How Ivanti Maps to NIST Cybersecurity Framework 2.0

Table of Contents

Introduction: An Overview of NIST CSF

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is a voluntary framework that helps organizations manage and mitigate cybersecurity risk based on existing standards, guidelines and best practices. The CSF consists of three primary components: the Framework Core, Tiers and Profiles.[1]

For organizations that want to defend themselves from evolving threats in an ever-changing digital landscape — especially as they move into remote and hybrid work environments — it's essential to employ IT management and security tools that are abreast of CSF and align with its framework.

Updates to the NIST CSF

CSF 2.0, released in February 2024, is a major update to the NIST CSF. It reflects changes in the cybersecurity landscape and makes it easier to put the CSF into practice for all organizations. There are several important differences between the CSF 2.0 and the CSF 1.1:[2]

- The CSF 2.0 has an expanded scope that covers not only critical infrastructure sectors, but also other types of organizations and systems, such as cloud services, Internet of Things and supply-chain security.
- It adds a sixth function, Govern, to the Framework Core, which provides guidance on how to establish and maintain effective governance structures and processes for cybersecurity.
- It improves and expands the guidance on creating and using Profiles, which are customized representations of an organization's cybersecurity objectives, current state and desired state.
- It includes implementation examples for each Subcategory in the Framework Core, which illustrate how different organizations can apply the CSF to achieve specific outcomes.
- It updates the Informative References, which are external sources of standards, guidelines and practices that support the implementation of the Framework Core.

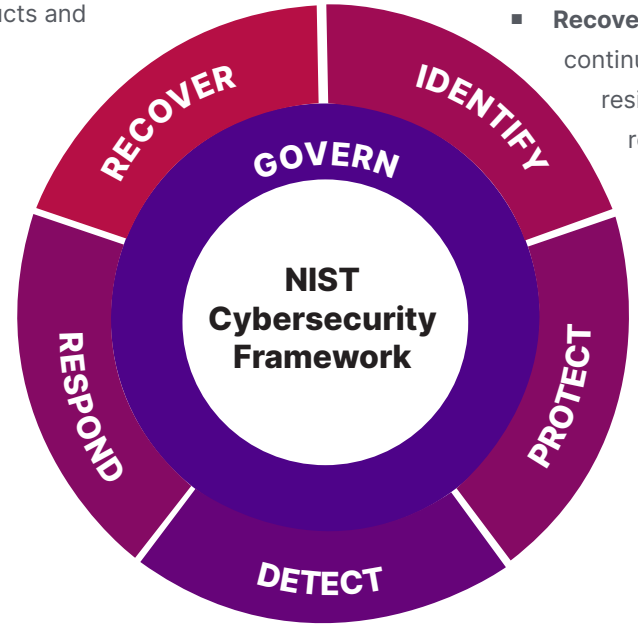
The CSF 2.0 aims to provide **a more flexible, adaptable and user-friendly framework** for improving cybersecurity across sectors and domains, incorporating feedback from the public comment period and workshops.

Functions of the CSF

In brief, here are the **six core functions** within the CSF 2.0 framework:

- **Govern:** This new function establishes and monitors an organization's cybersecurity risk management strategy, expectations and policy and covers people, process and technology elements that include the roles, responsibilities, policies, procedures and oversight in addition to the technology involved in implementing CSF 2.0. This function will help align the other five core CSF Functions with the broader organizational mission and stakeholder expectations.

- **Identify:** Having a complete inventory of assets and solutions is crucial for effective cybersecurity. After identifying and documenting the data collected, network flows and how data is stored, the next steps include finding and addressing threats and vulnerabilities; establishing cybersecurity policies, access controls and roles and responsibilities for employees; and maintaining a comprehensive risk-management strategy.
- **Protect:** It is essential to protect sensitive data, effective processes and technology controls. These include enforcing strong authentication, encrypting data, performing regular backups, deploying security products and using conditional access controls.
- **Detect:** Detecting cybersecurity incidents is crucial for any organization to prevent data breaches, ransomware, business disruption and advanced persistent threats. To achieve this, organizations need to implement control processes and procedures that are regularly evaluated. This involves leveraging automation and machine intelligence to monitor system logs, data flows and network instrumentation.
- **Respond:** This function ensures that your organization can quickly and efficiently respond to potential threats. This involves proper documentation, regular testing of response procedures and coordination with stakeholders. You can also implement automated response controls, such as outbound traffic detection, network segmentation and dynamic access control policies.
- **Recover:** This involves business continuity planning, recovery and resiliency testing. It includes root-cause analysis with documentation updates, managing public relations and company reputation and ensuring successful integration of ITIL (Information Technology Infrastructure Library) processes.



Using this document

Ivanti's solutions are designed to help organizations identify and prioritize potential threats and vulnerabilities, protect their critical assets and data, detect and respond to threats and incidents and complete the cybersecurity cycle by recovering from attacks.

In this document, we map Ivanti solutions packages to the NIST CSF 2.0 Functions, Categories and Subcategories, and explain how they align in detail. This will help you assess how Ivanti solutions will enable you to fulfill CSF 2.0 best practices.

Ivanti's Integrated Solutions

Enterprise Service Management (ESM) reduces costs, optimizes service performance and creates a secure, agile environment that is ready for the future.

Secure Unified Endpoint Management (SUEM) provides a unified view of devices, enabling efficient discovery, management and security of endpoints and vulnerabilities with accurate and actionable insights to enable faster remediation.

Vulnerability Management and Response (VM&R) efficiently and effectively prioritizes the vulnerabilities and weaknesses that pose your organization the most risk, for faster remediation to better protect against data breaches, ransomware and other cyberthreats.

Zero Trust Network Access (ZTNA) secures remote access to the web, cloud services and private applications.

Cyber Asset Attack Surface Management (CAASM) allows an organization to see all internal and external assets, identify and assess vulnerabilities and gaps in security controls and provide risk management with prioritization of vulnerabilities to quickly remediate threats.

How Ivanti Solutions Map to NIST CSF 2.0

This table shows how Ivanti's five integrated solutions align with the six core functions of CSF 2.0.

Ivanti Solution and NIST CSF Function	Govern (GV)	Identify (ID)	Protect (PR)	Detect (DE)	Respond (RS)	Recover (RC)
Enterprise Service Management (ESM)	GV.OC-01, GV.OC-02, GV.OC-03, GV.OC-04, GV.OC-05; GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07, GV.SC-02, GV.SC-03, GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-08, GV.SC-09	ID.AM-01, ID.AM-02, ID.RA-03, ID.RA-04, ID.IM-01, ID.IM-02, ID.OM-03, ID.IM-04	PR.DS-09, PR.PS-01, PR.PS-02	DE.CM-02, DE.COM-03, DE.CM-06, DE.AE-06, DE.AE-08	RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05; RS.AN-03, RS.MA-06, RS.AN-08, RS.CO-02, RS.CO-03	RC.RP.-01, RC.RP-02, RC.RP.-04, RC.RP-05, RC.RP.-06, RC.RP-03, RC.CO-04

Ivanti Solution and NIST CSF Function	Govern (GV)	Identify (ID)	Protect (PR)	Detect (DE)	Respond (RS)	Recover (RC)
Secure Unified Endpoint Management (SUEM)		ID.AM-01, ID.AM-02, ID.AM-05	PR.AA-01, PR.AA-03, PR.AA-04, PR.DS-01, PR.DS-02, PR.PS-01, PR.PS-02, PR.PS-05. PR.PS-06, PR-IR-01	DE.CM-02, DE.COM-03, DE.CM-06, DE.AE-06, DE.AE-08	RS.MI-01	
Vulnerability Management & Response (VMR)	G.V.RM-01, CV.RM-02, CV.RM-03, CV.RM-04, CV.RM-05, CV.RM-06,	ID.AM-01, ID.AM-02, ID.AM-05, ID.RA-01, ID.RA-02, ID.RA-04, ID.RA-05, ID.RA-06,		DE.AE-07	RS.MI-01, RS.MI-02	
Zero Trust Network Acess (ZTNA)		ID.AM-01, ID.AM-10	PR.AA-01, PR.AA-03 PR.AA-04, PR.AA-05 PR.AA-02, PR.AA-10 PR.IR-01	DE.CM-01, DE.COM-03	RS.MI-01	
Cyber Asset Attack Surface Management (CAASM)		ID.AM-01, ID.AM-02, ID.AM-05			RS.MI-01, RS.MI-02	

These solutions offer **a comprehensive, unified approach to cybersecurity**, addressing the core Functions, Categories and Subcategories within CSF 2.0. With them, organizations can effectively and efficiently secure their critical systems, applications and data.

Ivanti always recommends a **multilayered defense-in-depth cybersecurity strategy** to mitigate today's threats. Simply, the solution is to place as many impediments as possible in front of cybercriminals, increasing the chance that they will give up.

Ivanti-to-CSF 2.0 Mapping Details

In-depth descriptions of how Ivanti solutions align with NIST CSF 2.0.

Govern

Establish and monitor the organization's cybersecurity risk management strategy, expectations and policy.

Organizational Context (GV.OC):

The circumstances — mission, stakeholder expectations and legal, regulatory and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE).

ESM

With **Ivanti Neurons for IT Service Management** and/or **Ivanti Neurons for Security Operations Management**, security incidents occurring within your organization such as theft, data breach, phishing and policy violations can be addressed in a structured manner with automated workflows. They also help employees easily report security incidents and request security services.

Ivanti Neurons for Governance, Risk and Compliance enables your organization to automate tracking and compliance by centralizing all authority documents and frameworks, citations, controls and risks into a single system. Authority documents can be used to share your organization's policies and standards for cybersecurity risk management decisions; identify internal and external stakeholders; determine a process to track and manage legal and regulatory requirements regarding protection of an individual's private data (HIPAA [Health Insurance Portability and Accountability], CCPA [California Consumer Privacy Act] and GDPR [General Data Privacy Regulations], etc.) and ensure that critical objectives,

capabilities and services from your organization are determined and communicated in terms all stakeholders can understand. (GV.OC-01, GV. OC-02, GV.OC-03, GV.OC-04, GV.OC-05)

Risk Management Strategy (GV.RM):

The organization's priorities, constraints, risk tolerance and appetite statements and assumptions are established, communicated and used to support operational risk decisions (formerly ID.RM).

ESM and VM&R

Ivanti Neurons for Governance, Risk and Compliance., **Ivanti Neurons for Security Operations Management** and/or I**vanti Neurons for Risk-Based Vulnerability Management (RBVM)** can all be used to:

- Establish and manage risk management objectives
- Establish a standardized method for calculating, documenting, categorizing and prioritizing cybersecurity risks
- Determine, maintain and communicate risk appetite and risk tolerance, including positive risks, along with strategic direction with appropriate risk response options
- Process cybersecurity risk management activities, outcomes and lines of communication across your organization, including risks from internal and external suppliers

(GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07)

Cybersecurity Supply Chain Risk Management (GV.SC):

Cyber supply chain risk management processes are identified, established, managed, monitored and improved by organizational stakeholders (formerly ID.SC).

VM&R

Ivanti Neurons for Risk-Based Vulnerability Management and **Ivanti Neurons for Application Security Orchestration and Correlation** can be used to establish a risk-based vulnerability management approach to improve your organization's cybersecurity risk management strategy in a supply chain process. These offerings continuously correlate an organization's infrastructure (RBVM) and applications (ASOC) with vulnerability data, threat intelligence, manual pen test and research-based findings, and business asset criticality to measure risk and prioritize remediation activities. (GV.SC-01)

ESM

Ivanti Neurons for IT Asset Management with **Service Mapping** consolidates your IT asset data and lets you identify, prioritize and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process. It also lets you understand how assets are connected to better identify upstream/downstream risk. It can track, configure, optimize and strategically manage your internal supply chain assets throughout their full lifecycle. Further, Ivanti Neurons for GRC enhances the vendor onboarding process by performing Risk Assessments of new vendors prior to them being approved, maintaining controls associated with vendors and continuously assessing risks. (GV.SC-02, GV.SC-03, GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10)

Roles, Responsibilities and Authorities (GV.RR):

Cybersecurity roles, responsibilities and authorities to foster accountability, performance assessment and continuous improvement are established and communicated (formerly ID.GV-02).

ESM

Ivanti Neurons for Governance, Risk and Compliance. fulfills the subcategories listed below. Within the product, the out-of-the-box GRC Manager role can set up Control frameworks, Policies and Audits, and the GRC Analyst role facilitates completion of Control and Compliance activities and gathers evidence for Audits. Both roles can designate roles, responsibilities and authority, and who has permission to manage incidents, including human resources practices, to other teams and team members. Both roles can also keep track of response plans and approvals executed during or after an event.

Ivanti Neurons for Security Operations Management also fulfills the subcategories listed below by allowing users to define the roles they require within the platform and providing the flexibility to add, remove and designate as needed. (GV.RR-01, GV.RR-02, GV.RR-03, GV.RR-04)

Policies, Processes and Procedures (GV.PO):

Organizational cybersecurity policies, processes and procedures are established, communicated and enforced (formerly ID.GV-01)

ESM

Ivanti Neurons for IT Service Management facilitates documentation and ticketing of configuration change control processes. **Ivanti Neurons for Security Operations Management** keeps track of response plans and approvals executed during or after an event. It can also designate teams and team members to manage incidents. Also, with **Ivanti Neurons for IT Service Management** and **Ivanti Neurons for GRC** combined, security policies can be created, submitted for approval and reviewed. They can also enforce Policies by implementing Controls and monitoring compliance against the policies. (GV.PO-01, GV.PO-02)

VM&R

Ivanti Neurons for Risk-Based Vulnerability Management and **Ivanti Neurons for App Security Orchestration & Correlation (ASOC)** provide the tools to manage and implement a vulnerability response plan, including automated tasks using service-level agreements (SLAs). **Ivanti Neurons for Risk-Based Vulnerability Management** also facilitates end-to-end vulnerability identification, assessment and prioritization to patch remediation through direct integration with **Ivanti Neurons for Patch Management.** (GV.PO-02)

Oversight (GV.OV):

Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve and adjust the risk management strategy.

ESM

Ivanti Neurons for Security Operations Management feature keeps track of response plans and approvals executed during or after an event. It can also designate which teams and team members will manage incidents. Integrations with Atlassian Jira and Microsoft Azure DevOps can route code-related security incidents to software development teams working with these tools to synchronize with **Ivanti Neurons for IT Service Management** for status, comments, attachments, etc. This enables a unified platform to report on your organizational cybersecurity and risk management.

Ivanti Neurons for IT Service Management can record contacts for incidents, including who logged the record and who needs to be notified regarding updates. It can track and manage process documentation with approvals and review timeframes, and can manage roles and responsibilities related to the incident management process. It can also record communication mechanisms and set priority on these incidents, and it differentiates incidents from events as different record types. Security incidents can be categorized as malware, data breach, phishing, vulnerability and more. (GV.OV-01, GV.OV-02, GV.OV-03)

Identify

Help determine the current cybersecurity risk to the organization.

Asset Management (ID.AM):

Assets (e.g., data, hardware, software, systems, facilities, services, people) 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.

SUEM

Ivanti Neurons for Discovery provides accurate real-time inventories of all your IT assets — including all hardware, software, systems, data, services and people — and their management and maintenance. All assets are tracked and prioritized based on classification, criticality, resources and impact on your organization. (ID.AM-01, ID.AM-02, ID.AM-05)

Ivanti Neurons for Unified Endpoint Management manages an inventory of all registered mobile devices, desktop clients and all installed software, operating systems and applications. The solution also ensures all mobile devices and clients are always under management and enforces compliance with your company's security and privacy policies. These managed devices and their content are classified by criticality and business value. (ID.AM-01, ID.AM-02)

Ivanti Neurons for Spend Intelligence delivers insights into your software landscape and application asset inventory with instant visibility into software usage, software configuration drift and software end-of-life. (ID-AM-02)

ESM

Ivanti Neurons for IT Asset Management with **Service Mapping** using Audit Assets, Control and Policy maintains accurate inventory and actionable insights of hardware, server, client, virtual, cloud or software assets throughout their entire lifecycle. (ID. AM-01, ID.AM-02)

Risk Assessment (ID.RA):

The organization understands the cybersecurity risk to the organization, assets and individuals.

VM&R

Ivanti Neurons for Risk-Based Vulnerability Management and **Ivanti Neurons for Application Security Orchestration & Correlation** deliver automated insights into your organization's risk exposure by providing remediation prioritization based on adversarial risk. These products identify and document asset weaknesses and vulnerabilities. Threat and vulnerability information is received from information-sharing forums and crowdsources. Potential business impacts and trends are also identified whereby threats, vulnerabilities, trends, asset criticality and internal or external accessibility are used to determine risk, and appropriate responses are identified and prioritized for automated remediation. (ID.RA-01, ID.RA-02, ID.RA-04, ID-RA-05, ID-RA-06)

Ivanti Neurons for Patch Management scans all endpoints for vulnerabilities and exposures by identifying and correlating missing software updates to CVEs (Common Vulnerabilities and Exposures) and Ivanti's vulnerability knowledge base. This allows organizations to implement a risk-based approach to their enterprise patching strategy. (ID.RA-01)

ESM

Ivanti Neurons for Governance, Risk and Compliance identifies and documents internal and external threats, their risk assessment, potential business impacts and likelihoods. (ID.RA-03, ID.RA-04)

Improvement (ID.IM):

Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all Framework Functions.

ESM

Ivanti Neurons for Governance, Risk and Compliance using policies, audit and indicators can be used to document and track risk management processes, procedures and activities for continuous evaluation to identify improvements, including lessons learned for future incident response activities. Specifically, **Ivanti Neurons for Governance, Risk and Compliance.** can monitor controls with compliance indicators and control tests to identify improvements and continuously monitor the effectiveness of your organization's compliance activities. Also, cybersecurity plans that affect operations are communicated, maintained and improved. (ID.IM-01, ID.IM-02, ID.OM-03, ID.IM-04)

Protect

Use safeguards to prevent or reduce cybersecurity risk.

Identity Management, Authentication and Access Control (PR.AA):

Access to physical and logical assets is limited to authorized users, services and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC).

SUEM

Ivanti Neurons for Unified Endpoint Management with **Ivanti Access** integrates with your existing identity provider (IdP) and can enforce conditional access based on trusted user, device, application, network and context rules, while **Ivanti Zero Sign-On** manages the issuance, verification, revocation, monitoring and auditing of identities and credentials for authorized users, devices and services. All identity assertions used for single sign-on (SSO) and between federated systems are protected, conveyed and verified. (PR.AA-01, PR.AA-03, PR.AA-04)

ZTNA

Ivanti Neurons for Zero Trust Access manages and provides secure remote access to on-premises, data centers and cloud (SaaS-based) resources. Authorized users, devices, applications, networks, services and context are authenticated by implementing multi-factor authentication (MFA) while using the stronger and adaptive factors. Access permissions, entitlements and authorizations are defined in a policy, managed, reviewed and enforced using least privilege and user role and duties. (PR.AA-01, PR.AA-03, PR.AA-04, PR.AA-05)

Also, **Ivanti Network Access Control** can enforce micro-segmentation, ensuring network integrity for not only north-south but also east-west network data traffic. (PR.AA-05)

Awareness and Training (PR.AT):

The organization's personnel are provided cybersecurity awareness and training so they can perform their cybersecurity-related tasks. Ivanti does not offer a solution in this regard.

Data Security (PR.DS): Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity and availability of information. Ivanti does not offer a solution in this regard.

SUEM

Ivanti Neurons for Unified Endpoint Management can enable, check and enforce file-based encryption on iOS, iPadOS and Android mobile devices and full-disk encryption using BitLocker for Windows and FileVault for macOS clients to protect the confidentiality, integrity and availability of data at rest and data in use. It can also enable WPA3-Personal (Simultaneous Authentication of Equals) and Enterprise for wireless networks. **Ivanti Tunnel** supplies an on-demand, always-on and per-app VPN (Virtual Private Network) from client to gateway for protection of using Transport Layer Security (TLS) 1.2 cipher suites. (PR. DS-01, PR.DS-02)

ZTNA

Ivanti Neurons for Zero Trust Access implements the strong cryptographic cipher suites with Transport Layer Security version 1.3 to protect data in transit and data in use, along with enforcing user behavior, analytics and risk, multi-factor and adaptive authentication and authorization, device posture, trusted application and access context (location and time) controls. Integration with Lookout Cloud Access Security Broker (CASB) and Secure Web Gateway (SWG) solutions, specifically the API controls deployment, helps with insider threats and data leakage. (PR.DS-02, PR.DS-10)

Also, **Ivanti Neurons for Zero Trust Access** arbitrates micro-segmentation of the customer's development and testing environments separate from the production environment by enforcing user and application least privileges. (PR-DS-02)

ESM

Ivanti Neurons for IT Asset Management and **ITSM: Ivanti Neurons for IT Service Management** formally manage digital assets throughout their lifecycle from removal, transfers and disposition and track systems with sensitive data. (PR.DS-09)

Platform Security (PR.PS):

The hardware, software (e.g., firmware, operating systems, applications) and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect its confidentiality, integrity and availability.

ESM and SUEM

Ivanti Neurons for IT Service Management with **Ivanti Neurons for Healing** delivers approved and controlled tools to ensure configuration management practices are applied and software is maintained, replaced and removed in accordance with risk and audited and performed in a timely manner. (PR.PS-01, PR.PS-02)

Ivanti Neurons for Modern Device Management with **Ivanti Neurons for Mobile Threat Defense** can prevent the installation and execution of unauthorized software on your organizational assets and block access to known malicious domains using secure DNS (phishing and content protection). (PR.PS-05)

The Software Distribution capability of **Ivanti Neurons** uses secure hashing algorithms to maintain software used in production environments and securely dispose of software once it is no longer needed. (PR.PS-06)

Technology Infrastructure Resilience (PR.IR):

Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, availability and organizational resilience.

ZTNA

Ivanti Neurons for Zero Trust Access incorporates the principle of least functionality and micro-segmentation by configuring networks, environments and systems to supply only essential permissions and capabilities for end users. (PR.IR-01)

Ivanti Neurons for Unified Endpoint Management can protect communications and control networks. (PR.IR-01)

And **Ivanti Virtual Application Delivery Controller** supplies network failsafe mechanisms for load balancing and hot swapping to achieve resilience requirements in normal and adverse situations. (PR.IR-01)

SUEM

Ivanti Neurons for Unified Endpoint Management protects networks and environments from unauthorized logical access and usage by logically segmenting the internal corporate network from external networks and permitting only necessary communications to enter the corporate network from the external networks. (PR.IR.01)

Detect

Find and analyze possible cybersecurity attacks and compromises.

Continuous Monitoring (DE.CM):

Assets are monitored to find anomalies, indicators of compromise and other potentially adverse events.

ZTNA

Ivanti Neurons for Zero Trust Access with Lookout **Security Service Edge** uses the web to create a secure connection from the device to an application through gateways while constantly verifying the user, the device, applications, time of day and source geolocation based on granular constraints to detect and record authorized access events. Networks, network services, personnel activity and technology usage are all checked for potentially adverse events. (DE.CM-01, DE.CM-03)

SUEM

Ivanti Neurons for Modern Device Management with **Ivanti Neurons for Mobile Threat Defense** can monitor email, web, file sharing and collaborative services to detect malware, phishing, data leaks and exfiltration, monitor software configuration drift from security baselines, and detect malware infections and unauthorized software on managed corporate endpoints. **Ivanti Neurons for Patch Management** can detect missing patches on corporate endpoints.
(DE.CM-09)

ESM

Recurring checks are a feature of **Ivanti Neurons for Governance, Risk and Compliance** that allow you to schedule

periodic audits or assessments for your compliance controls. You can define the frequency, scope and assignee of the recurring checks and track their progress and results in the Audit Calendar. Recurring checks help you ensure that your controls are always up to date and effective. This can be used to monitor and find potentially adverse events found in physical environments, personnel activity and external service provider activities. (DE.CM-02, DE.CM-03, DE.CM-06)

Adverse Event Analysis (DE.AE):

Anomalies, indicators of compromise and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents (formerly DE.AE, DE.DP-02).

ESM

Ivanti Neurons for IT Service Management holds information on adverse events and is provided to authorized staff and tools. Incidents are declared when adverse events meet the defined incident criteria. (DE.AE-06, DE.AE-08)

VM&R

Ivanti Neurons for Risk-Based Vulnerability Management, Ivanti Neurons for Application Security Orchestration and Correlation and **Ivanti Neurons for Vulnerability Knowledge Base** supply cyberthreat intelligence on both vulnerabilities (CVE) and software weaknesses (CWE) plus other contextual information that can be integrated into the response and remediation analysis. (DE.AE-07)

Respond

Take action regarding a detected cybersecurity incident.

Incident Management (RS.MA):

Responses to detected cybersecurity incidents are managed (formerly RS.RP).

ESM

Ivanti Neurons Security Operations Management keeps track of response plans and approvals executed during or after an event. It can also designate which teams and team members will manage incidents.

Ivanti Neurons for IT Service Management can record contacts for incidents, including who logged the record and who needs to be notified regarding updates. It can track and manage process documentation with approvals and review timeframes, and can manage roles and responsibilities related to the incident-management process. It can also record communication mechanisms and set priority on these incidents, and it differentiates incidents from events as different record types. Security incidents can be categorized as malware, data breach, phishing, vulnerability and more. (RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05)

Incident Analysis (RS.AN):

Investigation is conducted to ensure effective response and support forensics and recovery activities.

ESM

Ivanti Neurons for Security Operations Management keeps track of effective response plans, including forensics and recovery activities and approvals executed during or after an event. (RS.AN-03, RS.AN-06, RS.AN-08)

Incident Response Reporting and Communications (RS.CO):

Response activities are coordinated with internal and external stakeholders as required by laws, regulations or policies.

ESM

Ivanti Neurons for Security Operations Management feature keeps track of response plans, including coordinating internal and external communications required by policies, laws and regulations and approvals executed during or after an event. (RS.CO-02, RS.CO-03)

Incident Mitigation (RS.MI):

Activities are performed to prevent expansion of an event and mitigate its effects.

VM&R

Ivanti Neurons for Risk-Based Vulnerability Management is an adaptive risk-based vulnerability management product. With this product, your organization needs only minutes to know and manage the actions that will shut down exposure across its attack surface. The administrator will know what actions to take in seconds and can accelerate remediation activities for the most important vulnerability exposure points across your attack surface, infrastructure, applications and development frameworks. Threats and incidents can then be eradicated with the integration of **Ivanti Neurons for Patch Management.** (RS.MI-01, RS.MI-02)

ZTNA and SUEM

Ivanti Neurons for Zero Trust Access and **Ivanti Access** integrated with **Ivanti Neurons for Mobile Threat Defense** can contain incidents using device isolation and blocking access to corporate applications and data if a threat is detected on a corporate device. (RS.MI-01)

Recover

Restore assets and operations affected by a cybersecurity incident.

Incident Recovery Plan Execution (RC.RP):

Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents.

ESM

Ivanti Neurons for IT Service Management and/or **Ivanti Neurons for Security Operations Management** using Security Incidents can be used to initiate the incident response process and allocate the required recovery actions and checklists to appropriate teams and individuals, including critical functions and cybersecurity risk management considerations. Assets and systems can be identified using the CMDB (configuration management database) and related to the security incident, and notifications across stakeholders can be automated from within the security incident. At completion of the restoration, follow-up documentation and learnings can be recorded against the security incident. (RC.RP-01, RC.RP-02, RC.RP-04, RC.RP-05, RC.RP-06)

Incident Recovery Communications (RC.CO):

Restoration activities are coordinated with internal and external parties.

ESM

Ivanti Neurons for IT Service Management using Security Incidents tasks, Security Announcements and Security Knowledge Base capabilities can be configured for cybersecurity announcements — including recovery activities and progress in restoring operational capabilities to internal and external stakeholders — which will be displayed in the Self-Service portal. Public updates on incident recovery are properly shared using approved methods and messaging. Automated notifications from within the security incidents can ensure that appropriate stakeholders are notified. (RC.CO-03, RC.CO-04)

About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com

ivanti

For more information, or to contact Ivanti, please visit ivanti.com.

1. Cybersecurity Framework | NIST. (2023, November 16). NIST. https://www.nist.gov/cyberframework
2. NIST releases releases version 2.0 of landmark cybersecurity framework: https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework