: Cloud service configurations lack comprehensive security assessment and vulnerability scanning

KSI-MLA-05

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 3 | Failed: 3

**Iacconfigurationtesting Checks:**

* **✅ PASS** | HIGH | Infrastructure as Code Security Scanning
* Description: Infrastructure as Code templates should undergo comprehensive security scanning and validation
* **✅ PASS** | MEDIUM | Configuration Drift Detection and Management
* Description: System configurations should be continuously monitored for drift from approved baselines
* **✅ PASS** | HIGH | Automated Configuration Testing in CI/CD
* Description: Configuration changes should be automatically tested and validated within CI/CD pipelines
* **❌ FAIL** | HIGH | Incomplete Infrastructure Testing Coverage
* Description: Infrastructure testing lacks comprehensive coverage across all deployment scenarios and environments
* **❌ FAIL** | MEDIUM | Missing Policy as Code Implementation
* Description: Security and compliance policies lack systematic implementation as code with automated enforcement
* **❌ FAIL** | LOW | Limited Configuration Baseline Management
* Description: System configuration baselines lack comprehensive management and enforcement capabilities

KSI-MLA-06

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 3 | Failed: 4

**Centralizedvulnerabilitytracking Checks:**

* **✅ PASS** | HIGH | Comprehensive Vulnerability Management Platform
* Description: Centralized vulnerability management platform should track and prioritize vulnerabilities across all assets
* **✅ PASS** | MEDIUM | Vulnerability Risk Assessment and Business Context
* Description: Vulnerability assessments should incorporate business context and organizational risk factors
* **✅ PASS** | HIGH | Automated Vulnerability Remediation Workflows
* Description: Vulnerability remediation should be supported by automated workflows and integration with change management
* **❌ FAIL** | HIGH | Incomplete Vulnerability Data Integration
* Description: Vulnerability management lacks comprehensive integration across all security tools and data sources
* **❌ FAIL** | MEDIUM | Inadequate Vulnerability Metrics and Reporting
* Description: Vulnerability management metrics and reporting lack comprehensive business alignment and actionable insights
* **❌ FAIL** | MEDIUM | Limited Vulnerability Intelligence and Threat Context
* Description: Vulnerability management lacks advanced threat intelligence integration and contextual threat analysis
* **❌ FAIL** | LOW | Insufficient Vulnerability Management Governance
* Description: Vulnerability management lacks comprehensive governance framework and strategic oversight

PIY - Privacy & Information Handling

KSI-PIY-01

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 3 | Failed: 3

**Informationresourceinventory Checks:**

* **✅ PASS** | HIGH | Infrastructure as Code Asset Definition
* Description: All infrastructure resources should be defined and managed through Infrastructure as Code with comprehensive asset tracking
* **✅ PASS** | HIGH | Software Asset Management and Tracking
* Description: All software assets including applications, libraries, and dependencies should be comprehensively tracked and managed
* **✅ PASS** | HIGH | Service and API Inventory Management
* Description: All services, APIs, and external integrations should be inventoried with comprehensive documentation and security assessment
* **❌ FAIL** | HIGH | Personnel and Access Inventory Gaps
* Description: Personnel inventory and access tracking systems lack comprehensive coverage and real-time synchronization
* **❌ FAIL** | HIGH | Data Asset Inventory Deficiencies
* Description: Data asset inventory lacks comprehensive data classification, lineage tracking, and privacy compliance management
* **❌ FAIL** | MEDIUM | Network and Security Asset Inventory Gaps
* Description: Network infrastructure and security asset inventory lacks real-time discovery and comprehensive vulnerability tracking

KSI-PIY-02

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 3 | Failed: 4

**Securitypolicy Checks:**

* **✅ PASS** | HIGH | Comprehensive Security Policy Framework
* Description: Organization should have a comprehensive security policy framework covering all aspects of information security
* **✅ PASS** | HIGH | Azure Policy and Governance Implementation
* Description: Azure policies should be implemented to enforce security objectives and compliance requirements across all cloud resources
* **✅ PASS** | MEDIUM | Security Awareness and Training Policy Implementation
* Description: Security awareness and training policies should be implemented to ensure all personnel understand their security responsibilities
* **❌ FAIL** | HIGH | Incomplete Policy Documentation and Standards
* Description: Security policy documentation lacks comprehensive technical standards and implementation guidance
* **❌ FAIL** | HIGH | Inadequate Third-Party and Vendor Security Policies
* Description: Third-party and vendor security policies lack comprehensive requirements and enforcement mechanisms
* **❌ FAIL** | MEDIUM | Limited Security Policy Enforcement and Monitoring
* Description: Security policy enforcement mechanisms lack automated monitoring and consistent violation response procedures
* **❌ FAIL** | MEDIUM | Insufficient Privacy and Data Protection Policy Implementation
* Description: Privacy and data protection policies lack comprehensive implementation and automated privacy controls

KSI-PIY-03

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Vulnerabilitydisclosureprogram Checks:**

* **✅ PASS** | HIGH | Formal Vulnerability Disclosure Policy
* Description: Organization should have a formal vulnerability disclosure policy that provides clear guidance for security researchers
* **✅ PASS** | MEDIUM | Bug Bounty Program Implementation
* Description: Organization should implement a bug bounty program to incentivize security research and vulnerability discovery
* **❌ FAIL** | HIGH | Inadequate Vulnerability Intake and Triage Process
* Description: Vulnerability intake and triage processes lack automated workflows and comprehensive classification systems
* **❌ FAIL** | HIGH | Limited Vulnerability Remediation and Disclosure Coordination
* Description: Vulnerability remediation processes lack systematic prioritization and coordinated disclosure management
* **❌ FAIL** | MEDIUM | Insufficient Security Research Community Engagement
* Description: Security research community engagement lacks comprehensive outreach and relationship building programs
* **❌ FAIL** | LOW | Limited Legal and Compliance Framework Integration
* Description: Vulnerability disclosure program lacks comprehensive legal and regulatory compliance integration

KSI-PIY-04

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 3 | Failed: 4

**Securedevlopmentlifecycle Checks:**

* **✅ PASS** | HIGH | Secure Development Lifecycle Policy Implementation
* Description: Organization should have comprehensive SDL policies and procedures aligned with CISA Secure by Design principles
* **✅ PASS** | HIGH | Secure Architecture and Design Implementation
* Description: Security should be integrated into architecture and design phases with comprehensive threat modeling
* **✅ PASS** | HIGH | Automated Security Testing Integration
* Description: Comprehensive automated security testing should be integrated throughout the development pipeline
* **❌ FAIL** | HIGH | Insufficient Secure Coding Standards Implementation
* Description: Secure coding standards lack comprehensive implementation and enforcement across development teams
* **❌ FAIL** | HIGH | Inadequate Security Requirements and Design Review Process
* Description: Security requirements gathering and design review processes lack systematic implementation and stakeholder engagement
* **❌ FAIL** | MEDIUM | Limited Security Testing and Quality Assurance Integration
* Description: Security testing integration lacks comprehensive coverage and quality assurance validation throughout testing phases
* **❌ FAIL** | LOW | Insufficient DevSecOps Culture and Capability Maturity
* Description: DevSecOps culture and organizational capability lack comprehensive maturity and systematic improvement programs

KSI-PIY-05

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Informationresourceevaluation Checks:**

* **✅ PASS** | HIGH | Technical Evaluation Framework Implementation
* Description: Organization should have comprehensive technical evaluation methods for all information resource implementations
* **✅ PASS** | HIGH | Performance and Security Benchmarking
* Description: Information resource implementations should be evaluated against established performance and security benchmarks
* **❌ FAIL** | HIGH | Insufficient Evaluation Documentation Standards
* Description: Information resource evaluation methods lack comprehensive documentation and standardization across teams
* **❌ FAIL** | MEDIUM | Limited Technical Validation Testing
* Description: Information resource evaluation lacks comprehensive technical validation testing and verification procedures
* **❌ FAIL** | MEDIUM | Inadequate Evaluation Process Governance
* Description: Information resource evaluation processes lack comprehensive governance, oversight, and continuous improvement mechanisms
* **❌ FAIL** | LOW | Limited Stakeholder Engagement and Communication
* Description: Information resource evaluation processes lack comprehensive stakeholder engagement and effective communication strategies

KSI-PIY-06

**Status:** ❌ FAIL | Total Checks: 0 | Passed: 0 | Failed: 0

KSI-PIY-07

**Status:** ❌ FAIL | Total Checks: 0 | Passed: 0 | Failed: 0

RPL - Risk & Policy Management

KSI-RPL-01

**Status:** ⚠️ PARTIAL | Total Checks: 5 | Passed: 2 | Failed: 3

**Recoveryobjectives Checks:**

* **✅ PASS** | HIGH | RTO/RPO Documentation and Tracking
* Description: Recovery Time Objectives and Recovery Point Objectives should be formally documented and systematically tracked
* **✅ PASS** | MEDIUM | Infrastructure Capability Assessment
* Description: Infrastructure capabilities should be assessed and validated against defined recovery objectives
* **❌ FAIL** | HIGH | Inadequate Business Impact Analysis
* Description: Business impact analysis lacks comprehensive assessment and stakeholder validation for recovery objectives
* **❌ FAIL** | MEDIUM | Missing Service Dependency Mapping
* Description: Service dependency mapping lacks comprehensive analysis for recovery objective determination
* **❌ FAIL** | MEDIUM | Insufficient Recovery Objective Validation
* Description: Recovery objectives lack regular validation and real-world testing to ensure achievability

KSI-RPL-02

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Recoveryplan Checks:**

* **✅ PASS** | HIGH | Recovery Plan Documentation and Version Control
* Description: Recovery plans should be comprehensively documented with proper version control and change management
* **✅ PASS** | MEDIUM | RTO/RPO Alignment Validation
* Description: Recovery plans should demonstrate clear alignment with defined RTO and RPO objectives
* **❌ FAIL** | HIGH | Incomplete Stakeholder Training and Awareness
* Description: Recovery plan stakeholders lack comprehensive training and awareness of their roles and responsibilities
* **❌ FAIL** | MEDIUM | Limited Recovery Automation and Orchestration
* Description: Recovery plans lack comprehensive automation and orchestration capabilities to meet recovery objectives
* **❌ FAIL** | MEDIUM | Inadequate Cross-Functional Coordination
* Description: Recovery plans lack comprehensive cross-functional coordination and communication procedures
* **❌ FAIL** | HIGH | Missing Plan Currency and Maintenance
* Description: Recovery plans lack systematic currency maintenance and regular updates to reflect changing business and technical environments

KSI-RPL-03

**Status:** ⚠️ PARTIAL | Total Checks: 5 | Passed: 3 | Failed: 2

**Systembackup Checks:**

* **✅ PASS** | HIGH | Backup Policy Alignment with Recovery Objectives
* Description: System backup policies should be aligned with defined RTO and RPO objectives for effective recovery
* **✅ PASS** | HIGH | Automated Backup Success Monitoring
* Description: Backup operations should be continuously monitored with automated success validation and failure alerting
* **✅ PASS** | HIGH | Backup Storage and Data Integrity Validation
* Description: Backup storage should ensure data integrity with comprehensive validation and verification procedures
* **❌ FAIL** | MEDIUM | Limited Backup Testing and Restore Validation
* Description: Backup systems lack comprehensive testing and restore validation to ensure recovery capability effectiveness
* **❌ FAIL** | MEDIUM | Insufficient Backup Recovery Documentation and Procedures
* Description: Backup recovery procedures lack comprehensive documentation and standardized processes for effective restoration

KSI-RPL-04

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Recoverytesting Checks:**

* **✅ PASS** | HIGH | Recovery Testing Schedule and Frequency
* Description: Recovery testing should be conducted regularly according to a defined schedule that aligns with business requirements
* **✅ PASS** | MEDIUM | Recovery Testing Environment Management
* Description: Recovery testing environments should accurately represent production with proper isolation and configuration management
* **❌ FAIL** | HIGH | Limited Recovery Testing Scope and Coverage
* Description: Recovery testing lacks comprehensive scope and coverage to validate all critical recovery scenarios and dependencies
* **❌ FAIL** | MEDIUM | Inadequate Recovery Testing Automation
* Description: Recovery testing processes lack comprehensive automation to ensure consistent, repeatable, and efficient testing execution
* **❌ FAIL** | MEDIUM | Missing Recovery Performance Validation
* Description: Recovery testing lacks comprehensive performance validation to ensure recovery objectives and user experience requirements are met
* **❌ FAIL** | MEDIUM | Limited Recovery Testing Documentation and Reporting
* Description: Recovery testing lacks comprehensive documentation and reporting to capture lessons learned and drive continuous improvement

SVC - Service Operations

KSI-SVC-01

**Status:** ⚠️ PARTIAL | Total Checks: 3 | Passed: 2 | Failed: 1

**Networkhardening Checks:**

* **✅ PASS** | HIGH | Virtual Network Security Configuration
* Description: Virtual Network should be properly segmented with hardened security controls
* **✅ PASS** | HIGH | Azure Firewall Advanced Security Configuration
* Description: Azure Firewall should be configured with advanced security features and threat intelligence
* **❌ FAIL** | CRITICAL | Network Security Group Misconfigurations
* Description: Network Security Groups should follow least privilege principle and deny unnecessary traffic

KSI-SVC-02

**Status:** ⚠️ PARTIAL | Total Checks: 4 | Passed: 2 | Failed: 2

**Encryptionverification Checks:**

* **✅ PASS** | HIGH | Application Gateway SSL/TLS Configuration
* Description: Application Gateway should enforce strong encryption for all traffic
* **✅ PASS** | HIGH | VPN Gateway IPSec Encryption
* Description: VPN Gateway should use strong IPSec encryption for site-to-site connections
* **❌ FAIL** | CRITICAL | Storage Account Insecure Transport
* Description: Storage Account should enforce HTTPS and disable insecure transport protocols
* **❌ FAIL** | HIGH | SQL Database Encryption Deficiencies
* Description: SQL Database should have comprehensive encryption for data at rest and in transit

KSI-SVC-03

**Status:** ⚠️ PARTIAL | Total Checks: 3 | Passed: 1 | Failed: 2

**Storageencryption Checks:**

* **✅ PASS** | HIGH | Azure Storage Account Comprehensive Encryption
* Description: Storage Account should have comprehensive encryption at rest with customer-managed keys
* **❌ FAIL** | CRITICAL | Virtual Machine Disk Encryption Failures
* Description: Virtual Machine disks should be encrypted using Azure Disk Encryption
* **❌ FAIL** | HIGH | SQL Database TDE Configuration Issues
* Description: SQL Database should have Transparent Data Encryption enabled with proper key management

KSI-SVC-04

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 3 | Failed: 4

**Centralconfigurationmanagement Checks:**

* **✅ PASS** | MEDIUM | Azure App Configuration Service Implementation
* Description: Application configuration should be centrally managed through Azure App Configuration
* **✅ PASS** | HIGH | Azure Key Vault Secrets Management
* Description: Sensitive configuration data should be stored in Azure Key Vault with proper access controls
* **✅ PASS** | MEDIUM | Azure Policy Governance Implementation
* Description: Configuration standards should be enforced through Azure Policy
* **❌ FAIL** | HIGH | Application Settings Scattered Across Resources
* Description: Application configurations are decentralized and inconsistently managed
* **❌ FAIL** | HIGH | Infrastructure Configuration Management Gaps
* Description: Infrastructure configurations lack centralized management and version control
* **❌ FAIL** | MEDIUM | Database Configuration Management Issues
* Description: Database configurations are manually managed without centralized control
* **❌ FAIL** | MEDIUM | Monitoring and Alerting Configuration Inconsistencies
* Description: Monitoring configurations are inconsistently applied across resources

KSI-SVC-05

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Cryptographicintegrity Checks:**

* **✅ PASS** | HIGH | Container Image Signing and Verification
* Description: Container images should be cryptographically signed and verified before deployment
* **✅ PASS** | MEDIUM | Infrastructure as Code Template Validation
* Description: IaC templates should be cryptographically signed and validated before deployment
* **❌ FAIL** | CRITICAL | Virtual Machine Boot Integrity Failures
* Description: Virtual machines lack proper boot integrity verification
* **❌ FAIL** | HIGH | Application Code Integrity Gaps
* Description: Application code lacks proper cryptographic integrity verification
* **❌ FAIL** | HIGH | Database Integrity Protection Deficiencies
* Description: Database lacks comprehensive cryptographic integrity protection
* **❌ FAIL** | MEDIUM | File System Integrity Monitoring Gaps
* Description: File system lacks comprehensive integrity monitoring and protection

KSI-SVC-06

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 3 | Failed: 4

**Keyandcertificaterotation Checks:**

* **✅ PASS** | HIGH | Azure Key Vault Automatic Key Rotation
* Description: Encryption keys should have automatic rotation policies configured
* **✅ PASS** | HIGH | SSL/TLS Certificate Lifecycle Management
* Description: SSL/TLS certificates should have automated renewal and deployment
* **✅ PASS** | MEDIUM | Azure App Service Managed Certificate Automation
* Description: App Service should use managed certificates with automatic renewal
* **❌ FAIL** | CRITICAL | Manual Certificate Management on Legacy Systems
* Description: Legacy systems using manual certificate management without rotation automation
* **❌ FAIL** | HIGH | Service Principal Secret Rotation Failures
* Description: Service principal secrets lack automated rotation causing security risks
* **❌ FAIL** | HIGH | Database Connection String Rotation Gaps
* Description: Database connection strings and authentication credentials lack proper rotation
* **❌ FAIL** | MEDIUM | API Key and Token Management Deficiencies
* Description: API keys and authentication tokens lack proper lifecycle management

KSI-SVC-07

**Status:** ⚠️ PARTIAL | Total Checks: 8 | Passed: 3 | Failed: 5

**Resourcepatching Checks:**

* **✅ PASS** | HIGH | Azure Update Management Automation
* Description: Virtual machines should use Azure Update Management for consistent patching
* **✅ PASS** | HIGH | Container Image Vulnerability Management
* Description: Container images should be regularly scanned and updated for vulnerabilities
* **✅ PASS** | MEDIUM | Azure PaaS Service Auto-Updates
* Description: PaaS services should have automatic updates enabled where available
* **❌ FAIL** | CRITICAL | Legacy System Patching Inconsistencies
* Description: Legacy systems show inconsistent and outdated patching practices
* **❌ FAIL** | HIGH | Third-Party Software Update Management Gaps
* Description: Third-party software lacks consistent update management and vulnerability tracking
* **❌ FAIL** | HIGH | Database and Middleware Patching Delays
* Description: Database and middleware systems show significant patching delays
* **❌ FAIL** | MEDIUM | Network Device Firmware Management Deficiencies
* Description: Network devices and security appliances lack consistent firmware update management
* **❌ FAIL** | MEDIUM | Mobile Device and Endpoint Patching Gaps
* Description: Mobile devices and endpoints show inconsistent patch management

TPR - Third Party & Resource Management

KSI-TPR-01

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 3 | Failed: 3

**Thirdpartyresourceidentification Checks:**

* **✅ PASS** | HIGH | Software Dependency Inventory
* Description: All software dependencies should be automatically discovered and cataloged across all environments
* **✅ PASS** | HIGH | Infrastructure as Code Dependency Scanning
* Description: IaC templates should be scanned to identify all third-party resources and dependencies
* **✅ PASS** | MEDIUM | Runtime Environment Discovery
* Description: Runtime environments should be continuously monitored to discover dynamically loaded third-party resources
* **❌ FAIL** | HIGH | Incomplete Third-Party Resource Documentation
* Description: Third-party resources lack comprehensive documentation including risk assessments and approval records
* **❌ FAIL** | MEDIUM | Shadow IT and Unauthorized Dependencies
* Description: Unauthorized third-party resources are being used without proper approval or security validation
* **❌ FAIL** | LOW | Third-Party Resource Change Detection Gaps
* Description: Changes to third-party resources are not consistently monitored and tracked for security implications

KSI-TPR-02

**Status:** ⚠️ PARTIAL | Total Checks: 5 | Passed: 2 | Failed: 3

**Fedrampauthorizationverification Checks:**

* **✅ PASS** | CRITICAL | FedRAMP Marketplace Authorization Verification
* Description: All cloud services handling federal information should be verified against the FedRAMP Marketplace
* **✅ PASS** | HIGH | Service Configuration Security Validation
* Description: FedRAMP authorized services should be configured according to security baselines and best practices
* **❌ FAIL** | CRITICAL | Unauthorized Service Usage Detection
* Description: Non-FedRAMP authorized services are being used to handle federal information
* **❌ FAIL** | HIGH | Service Authorization Monitoring Gaps
* Description: Continuous monitoring of service authorization status lacks comprehensive coverage and automation
* **❌ FAIL** | MEDIUM | Data Flow Analysis and Federal Information Identification
* Description: Data flows to third-party services lack comprehensive analysis to identify federal information handling

KSI-TPR-03

**Status:** ⚠️ PARTIAL | Total Checks: 6 | Passed: 2 | Failed: 4

**Supplychainriskassessment Checks:**

* **✅ PASS** | HIGH | Vendor Risk Scoring and Prioritization
* Description: Third-party vendors should be systematically assessed and prioritized based on risk factors
* **✅ PASS** | MEDIUM | Supply Chain Threat Intelligence Integration
* Description: Supply chain risk assessment should integrate threat intelligence for proactive risk identification
* **❌ FAIL** | HIGH | Incomplete Risk Mitigation Planning
* Description: Supply chain risk mitigation lacks comprehensive planning and implementation tracking
* **❌ FAIL** | MEDIUM | Limited Vendor Performance Monitoring
* Description: Vendor performance monitoring lacks comprehensive metrics and proactive management
* **❌ FAIL** | HIGH | Inadequate Business Continuity Planning
* Description: Business continuity planning lacks comprehensive vendor dependency analysis and alternative sourcing strategies
* **❌ FAIL** | MEDIUM | Missing Supply Chain Governance Framework
* Description: Supply chain governance lacks structured framework for risk oversight and decision-making

KSI-TPR-04

**Status:** ⚠️ PARTIAL | Total Checks: 7 | Passed: 3 | Failed: 4

**Thirdpartysoftwarevulnerabilitymonitoring Checks:**

* **✅ PASS** | CRITICAL | Automated Vulnerability Scanning
* Description: Third-party software components should be continuously scanned for known vulnerabilities
* **✅ PASS** | HIGH | Vulnerability Intelligence Integration
* Description: Vulnerability monitoring should integrate multiple intelligence sources for comprehensive threat awareness
* **✅ PASS** | MEDIUM | Contractual Notification Requirements
* Description: Vendor contracts should include security vulnerability notification requirements and SLAs
* **❌ FAIL** | HIGH | Incomplete Vulnerability Remediation Tracking
* Description: Vulnerability remediation lacks comprehensive tracking and SLA enforcement
* **❌ FAIL** | MEDIUM | Limited Vendor Security Communication
* Description: Vendor security communication lacks standardization and proactive engagement
* **❌ FAIL** | MEDIUM | Inadequate Threat Intelligence Integration
* Description: Threat intelligence lacks integration with vulnerability management for contextual risk assessment
* **❌ FAIL** | LOW | Missing End-of-Life and Deprecation Tracking
* Description: Third-party software end-of-life and deprecation status lacks systematic tracking and planning