Function	Category	Subcategory	DNS Relevant activities/outcomes
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	· Document inventory of recursive DNS servers · Document inventory of internal authoritative DNS servers · Document inventory of external authoritative DNS servers · Document use of external DNS providers for recursion or authoritative DNS · Document inventory of resolvers (clients, stub resolvers)
		ID.AM-2: Software platforms and applications within the organization are inventoried	· Document DNS vendor and software version for recursive DNS servers · Document DNS vendor and software version for authoritative DNS servers · Document DNS vendor and software version for external authoritative DNS servers · Document resolver vendor and version of resolvers (clients, stub resolvers)
		ID.AM-3: Organizational communication and data flows are mapped	· Map Internet DNS resolution data flows - resolvers perhaps scoped within a given geography resolve to a given set of recursive servers which may forward to centralized caching servers and out to the Internet and back · Map internal DNS resolution data flows - resolvers perhaps scoped within a given geography resolve to a given set of recursive servers which may forward to centralized caching servers and to internal authoritative DNS servers and back · External DNS servers should be queried only from Internet sources and should have recursion disabled · Map communications flows for threat monitoring, detection, reporting, escalation, recovery, postmortem, and external communications
		ID.AM-4: External information systems are catalogued	· Documentation of DNS policies consistent with enterprise security policy related to external devices · External DNS system services for recursive and authoritative services comply with organizational and relevant regulatory security requirements · External DNS services administrator access policies including access recovery procedures are documented
		ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	· Categorize and prioritize DNS servers accordingly, plan for contingencies compromise could affect ability to resolve DNS (recursive, resolver) and redirect external end users (authoritative compromise) · Categorize DNS software vendor supply chain risk · Define contingencies for DNS server failure or failure of external DNS provider(s)
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· Document roles and responsibilities for those responsible for each DNS server including third parties and service provider(s) · Consider DNS within business process definitions for information security and resulting risk, along with information protection needs (e.g., DNS tunneling, APTs)
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	· Procure and deploy DNS servers and/or DNS services which include security features, non-custom configurations, from diverse suppliers on an approved vendors list from approved countries, etc.
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	· Categorize and prioritize DNS servers according to criticality, plan for continencies compromise could affect ability to resolve DNS (recursive, resolver) and redirect external end users (authoritative compromise) · Define contingencies for DNS server failure or failure of external DNS provider(s)
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· Consider DNS within business process definitions for information security and resulting risk, critcality assessment, along with information protection needs (e.g., DNS tunneling, APTs)
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· Include DNS infrastructure in critical infrastructure plan · Plan for protected and /or uninterruptible power for DNS servers as appropriate · Plan for diverse telecom facilities to the Internet and DNS service providers · Plan for diversity for external trust sector with in-house and/or one or more external DNS service providers · Consider DNS within business process definitions for information security and resulting risk, critcality assessment, along with information protection needs (e.g., DNS tunneling, APTs)
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)	· Procure and deploy DNS servers and/or DNS services which include security features, non-custom configurations, from diverse suppliers on an approved vendors list from approved countries, etc. · Deploy DNS servers in accordance with the trust sector architecture · Deploy DNS servers with both IPv4 and IPv6 communications capabilities · External DNS services should be contracted to include high availability SLAs with one or more service providers · Consider DNS within business process definitions for information security and resulting risk, critcality assessment, along with information protection needs (e.g., DNS tunneling, APTs)

Function	Category	Subcategory	DNS Relevant activities/outcomes
IDENTIFY (ID)	**Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	· DNS inclusion in the organization's information security policy document, which is approved by management and published to employees and relevant external associates.
		ID.GV-2: Cybersecurity roles & responsibilities are coordinated and aligned with internal roles and external partners	· Roles and responsibilities for DNS security functions and processes and documented and communicated to associated employees and/or external (third party) associates
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· DNS inclusion in the organization's information security policy document, which is approved by management and published to employees and relevant external associates. Training is provided and acknowledgement of understanding of material is obtained.
		ID.GV-4: Governance and risk management processes address cybersecurity risks	· DNS inclusion in the organization's risk management processes which is approved by management and published to employees and relevant external associates. Training is provided and acknowledgement of understanding of material is obtained.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	· Document and track vulnerabilities for DNS server hardware components · Document and track vulnerabilities for DNS server kernels · Document and track vulnerabilities for DNS server operating systems · Document and track vulnerabilities for DNS server software applications · Document and track vulnerabilities for DNS resolver software applications on end user and other devices · Document and track vulnerabilities for the DNS protocol
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	· Actively monitor threat and vulnerability information sources like CERT, your DNS software vendor alerts and related reputable web resources · Collaborate with other security personnel especially within your industry to promote open sharing of threats, vulnerabilities and mitigations · Subscribe to security feeds offered by vendors who produce the operating systems and applications (DNS) software in use within your network.
		ID.RA-3: Threats, both internal and external, are identified and documented	· Monitor, document and track detected and reported vulnerabilities for DNS resolver and server software applications · Document threats related to personnel issues as well as natural and unnatural disasters. · Monitor, document and track detected and reported vulnerabilities for external DNS services and applications
		ID.RA-4: Potential business impacts and likelihoods are identified	· For each identified threat and vulnerability, document the related business impacts should the threat materialize. · For each identified threat and vulnerability, document the likelihood of the occurrence.
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· Assess the risk of each identified threat and vulnerability based on the likelihood and related business impacts of the occurrence · Iterate your analysis to consider the relative risk for higher priority assets, e.g., DNS servers, as identified in subcategory ID.AM-5. A given threat may have a higher impact when imposed on a master DNS server versus a slave for example.
		ID.RA-6: Risk responses are identified and prioritized	· Define and document the response procedures for each risk identified
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	· Establish and document risk management processes and garner participation and agreement by relevant organizational stakeholders
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· Define and gain consensus regarding the process for determining and documenting organizational risk including DNS
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	· Define and gain consensus regarding risk tolerance for each identified DNS risk
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1**: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	· Establish and document cyber supply chain risk management processes and garner participation and agreement by relevant organizational stakeholders
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	· Leverage the supply chain risk assessment process defined in the cyber risk management process document · Identify and document all DNS server hardware providers · Identify and document all DNS server software suppliers · Identify and document all external DNS service providers · Identify and document all resolver software providers · Assess and prioritize these providers with respect to the cyber supply chain risk assessment process
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	· Include appropriate security measures in contracts with third party partners and suppliers, particularly external DNS providers, to meet objectives outlined in the cyber supply chain risk management plan · Terms to consider including are vulnerability communications, business continuity scenarios, practices and testing, and incident management and recovery processes
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	· Periodically audit suppliers' and third party parnters' adherence to security-oriented contract terms, assesssing and documenting findings in accordance with the cyber supply chain management process · Review any adverse findings with corresponding suppliers to seek correction and/or remedies
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	· Exercise defined incident management and recovery processes with suppliers, particularly external DNS providers, to rehearse and validate defined action plans in advance of potential incidents.

Function	Category	Subcategory	DNS Relevant activities/outcomes
PROTECT (PR)	**Identity Management, Authentication, and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked and audited for authorized devices, users, and processes	· For each DNS component, identify and document authorized users · For each DNS component, enforce credentials requirements · For each DNS component, manage credentials refresh policies · For each DNS component, document an approval process for authorizing new users or expansion or contraction of existing users' permissions · For each DNS component, audit who has access and respective level of access and confirm or modify based on current job role
		PR.AC-2: Physical access to assets is managed and protected	· For each DNS component, define appropriate physical access protection requirements · For each DNS component, deploy in accordance with physical access requirements, e.g., within badge accessible data center · Document physical access permissions to restricted areas where DNS servers are deployed to confirm user permission with user appropriateness for access · Audit physical access logs and surveillance videos if appropriate with respect to access to restricted areas to confirm only appropriate users access
		PR.AC-3: Remote access is managed	· Deploy an extranet trust sector to partition remote access from a DNS perspective · Only staff (internal or contractors) with a job function and scope of responsibility necessitating remote access should be permitted access. · Login/password authentication should be required and communications should require an encrypted connection. · Command sets should be restricted if possible to only those required by each user.
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	· For each user identity, the level of access should provide only those commands or functions required of that user to perform his or her job function.
		PR.AC-5: Network integrity is protected (e.g., network segregation network segmentation)	· Deployment of DNS components in accordance with defined trust sectors provides containment to the corresponding trust sector.
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions when appropriate	· Validate user identities and corresponding credentials and manage ongoing with credentials or user responsibilities/need to know changes for DNS server local or remote access or access to external providers · Strong credentials for remote access are needed for identity verification. · Remote access is to be logged as is DNS server commands and diagnostic actions.
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	· Enable stricter credentials requirements if possible for riskier transactions such as deleting zones. · Command sets should be restricted if possible to only those required by each user. · Login/password authentication should be required and remote communications should require an encrypted connection.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	· Devise, develop and deliver a training program for IT security including DNS elements and garner acknowledgement of key aspects. · Keep training material up to date and require periodic update training for all users
		PR.AT-2: Privileged users understand their roles and responsibilities	· Document well-defined job descriptions outlining roles and responsibilities for all users. · For users whose job functions require privileged access, provide training and garner acknowledgement of respective responsibilities
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	· For third party stakeholders who require access, provide training and garner acknowledgement of respective responsibilities. · For external DNS services, document respective roles and responsibilities
		PR.AT-4: Senior executives understand their roles and responsibilities	· For executives, provide training and garner acknowledgement of respective roles and responsibilities.
		PR.AT-5: Physical and information security personnel understand their roles and responsibilities	· For physical and information security personnel, provide training and garner acknowledgement of respective roles and responsibilities.

Function	Category	Subcategory	DNS Relevant activities/outcomes
PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	· Secure DNS component hardware, harden your operating system, kernel and software · ACLs and transaction keys are implemented to protect authoritative DNS data from updates and zone transfers · ACLs are defined to control management access and management transactions are encrypted · Sign DNS zone data using DNSSEC; secure DNSSEC private keys and document rollover processes including emergency rollover · Periodic backups and storage of DNS configuration and logging data offsite provides a fallback for restoration in the event of server failure. · DNS logging and configuration data stored offsite must be transported and stored securely via encryption. · Monitor vulnerability sources and deploy vendor patches affecting data at rest. · Periodically audit DNS component access logs and functions performed to align with roles and responsibilities
		PR.DS-2: Data-in-transit is protected	· Configuration and zone data updated via console, remote access, or IPAM system are authenticated and encrypted · DNS resolution data is signed using DNSSEC. Authoritative zone data is signed and recursive servers perform DNSSEC validation · Source port and TXID numbers are randomized for outbound queries · Query case is randomized · ACLs are configured to control entitlement for queries, cache access, and zone transfers · Zone transfers and notifies are signed · Secure the resolver-to-recursive DNS server link via cookies or encryption like DNSCrypt · Monitor for DNS tunneling · Implement a DNS firewall and monitor for malware C&C queries · Monitor vulnerability sources and deploy vendor patches affecting DNS data in motion. · Implement DoS/DDoS controls such as inbound and outbound rate limiting, query throttling and anycast · Periodically audit DNS component access logs and functions performed to align with roles and responsibilities
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· For all DNS servers and resolvers, any proposed addition, movement or removal of DNS components must be documented, reviewed and approved by involved parties prior to commencement · Additions, changes, or deletions of DNS service provider parameters are carefully managed, tracked and verified
		PR.DS-4: Adequate capacity to ensure availability is maintained	· Deploy sufficient DNS capacity within each trust sector to provide acceptable resolution performance even in the event of an outage within the network and/or within your DNS server infrastructure. · Monitor capacity utilization over time and deploy additional infrastructure as necessitated by growing demand as appropriate
		PR.DS-5: Protections against data leaks are implemented	· ACLs are implemented to protect access to internal authoritative DNS data resolution. · External DNS authoritative data consists only of data relevant to externally accessible services · DNS tunneling detection and mitigation strategies are in place. · DNS firewall configuration helps prevent access to external sites for possible exfiltration
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· DNS configuration and zone file integrity checks are implemented to verify successful transfer and to detect changes · DNSSEC validation provides DNS resolution data integrity checking and origin authentication as well as authenticated denial of existence
		PR.DS-7: The development and testing environment(s) are separate from the production environment	· DNS servers are deployed within a lab network separate from the production network for testing of new releases, patches and new features
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	· Track serial numbers, ideally "burned into" and tamper-proof for each DNS server

Function	Category	Subcategory	DNS Relevant activities/outcomes
PROTECT (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	· For end user systems, the resolver software should be defined as included with the build, which almost always consists of that supplied with the corresponding device operating system. · For DNS servers, the list of hardware and software components, including operating systems, DNS software, security, monitoring and auditing utilities and so on, should be documented.
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	· Apply security engineering priciniples to your IT network and systems through integration with your systems development lifecycle, including in-house development projects from requirements analysis through coding and testing; product procurement activities likewise should include secrity considerations
		PR.IP-3: Configuration change control processes are in place	· The baseline configuration should be a controlled document, meaning that any additions, changes or deletions are proposed, reviewed, approved and communicated among relevant parties · Changes to the configuration of the authorized software, e.g., the DNS configuration, should also be planned, reviewed, approved and staged.
		PR.IP-4: Backups of information are conducted, maintained, and tested	· Backup DNS configuration files regularly for each set of servers as well as audit logs.
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	· Document and maintain policies and regulations regarding the physical operating environment for organizational assets such as DNS servers. This includes providing emergency power shut-off, fire protection, temperature and humidity controls, water damage protection and server room or datacenter access controls and auditing.
		PR.IP-6: Data is destroyed according to policy	· DNS configuration, resolution and log data deemed for disposal is destroyed according to policy to prevent information theft
		PR.IP-7: Protection processes are improved	· DNS data protection processes are continuously improved through periodic review, new technologies and lessons learned
		PR.IP-8: Effectiveness of protection technologies is shared	· DNS data protection technology effectiveness is shared with appropriate parties
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· DNS incident response and recovery plans are documented, communicated and managed. · DNS aspects of business continuity are incorporated into business continuity and disaster recovery plans
		PR.IP-10: Response and recovery plans are tested	· DNS incident response and recovery plans are tested and results fed back to improving such plans.
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· Security is incorporated into human resources processes relating to recruiting, hiring, evaluations as appropriate, training, and deprovisioning
		PR.IP-12: A vulnerability management plan is developed and implemented	· A DNS vulnerability management plan is developed and implemented incorporating those discussed within this book

Function	Category	Subcategory	DNS Relevant activities/outcomes
PROTECT (PR)	**Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	· Maintenance and repair of DNS servers should be performed and logged in a timely manner, with approved and controlled tools. · Maintenance and repairs should use pre-approved documented tools and processes. · Any repairs requiring support from outside personnel, e.g., vendor staff, should be pre-authorized and outside personnel should sign in and out and be escorted at all times by an authorized organization team member. · Repairs requiring removal of a DNS component must be approved along with associated contingencies and the component sanitized of any sensitive information such as user accounts.
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	· Any DNS server maintenance or repair performed remotely must be pre-approved and a remote connection opened for the duration of the activity. · Strong credentials for remote access are needed for identity verification. · Remote access is to be logged as is DNS server commands and diagnostic actions.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· DNS server and management system logs are identified and configured for tracking and storage for documentation of log records
		PR.PT-2: Removable media is protected and its use restricted according to policy	· Any removable media must be protected and its use restricted according to policy. Vendors may supply software updates via USB, DVD or other removable media format. Configuration and backup information may also be copied to removable media for backups. · Swappable hard drives may contain configuration or sensitive information. Such media must be securely stored to prevent unauthorized access to the media and such media must be securely transported if necessary and must be sanitized prior to disposal by the removal of any sensitive information stored on the media.
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	· Only those users whose job function and role necessitate access should be provided access to a given DNS component. · The breadth of functionality permitted for each user should be constrained to the extent possible by permission controls on the device. · DNS component access logs are periodically audited to verify appropriate user access and functions exectued match job function · The functionality of each component itself should be constrained to the minimum functionality required to perform that device's role. Hence, for a DNS server, any non-DNS related services excepting those necessary for diagnostics and auditing, should be removed. In addition, restrictions should be defined for unnecessary TCP/UDP ports, system or application files, processes, users, and the file system. DNS configuration maps to its respective trust sector role
		PR.PT-4: Communications and control networks are protected	· The deployment of trust sectors with accompanying ACLs and associated trust sector controls provide defense in depth protection · Management network access to DNS components is authenticated and encrypted
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	· Deploy DNS servers in accordance with a trust sector deployment approach with adequate redundancy and capacity to account for server outage(s). · Monitor DNS server vitals (CPU, I/O, etc.) to baseline "normal" levels and to detect spikes or rises in resource demand

Function	Category	Subcategory	DNS Relevant activities/outcomes
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	· DNS traffic is monitored and tracked historically to define a baseline of DNS traffic. · DNS server vitals (CPU, disk, memory, I/O) are monitored and tracked historically to define a baseline
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	· DNS traffic anomalies are analyzed to characterize each as a possible attack or otherwise; if an attack, attack details are discovered and documented for tracking and comparison with similarities to prior attacks to possibly apply prior solutions based on past lessons learned.
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	· DNS event data is aggregated and correlated with relevant network data from network and server event monitoring systems to supplement attack characterization and breadth · DNS event data is securely transmitted to broader network security event information systems to support correlation and troubleshooting
		DE.AE-4: Impact of events is determined	· The impact of DNS events is determined to facilitate prioritization of mitigation efforts
		DE.AE-5: Incident alert thresholds are established	· An incident response plan should be established to define potential incidents and the corresponding response plan. · The incident response plan should be reviewed, approved and updated periodically. · Thresholds and alerts in monitoring systems should be established to detect and report potential security incidents, e.g., for process and hardware states and well as I/O volumes. The response plan should also define incident analysis, containment, eradication and recovery, along with the communication of status reporting.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	· DNS traffic is monitored to detect cybersecurity events including general and DNS traffic volume (DOS/DDOS/PRSD/reflector), NXDOMAINS (bogus queries, malware/APTs), unusual traffic patterns (tunneling, malware/APTs) · DNS server vitals (CPU, disk, memory, I/O) are monitored against their baseline to detect unusually high utilization which could indicate a potential incident
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	· Monitoring of physical access controls and the physical environment where DNS components are located should be monitored to detect potential incidents. · Badge-in access should be required for access to critical infrastructure including DNS servers. · Access logs should be reviewed. · Surveillance systems should also be deployed and reviewed to detect "tailgating", the entry by an unauthorized person before the door closes for example, and physical removal of assets.
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	· DNS server and management system logs are reviewed periodically to confirm valid user access and activity; any anomalies are investigated as potential security events
		DE.CM-4: Malicious code is detected	· Regular virus scans are performed to detect malicious code · Monitor DNS traffic to identify characteristic DNS activity of malware · Block malware C&C center communications attempts with a DNS firewall
		DE.CM-5: Unauthorized mobile code is detected	· Regular virus scans are performed to detect malicious code · Monitor DNS traffic to identify characteristic DNS activity of malware · Block malware C&C center communications attempts with a DNS firewall
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· External system logs, e.g., for external DNS providers, cloud providers, etc., are reviewed periodically to confirm valid user access and activity; any anomalies are investigated as potential security events
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· Monitor for the incidence of unauthorized personnel in secure areas such as datacenters, connections to servers from unauthorized IP addresses, ports or credentials, any devices not specified within the asset inventory and any software installed on devices beyond that specified in the device baseline. · Any such incidence of noncompliance should trigger a notification for investigation in accordance with the incident response plan.
		DE.CM-8: Vulnerability scans are performed	· Periodic vulnerability scans should be performed to detect new vulnerabilities and to verify deployed mitigation controls. · Any new vulnerabilities or inadequate mitigation measures should be analyzed to assess overall relative risk based on likelihood and business impact and to define new or improved mitigation approaches for development and deployment.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	· Personnel roles and responsibilities for DNS security event detection within the organization are well defined
		DE.DP-2: Detection activities comply with all applicable requirements	· DNS security event detection activities are documented and enforced in accordance with event detection requirements
		DE.DP-3: Detection processes are tested	· DNS security event detection activities and systems are tested to characterize detection effectiveness
		DE.DP-4: Event detection information is communicated	· DNS security event detection information is communicated to appropriate parties in accordance with the incident response plan
		DE.DP-5: Detection processes are continuously improved	· DNS security event detection processes are continuously improved based on technology or process improvements as well as lessons learned from prior events

Function	Category	Subcategory	DNS Relevant activities/outcomes
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents	**RS.RP-1:** Response plan is executed during or after an incident	· As DNS security events are detected and characterized, relevant actions from the incident response plan are executed
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	· Personnel roles and responsibilities for DNS security event response within the organization are well defined within the incident response plan
		RS.CO-2: Incidents are reported consistent with established criteria	· DNS security incidents are detected and characterized in accordance with established criteria
		RS.CO-3: Information is shared consistent with response plans	· DNS security event response information is communicated to appropriate parties in accordance with the incident response plan
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· DNS security event response information is communicated to appropriate stakeholders in accordance with the incident response plan
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· DNS security event response information is communicated to external stakeholders in accordance with the incident response plan to faciltiate industry awareness of the attack and effective defensive measures
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	· DNS event detection systems are investigated to characterize the event as a potential attack or threat
		RS.AN-2: The impact of the incident is understood	· Upon incident detection, the incident should be analyzed to assess and understand the impact of the incident. · The incident response plan should be followed and impacted groups involved in responding to contain, eradicate, and recover from the incident, while communicating status in accordance with the response plan. · New information or lessons learned should be incorporated into an update of the response plan based on review, concurrence and approval by appropriate members of the organization.
		RS.AN-3: Forensics are performed	· Forensics analysis on detected incidents should be performed to go beyond the symptoms of the incident to identify the ultimate cause and to enumerate those vulnerabilities exploited or attacked. This analysis is useful for identifying new or morphed attack vectors and vulnerabilities, and to qualify the effectiveness of any defensive controls that were intended to protect against such an attack.
		RS.AN-4: Incidents are categorized consistent with response plans	· Incidents need to be categorized in a manner consistent with incident response plans. This is helpful in terms of prioritizing actions and inclusion of appropriate staff to analyze, contain, eradicate and resolve the incident in a timely manner.
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	· Define and document processes and procedures for obtaining, analyzing and responding to vulernability notifications that impact DNS including those for DNS vendor software, DNS protocol, operating system, kernel, or hardware components
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	· Deployment of DNS components in accordance with defined trust sectors provides containment to the corresponding trust sector. · Further containment steps must be undertaken based on the incident itself to prevent broader impact on multiple DNS servers, resolvers or other network systems.
		RS.MI-2: Incidents are mitigated	· As the incident is contained, contingency plans implemented, and forensics analyses conducted, mitigation approaches for the vulnerability that led to the successful incident should be defined, evaluated, agreed upon and implemented · Based on the particular incident, mitigate in accordance with recommended mitigation tactics. · The vulnerability list, risk assessment, incident response plan should be updated accordingly.
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	· Newly identified vulnerabilities need to be incorporated into the known vulnerability list. · Each new vulnerability should be analyzed with respect to likelihood and business impact to define relative risk. Based on this assessed risk, the vulnerability should be proactively mitigated or documented as an accepted risk.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	· After incident recovery, a post-mortem discussion with involved staff is useful for reviewing the incident, possible defensive and mitigation steps to improve response and recommended response plan updates to incorporate lessons learned.
		RS.IM-2: Response strategies are updated	· Incident response strategies should be reviewed and updated as appropriate
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	· The incident recovery plan is executed during or after an event. · During the event, contingencies and work-arounds are put in place to restore service levels in the face of a disruption, compromise or outage. · After incident eradication, affected systems should be restored to prior function to fully recovery to a known working state.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	· Recovery plans should also be updated to incorporate lessons learned.
		RC.IM-2: Recovery strategies are updated	· Recovery strategies should be reviewed and updated should any improvements be borne out of the analysis of the incident recovery.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	· Communications to customers and to the public in general are carefully managed to convey information regarding the incident, status of response and recovery and planned actions.
		RC.CO-2: Reputation is repaired after an event	· Typically the provisoin of meaningful information regarding the incident and what has been done to recover from the incident helps with preserving reputation but other steps may be necessary.
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	· Communications to internal stakeholders including executives and management are open and direct regarding the incident, status of response and recovery and planned actions including evaluation of alternative approaches if the attack persists