Data Security Self-Assessment

The checklist that follows includes a series of data security items that meet NIST 800-53 standards, which is required for some Federal contracts. This provides a good sense of where an organization falls in terms of data security. Your state agency might have different security standards or requirements. This example is meant to show a robust set of data security processes and controls and can help your IT department assess data security on various dimensions. To learn more about these controls, see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
Identification, Authorization, and Access Control				
1	Do your systems uniquely identify and authorize organizational users (or processes acting on behalf of organizational users) in a manner that cannot be repudiated and which sufficiently reduces the risk of impersonation? [IA-2, IA-4, IA-4(4)]			
2	Do your systems require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2(1), IA-2(3)]			
3	Do your systems fully comply with Digital Identity Level 2 (AAL2, IAL2, FAL2) or higher? [NIST SP 800-63]			*State the Digital Identity Level and provide sufficient details demonstrating that the system complies with this level, consistent with NIST SP 800-63 and FedRAMP guidance.*
4	Do your systems restrict non-authorized personnel’s access to resources? [AC-6(2)]			
5	Do your systems restrict non-privileged users from performing privileged function? [AC-6(10)]			
6	Do your systems ensure secure separation of customer data? [SC-4]			
7	Do your systems ensure secure separation of customer processing environments? [SC-2, SC-3]			
8	Do your systems restrict access of administrative personnel in a way that limits the capability of individuals to compromise the security of the information system? [AC-2(7)]			
Audit, Alerting, Malware, and Incident Response				
1	Do your systems have the capability to detect, contain, and eradicate malicious software? [SI-3, SI-3 (1), SI-3 (2), SI-3 (7), MA-3 (2)]			

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
2	Do your systems protect audit information from unauthorized access, modification, and deletion? [AU-7, AU-9]			
3	Do you or your agency have the capability to detect unauthorized or malicious use of the system, including insider threat and external intrusions? [SI-4, SI-4 (4), SI-7, SI-7 (7)]			
4	Do you or your agency have an Incident Response Plan and a fully developed Incident Response test plan? [IR-3, IR-8]			
5	Do you or your agency have a plan and capability to perform security code analysis and assess code for security flaws, as well as identify, track, and remediate security flaws? [SA-11, SA-11 (1), SA-11 (8)]			*If the system contains no custom software development, do not answer Y or N. Instead, state "NO CUSTOM CODE" here.*
6	Do you or your agency implement automated mechanisms for incident handling and reporting? [IR-4 (1), IR-6 (1)]			
7	Do you or your agency retain online audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and offline for at least one year to meet regulatory and organizational information retention requirements? [AU-7, AU-7 (1), AU-11]			
8	Do you or your agency have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? [FedRAMP Incident Communications Procedure]			
Contingency Planning and Disaster Recovery				
1	Do you or your agency have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? [CP-2, CP-2 (2), CP-2 (3), CP-9, CP-10]			
2	Do you or your agency have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with NIST Special Publication 800-34? [CP-2, CP-8]			
3	Do your systems have alternate storage and processing facilities? [CP-6, CP-7]			
4	Do your systems have or use alternate telecommunications providers? [CP-8, CP-8 (2)]			
5	Do your systems have backup power generation or other redundancy? [PE-11]			

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
6	Do you or your agency have service level agreements (SLAs) in place with all telecommunications providers? [CP-8 (1)]			
Configuration and Risk Management				
1	Do you or your agency maintain a current, complete, and accurate baseline configuration of the information system? [CM-2]			
2	Do you or your agency maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8]			
3	Do you or your agency have a Configuration Management Plan? [CM-9, CM-11]			
4	Do you or your agency follow a formal change control process that includes a security impact assessment? [CM-3, CM-4]			
5	Do you or your agency employ automated mechanisms to detect inventory and configuration changes? [CM-2(2), CM-6(1), CM-8(3)]			
6	Do you or your agency prevent unauthorized changes to the system? [CM-5, CM-5(1), CM-5(5)]			
7	Do you or your agency establish configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6]			*If "yes," describe whether the configuration settings are based on Center for Internet Security (CIS) Benchmarks or United States Government Configuration Baseline (USGCB), or "most restrictive consistent with operational requirements."*
8	Do you or your agency ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP)-validated or SCAP-compatible (if validated checklists are not available)? [CM-6]			
9	Do you or your agency perform authenticated operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable? [RA-5, RA-5(5)]			*Describe how vulnerability scans were fully authenticated.*
10	Do you or your agency demonstrate the capability to remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days and Low vulnerabilities within 180 days? [RA-5, FedRAMP Continuous Monitoring Guide]			*Describe how you or your agency remediates High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days.*
11	When a High vulnerability is identified as part of ConMon activities, Do you or your agency			

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
	consistently check audit logs for evidence of exploitation? [RA-5(8)]			
Data Center Security				
1	Do you or your agency restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8]			
2	Do you or your agency monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8]			
3	Do you or your agency monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6 (1)]			
Security Awareness Training				
1	Do you or your agency train personnel annually on security awareness and role-based security responsibilities?			
Change Management Maturity				
1	Do you or your agency's change management capability include a fully functioning Change Control Board (CCB)?			
2	Do you or your agency have and use development and/or test environments to verify changes before implementing them in the production environment?			
Vendor Dependencies and Agreements				
1	Do your systems have any dependencies on other vendors, such as a leveraged service offering, hypervisor and operating system patches, physical security, and/or software and hardware support?			
2	Within the system, are all products still actively supported by their respective vendors?			*If any are not supported, answer, "No."*
3	Do you or your agency have a formal agreement with a vendor, such as for maintenance of a leveraged service offering?			
4	Does your organization intend to use a vendor that will have access to MDRC's information and if so, do you evaluate the vendor's security programs to ensure they are capable of protecting the data they will receive? Please describe.			
5	If yes, in which country is the vendor located?			
Continuous Monitoring (ConMon) Capabilities				

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Do you or your agency have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period?			
2	Do you or your agency have the ability to scan all hosts in the inventory?			
3	Do you or your agency have the ability to provide scan files in a structured data format, such as CSV, XML, or .nessus files?			
Federal Mandates				
1	Are FIPS 140-2 Validated cryptographic modules consistently used where cryptography is required?			
2	Do you or your agency have the ability to consistently remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days?			
4	Do your systems's external DNS solution support DNS Security (DNSSEC) to provide origin authentication and integrity verification assurances? Please note: You may consider alternative implementations for DNSSEC. Be sure to describe an alternative implementation for DNSSEC in the Comments section.			
5	Do your systems's external DNS solution support DNS Security (DNSSEC) to provide origin authentication and integrity verification assurances? Please note: You may consider alternative implementations for DNSSEC. Be sure to describe an alternative implementation for DNSSEC in the Comments section.			

Source: MDRC FedRamp Third Party Security Assessment