NIST Compliance for Services

SL No:	Services	NIST compliance control list	Description
1	24x7 Security Operation Center – Implementation and Finetuning	AU-2 EVENT LOGGING	Identify the types of events that the system is capable of logging in support of the audit function a. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; b. Specify the event types for logging within the system]; c. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and d. Review and update the event types selected for logging e. Review and update the event types selected for logging
		AU-3 CONTENT OF AUDIT RECORDS	Ensure that audit records contain information that establishes the following: What type of event occurred; a. When the event occurred; b. Where the event occurred; c. Source of the event; d. Outcome of the event; and e. Identity of any individuals, subjects, or objects/entities associated with the event. f. Identity of any individuals, subjects, or objects/entities associated with the event.
		AU-4 AUDIT LOG STORAGE CAPACITY	Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.
2	24x7 Security Operation Center – Active Monitoring	CA-7 CONTINUOUS MONITORING	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes: Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics]; a. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness; b. Ongoing control assessments in accordance with the continuous monitoring strategy; c. Ongoing monitoring of the system and organization-defined metrics in accordance with the continuous monitoring strategy; d. Correlation and analysis of information generated by control assessments and monitoring; e. Response actions to address results of the analysis of control assessment and monitoring information; and

			f. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]. g. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].
		IR-5 INCIDENT MONITORING	Track and document incidents.
		RA-5 VULNERABILITY MONITORING AND SCANNING	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.
3	Security Advisory services	CM-5 ACCESS RESTRICTIONS FOR CHANGE	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
		CM-7 LEAST FUNCTIONALITY	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services:
4	Threat Hunting Services	RA-10 THREAT HUNTING	a. Establish and maintain a cyber threat hunting capability to: 1. Search for indicators of compromise in organizational systems; and 2. Detect, track, and disrupt threats that evade existing controls; and b. Employ the threat hunting capability [Assignment: organization-defined frequency].
5	Cyber Emergency Response	IR-8 INCIDENT RESPONSE PLAN	a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents;

			6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Addresses the sharing of incident information; 9. Is reviewed and approved 10. Explicitly designates responsibility for incident response b. Distribute copies of the incident response plan c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; d. Communicate incident response plan changes e. Protect the incident response plan from unauthorized disclosure and modification.
6	Active Vulnerability Management – External Network	CA-2 CONTROL ASSESSMENTS	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; d. Assess the controls in the system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; e. Produce a control assessment report that document the results of the assessment; and f. Provide the results of the control assessment
		CA-8 PENETRATION TESTING	Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies
7		CA-2 CONTROL ASSESSMENTS	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

	Active Vulnerability Management – Internal Network		b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; d. Assess the controls in the system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; e. Produce a control assessment report that document the results of the assessment; and f. Provide the results of the control assessment
		CA-8 PENETRATION TESTING	Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies
8	Active Penetration testing – Full Blackbox/Greybox	CA-8 PENETRATION TESTING	Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies
9	Active Penetration testing –Periodic Scans	CA-8 PENETRATION TESTING	Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies
10	Threat intelligence service	PM-16 THREAT AWARENESS PROGRAM	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

11	Red & Purple team activities	RA-3 RISK ASSESSMENT	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments; c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]]; d. Review risk assessment results [Assignment: organization-defined frequency]; e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.
12	OSINT Threat Exposure Assessment	SC-28 PROTECTION OF INFORMATION AT REST	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].
13	Threat Modeling	CM-4 IMPACT ANALYSES	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.
14	Wireless Penetration Testing	AC-18 WIRELESS ACCESS	Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access
		CA-8 PENETRATION TESTING	Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies
15	Security Configuration Assessment	CM-6 CONFIGURATION SETTINGS	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
		CM-2 BASELINE CONFIGURATION	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system:
16		IR-5 INCIDENT MONITORING	Control: Track and document incidents

	Active Attack Surface Monitoring	IR-6 INCIDENT REPORTING	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Report incident information to [Assignment: organization-defined authorities].
17	Malware Analysis	SI-3 MALICIOUS CODE PROTECTION	Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways, including by electronic mail, the world-wide web, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Malicious code protection mechanisms include both signature- and non-signature-based technologies. Non-signature-based detection mechanisms include artificial intelligence techniques that use heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective. Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Non-signature-based mechanisms also include reputation-based technologies. In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in commercial off-the-shelf software as well as custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions. In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended
18	Cyber Forensics	CP-10 SYSTEM RECOVERY AND RECONSTITUTION	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.
19	Response Readiness Assessment	IR-3 INCIDENT RESPONSE TESTING	Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations
		IR-7 INCIDENT RESPONSE ASSISTANCE	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.
		IR-8 INCIDENT RESPONSE PLAN	It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information (i.e., breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.