INFORMATION SECURITY ASSESSMENT TOOL

For Local Government Success

MRSC

ACCESS CONTROL	Policies, Procedures, and Account Management	NIST AC-1 to AC-6; AC-17 to AC-20 PCI 3.2; 7; 8 WCIA/20 CrCtrl CSC 1; CSC 7; CSC 12; CSC 15

LEVEL 1	This control addresses the need for policy and procedures that effectively implement controls around access to computer systems and devices. An optimized set of policies and procedures would require dedicated personnel to document, maintain and manage access and authentication provisioning. This should include:	Current Maturity Rating* (1-5)
L-1	Procedures for activating, monitoring and auditing all network authentication and connections	
L-1	Procedures for provisioning new user accounts, including least privilege standards (only grant privileges to systems and shares that are required for their job)	
L-1	A regularly scheduled review of all accounts and purging of cancelled, stale, or unused accounts	
L-1	Current contact information for all account owners or managers	
L-1	Vendor and third party access procedures, auditing, and standards	
L-1	Remote access procedures, auditing, and standards	
L-1	Wireless access procedures, auditing, and standards	
L-1	Mobile device procedures, auditing, and standards	
L-1	De-provisioning standards, procedures, auditing, and documentation	

AWARENESS AND TRAINING	Information Security Awareness Training, Auditing, and Exercises	NIST AT-1 to AT-5 PCI 12.6; 12.8 WCIA/20 CrCtrl CSC 9

LEVEL 1	A mature awareness program will require dedicated personnel to document, manage, deliver and maintain. It will include:	Current Maturity Rating* (1-5)
Documented training, auditing, and exercises for employees and vendors on:		
L-1	Acceptable use of all of the organization's cyber assets	
L-1	Email security guidelines and phishing prevention/awareness	
L-1	Password and antivirus policy	
L-1	Remote access policies, standards, and procedures	
L-1	Mobile device policies and standards	
L-1	Server and desktop security control and configuration standards (e.g. antivirus, firewall(s))	
L-1	Wireless device standards and procedures	
L-1	Personal device standards and policy	
L-1	Social media acceptable use and policy	
L-1	Indications of virus or other compromises	
L-1	Appropriate responses to issues or problems	
L-1	Up-to-date contact information to report issues or ask for assistance	

*1 = Initial | 2 = Repeatable | 3 = Defined | 4 = Managed | 5 = Optimizing See the *Information Security Assessment Tool User Guide* for maturity rating descriptions.

CONFIGURATION MANAGEMENT	Policy	NIST CM-2 to CM-5 PCI 1.x WCIA/20 CrCtrl CSC 10

LEVEL 1	A mature configuration management policy would require someone tasked with maintaining and documenting up-to-date configuration standards, procedures, and auditing for all of your cyber assets, including:	Current Maturity Rating* (1-5)
L-1	All network devices	
L-1	Any preventative or detective control systems, e.g. antivirus, firewall(s), Intrusion Prevention or Detection Systems (IPS/IDS)	
L-1	Desktops and laptops	
L-1	Mobile devices	
L-1	Databases	

CONFIGURATION MANAGEMENT	Malware Defense	NIST SI-3 PCI 5 WCIA/20 CrCtrl CSC 5

LEVEL 1	Mature malware defense requires:	Current Maturity Rating* (1-5)
L-1	Documented and audited procedure that ensures antivirus applications are consistent across the enterprise, kept up to date with current engines and signature files and consistently patched.	

PHYSICAL AND ENVIRONMENTAL PROTECTION	Physical Access Controls	NIST PE-1 to PE-20 PCI 9

LEVEL 1	A mature set of physical controls should include:	Current Maturity Rating* (1-5)
L-1	Full background checks for any new hires with access to sensitive or critical infrastructure data	
L-1	Secure physical access controls (e.g. card key locks & ID badges) for any rooms, areas, or facilities containing cyber assets	
L-1	Documented and audited authentication provisioning for access control systems (e.g. card keys)	
L-1	Regularly audited logging of ingress/egress events and retention of logs for an appropriate amount of time	
L-1	Enhanced authentication (biometric, two-factor, etc.) for critical or sensitive assets	
L-1	Guards, surveillance cameras, fences, “man-trap” doorways, locks, and/or hardened windows/entrances to prevent unauthorized access for all facilities	
L-1	Policy and regular training for employees on keeping their workplace physically safe, as well as appropriate remote access, physical security at home or on the road, and mobile device physical security, etc.	
L-1	Special training for guards on cyber asset protection	
L-1	Adequate, documented, audited, and continuous fire, flood, and other disaster protection and training	
L-1	Backup and redundant power and HVAC systems for physical systems requiring a constant power supply and temperature	

ACCESS CONTROL	Account Monitoring and Response	NIST AC-7 to AC-14 PCI 10 WCIA/20 CrCtrl CSC 16

LEVEL 2	A mature account monitoring system and process would require dedicated personnel responsible for the following.	Current Maturity Rating* (1-5)
	Monitoring and response to any anomalous behavior on the network or computer systems, e.g.: L-2 Unsuccessful login attempts L-2 Session locks or unexpected terminations L-2 Access by new or unauthorized accounts	

ASSESSMENT AND TRAINING	Continuous Monitoring	NIST CA-7 PCI 10 WCIA/20 CrCtrl CSC 14

LEVEL 2	A mature monitoring system and process would require dedicated personnel responsible for the following:	Current Maturity Rating* (1-5)
	L-2 Research and acquisitioning assistance for optimum network and desktop monitoring solutions L-2 Development and deployment of monitoring hardware and software L-2 Documented configuration and deployment procedures and standards L-2 Maintenance and updating procedures L-2 Configuration and ongoing refinement of alerting and response procedures	

CONFIGURATION MANAGEMENT	Patch Management	NIST CM-11; PL-2 PCI 6.2 WCIA/20 CrCtrl CSC 3

LEVEL 2	Maturity in a patch management system would require:	Current Maturity Rating* (1-5)
	L-2 Personnel dedicated to the monitoring, auditing, and management of all network, software or hardware assets and their upgrades or configuration changes, including documentation and follow-up of all changes	

CONFIGURATION MANAGEMENT	Configuration Settings	NIST CM-6 PCI 2.2 WCIA/20 CrCtrl CSC 3; CSC 10; CSC 11

LEVEL 2	Maturity in this area would require:	Current Maturity Rating* (1-5)
	L-2 Set of specific hardening guidelines and configuration settings for all devices and systems on the network.	

CONTINGENCY AND RESPONSE PLANNING	Comprehensive Computer Systems Backup Process	NIST CP-9; CP-10 PCI 9.5.1 WCIA/20 CrCtrl CSC 8

LEVEL 2	An optimized backup system should include:	Current Maturity Rating* (1-5)
L-2	Policy on when, how, and what is backed up that is signed by the highest executive in the organization	
L-2	Procedural and standards documentation on the devices and systems used to do the backups	
L-2	Documented configuration, storage, and retention standards for backup media, including encryption standards where appropriate	
L-2	Documented and audited backup schedules	
L-2	Tested and documented recovery procedures scheduled at least once per year	

RISK ASSESSMENT	Risk Management Procedures	NIST RA-1 to RA-6 PCI 12.2

LEVEL 2	A mature risk management process will include:	Current Maturity Rating* (1-5)
L-2	Personnel specifically tasked with facilitating, documenting, and acquiring executive approval/signatures for a regularly scheduled cyber risk assessment	
L-2	Assessments of penetration testing both from inside and outside the firewall(s)	
L-2	A thorough review of critical cyber assets and their associated vulnerabilities	
L-2	A risk-prioritizing formula used that takes into account the level of impact/cost if an asset is compromised, the likelihood that a vulnerability will be exploited against that asset, and the cost/time required to mitigate the vulnerability	
L-2	A prioritized and dynamically updated documentation of mitigation strategies including: (1) Specific assignments of tasks to be completed and responsible personnel (2) Timelines for completion (3) Financial budget estimates (4) Other resource estimates, including human and hardware/software and O&M	
L-2	Cyber Insurance policies as appropriate to your organization's mission, criticality, and risk level	

SYSTEMS AND COMMUNICATIONS PROTECTION	Application Data Security Controls	NIST SC-1 to SC-6 PCI 6 WCIA/20 CrCtrl CSC 6

LEVEL 2	Mature application data controls include:	Current Maturity Rating* (1-5)
L-2	Separation of application data sets into discreet virtual LANs	
L-2	Specific application access controls for administrators and users on a need-to-know basis	
L-2	Documented, monitored, and audited access logs for all applications and databases	
L-2	Robust redundant channels to protect against DDOS attacks	

ASSESSMENT AND TRAINING	Penetration Testing	NIST CA-8 PCI 11 WCIA/20 CrCtrl CSC 20

LEVEL 3	A mature penetration testing procedure would require dedicated personnel or third party contractors responsible for:	Current Maturity Rating* (1-5)
L-3	Regular updating and maintenance of penetration testing protocols and tools	
L-3	Regularly scheduled comprehensive testing of your network perimeter	
L-3	Regularly scheduled internal authenticated testing of all network systems	
L-3	Regularly scheduled testing for rogue wireless systems	
L-3	Reporting and mitigation plan development for all critical or high level issues or vulnerabilities identified	

CONFIGURATION MANAGEMENT	Change Control and Asset Management	NIST CM-8 to CM-11 PCI 1.1.1; 6.4 WCIA/20 CrCtrl CSC 1; CSC 2

LEVEL 3	A mature change control procedures and policy would require:	Current Maturity Rating* (1-5)
L-3	Documented procedure for identifying current software and hardware upgrades, testing and deploying those in a timely manner. It would also include comprehensive auditing and documentation of patch levels for all identified cyber assets.	

CONTINGENCY AND RESPONSE PLANNING	BC/DR Policy and Procedures	NIST CP-1 to CP-8

LEVEL 3	A mature set of BC/DR procedures would include:	Current Maturity Rating* (1-5)
L-3	All department management as stakeholders	
L-3	Detailed documentation of the specific vital and critical tasks assigned to each department and plans to continue those tasks after a disaster or other incident	
L-3	Defined roles and responsibilities for recovery	
L-3	Alternative worksites	
L-3	Data and IT specific guidance on secure maintenance of availability of data during and after an event	
L-3	A comprehensive communications plan	
L-3	A regular exercise program including all stakeholders	
L-3	After-action analysis of any exercise or event including a project plan to mitigate any findings	

INCIDENT RESPONSE	Cyber Incident Response Policy and Procedures	NIST IR-1 to IR-10 PCI 12.10 WCIA/20 CrCtrl CSC 18

LEVEL 3	A mature incident response capability will include:	Current Maturity Rating* (1-5)
L-3	At least one full-time employee tasked with the documentation, maintenance, and overall management of your incident response planning and procedures	
L-3	Regularly scheduled exercises and after-action documentation for each exercise (or major incident response)	
L-3	Formal project management for remediation of issues or suggested enhancements arising from after-action analyses	
L-3	Regular training for incident response team on event analysis, forensics techniques, etc.	
L-3	Documented procedures, including: • Defined roles and responsibilities for all responders • Alerting and triage procedures • Communications and reporting guidelines • Specific regulatory sections (e.g. PCI required breach response protocol for Visa, MC, etc.) • Signed by executive – highest level possible	
L-3	Documented response playbook, including: • First on scene response check-list/triage guidance • Up-to-date and regularly maintained contact information for executives and incident response team • Up-to-date and regularly maintained contact information for all responders or possible stakeholders (e.g. department management, public safety, physical facilities managers, HR, legal, PIO, executive admins; execs) • Responsibilities checklist for each of the roles defined in the incident response procedure document • Full, complete, precise, and up-to-date documentation of all organizational network systems including contact information for the custodians or any third party vendors tasked with maintenance and monitoring of the network (who should be on your incident response team) • Specific guidance for responding to a breach of personally identifiable information (PII) • A detailed communications plan including sample messages to different stakeholders and management, frequency of notification guidance, and sample report templates • Guidance and contact information on when it is appropriate to contact law enforcement or other third parties for assistance (or just to notify), including what should be shared and the secure and safe way to share it • Up-to-date documentation and technical instructions on use of response and computer forensics tools and systems	

MEDIA PROTECTION	Data Categorization Procedures and Standards	NIST MP-1 to MP-8; SC-12 PCI 3 WCIA/20 CrCtrl CSC 15

LEVEL 3	A mature data categorization program will include:	Current Maturity Rating* (1-5)
L-3	Documented standards and procedures to: (1) ascertain and assign different levels of data sensitivity (2) label and store data according to its sensitivity (3) encrypt data at rest and/or in transit based on its sensitivity and categorization	
L-3	Encryption protocols, standards, and tools	
L-3	Encryption key management procedures and documentation	
L-3	Data retention and destruction guidelines based on its categorization	
L-3	Data and data storage access controls based on need to know	
L-3	Documented monitoring and auditing procedures to enforce media protection	

SYSTEM AND SERVICES ACQUISITION	Computer Systems and Services Procurement and Vendor Controls	NIST SA-1 to SA-9; SA-12 to SA-14

LEVEL 3	A mature procurement and vendor security management program would include:	Current Maturity Rating* (1-5)
L-3	Specific cybersecurity qualification requirements in all RFQs	
L-3	Data security requirements as appropriate in contracts awarded	
L-3	Data security auditing language in any contract with third parties needing access to sensitive data or systems	
L-3	Specific procedures and guidelines for on-site or remote vendor access to any internal systems, applications, or data	

SYSTEM AND SERVICES ACQUISITION	Secure Development Controls	NIST SA-10 to SA-11; SA-15 to SA-22 PCI 6 WCIA/20 CrCtrl CSC 19

LEVEL 3	A mature program will include:	Current Maturity Rating* (1-5)
L-3	Specific guidance, documentation, testing, and auditing of all application development during the entire lifecycle of the application. It will also include ongoing training and testing of your or your vendor's developers in secure application development techniques and protocols.	

SYSTEMS AND COMMUNICATIONS PROTECTION	Boundary Defense	NIST SC-7 to SC-11 PCI 10 WCIA/20 CrCtrl CSC 13

LEVEL 3	A mature boundary defense program includes:	Current Maturity Rating* (1-5)
L-3	Limited external exposure via NAT firewall and physically separated sub-networks	
L-3	Comprehensive monitoring of inbound traffic	
L-3	Redundant and robust service providers to provide protection from DDOS attacks	
L-3	Detection and denial of known bad out-bound traffic	
L-3	Detection and denial of exfiltration of sensitive data	
L-3	Hardened port and systems protocols	

SYSTEM INTEGRITY PROTECTION	Malicious Code Protection	NIST SI-3 PCI 10 WCIA/20 CrCtrl CSC 5

LEVEL 3	Mature malicious code protection includes:	Current Maturity Rating* (1-5)
L-3	Host and client based intrusion detection and prevention tools (IDS/IPS)	
L-3	Documented procedures for consistent and dynamic updating of signature files	
L-3	Non-signature based anomaly detection tools	
L-3	File integrity monitoring systems	
L-3	Event log monitoring and alerting systems for all operating systems	
L-3	Database access logging and alerting systems	

SYSTEM INTEGRITY PROTECTION	Information System Monitoring	NIST SI-4 PCI 10 WCIA/20 CrCtrl CSC 14	
LEVEL 3	**A mature monitoring system and process would require dedicated personnel responsible for the following:**		**Current Maturity Rating* (1-5)**
L-3	Research and acquisitioning assistance for optimum network and desktop monitoring solutions		
L-3	Development and deployment of monitoring hardware and software		
L-3	Documented configuration and deployment procedures and standards		
L-3	Maintenance and updating procedures		
L-3	Configuration and ongoing refinement of alerting and response procedures		

This Information Security Assessment Tool was developed by MK Hamilton & Associates in cooperation with MRSC and the State Auditor's Office, Local Government Performance Center.