Qualys.

WHITEPAPER

Achieving NIST CSF 2.0 Adaptive Tier 4 Maturity

Contents

The National Institute of Standards and Technology (NIST) recently updated its popular Cybersecurity Framework (CSF) to version 2.0 to help organizations reduce cybersecurity risks. Designed for virtually all industry sectors from small to medium businesses (SMBs) through larger enterprises, NIST CSF v2.0 represents the first major update in more than a decade.

NIST released CSF v 1.0 in 2014 at the direction of a presidential executive order, with an emphasis on critical infrastructure, to help all firms reduce risks for security breaches. CSF 2.0 expands upon the existing five basic functions for Identify, Protect, Detect, Respond, and Recover and now includes a sixth function called Govern. NIST CSF 2.0 also more fully addresses supply chain risks.

The CSF 2.0 expanded scope goes well beyond protecting critical infrastructure, such as hospitals and power plants, and encompasses almost any organization at risk for cyberattacks. The new Govern function focuses on making and carrying out informed decisions on cybersecurity strategy. This component now emphasizes cybersecurity as a major risk factor that executives should prioritize as it can impact finances, litigation, and brand damage.

NIST CSF 2.0 Overview

In an era of rapidly evolving cyber threats, organizations across industries and geographies face the critical challenge of managing cybersecurity risks. The NIST CSF 2.0 has emerged as a comprehensive and widely adopted solution, enabling businesses of all sizes to assess, manage, and mitigate cyber risks effectively.

The NIST CSF's proven success in aiding risk management and reduction has led to its widespread adoption and incorporation into national risk frameworks worldwide. Some industries have even taken the step of mandating its implementation, recognizing the framework’s critical role in fortifying cybersecurity defenses. In May 2017, the White House issued an executive order requiring all federal agencies to immediately adopt the NIST CSF for protecting critical infrastructure within their enterprises. This mandate highlights the U.S. government's confidence in the framework’s ability to enhance cybersecurity risk management across federal agencies.

One of the key strengths of the NIST CSF lies in its ability to facilitate open and productive dialogue among internal and external stakeholders. By providing a common language that spans IT, operations, security, finance, the C-suite, and boards of directors, the framework promotes effective communication and collaboration. This open dialogue empowers organizations to accurately quantify risks and strategically prioritize investments, ensuring optimal allocation of resources for risk mitigation. For IT, security, and Governance/Risk/Compliance (GRC) teams, leveraging the NIST CSF 2.0 can significantly enhance your organization's cybersecurity posture and maturity level. By aligning risk management strategies with this globally recognized framework, you can:

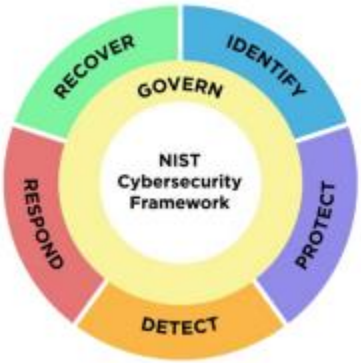
- Identify and prioritize critical assets and vulnerabilities
- Implement robust security controls and best practices
- Continuously monitor and improve cybersecurity maturity
- Comply with industry regulations and standards
- Communicate effectively with stakeholders and secure buy-in for cybersecurity initiatives

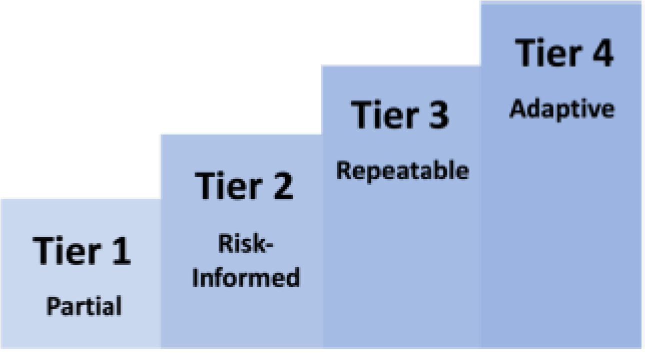
As cyber threats continue to evolve, organizations must adopt proactive and comprehensive approaches to manage cybersecurity risks. The NIST CSF 2.0 provides a powerful tool for Chief Information Officers CIOs) and Chief Information Security Officers (CISOs) and other stakeholders in an organization to assess, manage, and mitigate these risks effectively. By embracing the framework and aligning risk management strategies with NIST guidelines, organizations can strengthen their cybersecurity defenses, ensure compliance with industry standards, and foster a culture of continuous improvement in cybersecurity practices.

To unlock the full potential of the NIST CSF 2.0 and transform cybersecurity risk management within your organization, it is essential to engage with cybersecurity experts who can provide personalized guidance and support throughout the implementation process. Also, to implement industry best practices and to meet all the requirements.

NIST CSF 2.0 Maturity

Many businesses, both in the U.S. and other countries, underscore their Written Information Security Plan (WISP) with the NIST CSF. NIST now prescribes four levels of maturity, or tiers, that characterize the rigor of the firm's cybersecurity risk governance and management practices. They essentially provide context for how an organization views cybersecurity risks and its processes for managing those risks. The four tiers are Partial, Risk Informed, Repeatable, and Adaptive. NIST recommends that all firms should strive for the Adaptive top tier. To achieve this requires the implementation the most effective cybersecurity solutions.





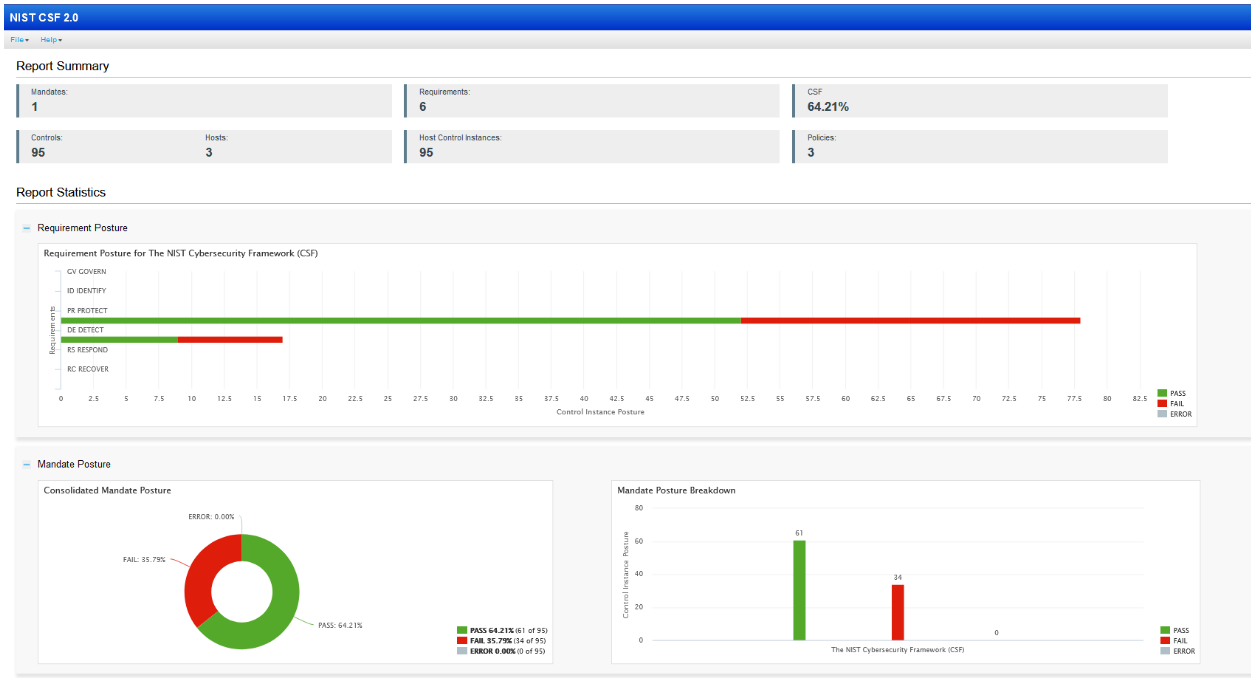
How Qualys Can Help

GOVERN (GV)

This is where your organization's cybersecurity risk management strategy, expectations, and policies are established, communicated, and monitored. This function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five functions in the context of its mission and stakeholder expectations. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

Qualys Policy Compliance (PC) offers a comprehensive NIST CSF 2.0 dashboard with details that outline your posture across all six functions including mandates, requirements, pass/fail status, and more. Executives can view their overall posture to ensure they are meeting the GOVERN requirements adequately and make adjustments to ensure proper risk management strategy. With Qualys PC, you can go beyond vulnerability management (VM) and security configuration assessment (SCA) to reduce security breach and compliance risks with a single cloud solution, multiple sensors, robust policy library, and seamless integration.

The Qualys PC app includes support for 1,000 policies, 22,000 controls, 400 technologies, and 100 regulations. This app can also dramatically improve an organization's security posture by increasing MITRE ATT&CK coverage and overall security postures by up to 79 percent over vulnerability management alone. Gartner says that 99 percent of cloud security breaches are related to mistakes and misconfigurations. Qualys PC allows you to find, prioritize, and automatically remediate misconfigurations that are missed by most other solutions. The app now integrates with Qualys Endpoint Detection and Response (EDR) to automatically remediate threats discovered by the EDR app. Qualys PC can ensure compliance with numerous mandates such as PCI DSS 4.0, GDPR, PSD2, CCPA, HIPAA 2023, FINRA, ISO, and many others.



Report Summary

Mandates: 1
Requirements: 6
CSF 64.21%
Controls: 95
Hosts: 3
Host Control Instances: 95
Policies: 3

Report Statistics

IDENTIFY (ID)

This addresses how your current cybersecurity risks are understood. Gaining an understanding of your assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks can help you prioritize efforts consistent with your risk management strategy and the mission needs identified under GOVERN.

As this function includes asset management, risk assessments, and improvements to ensure compliance, the Qualys CyberSecurity Asset Management (CSAM) app addresses requirements for asset management, and the Qualys Vulnerability Management Detection and Response (VMDR) app tackles requirements for risk assessment.

Qualys CSAM allows you to create a unified asset inventory with cyber risk and business context to turbocharge vulnerability management and remediation. With CSAM, you can improve asset coverage by 30 percent to turbocharge vulnerability management, proactively manage End of Life or Service by up to twelve months in advance to avoid unpatchable vulnerabilities, and map remediation tickets with 96 percent accuracy with bi-directional CMDB sync to unify IT and security teams.

Qualys VMDR continuously measures known and unknown risks, prioritizes and communicates risks across vulnerabilities, and allows you to patch any device anywhere to remediate, mitigate, and block the attack paths to eliminate risks. With VMDR, you can measure risks six times faster than with competitive VM platforms, communicate risks from over 200,000 vulnerabilities sourced from more than twenty-five threat intelligence feeds, and eliminate critical risks 60 percent faster with a one-click workflow and ITSM integrations.

Peter Drucker once said that “you can’t improve what you don’t measure.” Using CSAM and VMDR to ensure visibility and measure risks can help you cover the improvement requirements for this function.

Qualys TotalCloud offers a unified dashboard for managing cybersecurity across hybrid IT environments. This centralized visibility and control aligns with NIST Identify requirements for effective cybersecurity governance and risk management.

PROTECT (PR)

This function addresses safeguards used to manage the organization’s cybersecurity risks and how they are used. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities.

Outcomes covered by this function include identity management, authentication, and access control; awareness and training; data security; platform security, and the resilience of technology infrastructure.

Qualys CSAM and PC can ensure you’re covered for platform security by providing visibility, reporting, dashboards, and remediation so you can attain a top tier Adaptive NIST CSF 2.0 status.

Qualys TotalCloud can protect cloud infrastructure & SaaS apps up to 85 percent faster with a unified, prioritized view of risks.

DETECT (DE)

This function is designed to ensure you can find and analyze possible cybersecurity attacks and compromises. It enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This function supports successful incident response and recovery activities.

Qualys Endpoint Security solutions, including EDR and Extended Detection and Response (XDR), can help you stay covered for this function. Qualys Endpoint Security employs a multi-layered defense to protect your organization’s devices—such as laptops, desktops, and servers—from sophisticated cyber threats, including ransomware, phishing, data theft, and more. As noted earlier, Qualys EDR integrates seamlessly with Qualys PC to automatically remediate threats and misconfigurations, which helps you comply with the RESPOND function.

For continuous monitoring, Qualys File Integrity Monitoring (FIM) can be a critical app. Qualys FIM is a scalable cloud app that enables monitoring for critical files, directories, and registry paths for changes in real time, and helps adhere to compliance mandates such as PCI-DSS 4.0, CCPA, GDPR and others. Unique noise cancellation reduces false alerts by 90%+ to help mitigate audit failures for ignoring low level alerts. Qualys FIM includes support for non-agent network devices to alert on network configuration deviations, offering enhanced visibility for effective monitoring and response. Also, File Access Monitoring (FAM) to trigger alerts when critical host files, not intended for regular use, are accessed.

Qualys TotalCloud measures risk with 360-degree scanning to detect vulnerabilities, detect malware with up to 99 percent accuracy thanks to AI-powered deep learning threat detection.

RESPOND (RS)

This is about actions taken regarding a detected cybersecurity incident. It covers support for the ability to contain the effects of cybersecurity incidents. Outcomes within this function include incident management, analysis, mitigation, reporting, and communication.

Qualys Endpoint Protection solutions, as noted earlier, can help your analysts stay on top of incident analysis while mitigating false positive alerts that require additional IT support tickets and analyst triage. This can greatly reduce costs and efforts related to supporting this function.

As we discussed previously, Qualys PC helps ensure timely and automated incident management and incident mitigation, which will also reduce costs and efforts that can overrun resource-constrained teams.

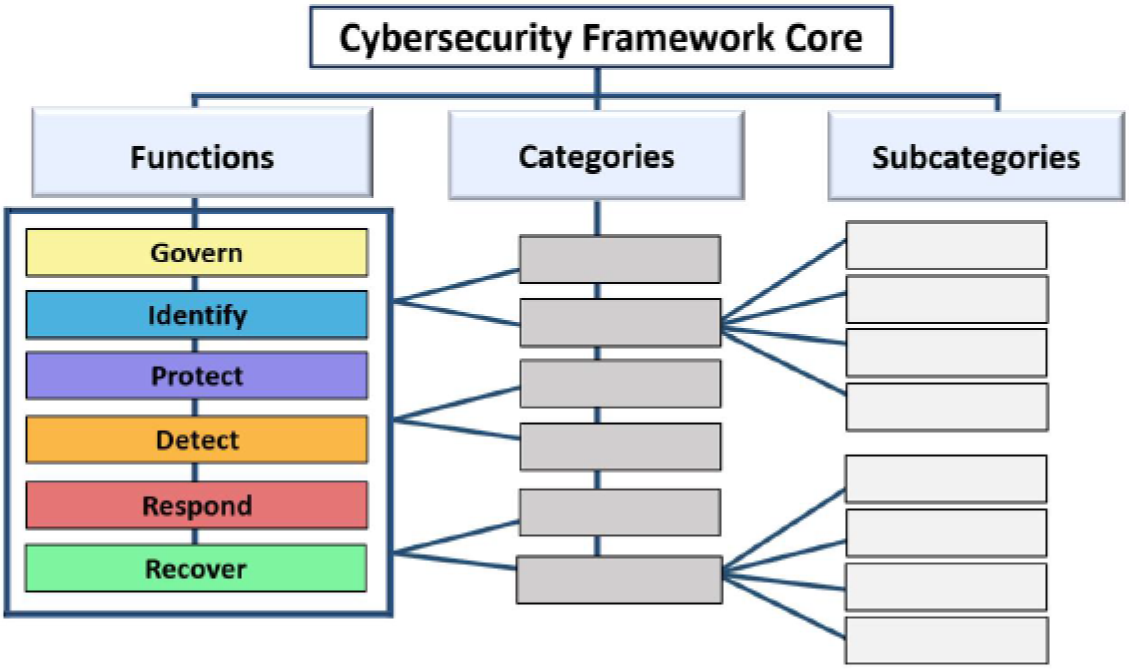
RECOVER (RC)

This function focuses on assets and operations affected by a cybersecurity incident and how they are restored. It’s all about supporting the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

Recovery is all about resilience, and not just executing your plan but doing so in a timely and efficient manner. Using Qualys Endpoint Protection and PC solutions to RESPOND can go a long way toward ensuring fast and effective recovery by automating manual processes that can result in mistakes and delays.

The Qualys Security Assessment Questionnaire (SAQ) app is a transformative cloud service used to conduct business process control assessments among your external and internal parties. SAQ addresses self-assessments required across all six functions.

Mapping Qualys Apps to NIST CSF 2.0



NIST CSF 2.0 Category	Subcategory	Qualys Solutions	Qualys Apps
GOVERN			
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	GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders. Examples: Establish measurable objectives for cybersecurity risk management. Senior leaders agree about cybersecurity objectives and use them for measuring and managing risk and performance.	The Qualys Enterprise TruRisk™ Platform, including the Qualys Vulnerability Management, Detection & Response (VMDR) app, allows you to calculate the known and unknown cyber risk across your internal and external attack surface and quantify it in a way that meets the unique demands of your business. The Qualys Self Assessment Questionnaire (SAQ) is recommended for all subcategories.	The Qualys Enterprise TruRisk™ Platform apps Qualys VMDR
	GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained. Examples: Determine and communicate risk appetite statements that convey expectations about the appropriate level of risk for the organization. Translate risk appetite statements into specific, measurable, and broadly understandable risk tolerance statements. Refine organizational objectives and risk appetite	TruRisk is the industry standard on how to apply risk-based prioritization to your cyber security program. While EPSS and CVSS are foundational metrics for severity, they can miss real threats and fail to filter out non-critical risk without complete business context of the environment. TruRisk aggregates ALL risk-factors from 73,000 vulnerability signatures, 25+ sources of threat intel, and integrations with third-party solutions.	The Qualys Enterprise TruRisk™ Platform apps

	periodically based on known risk exposure and residual risk.		
	GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes. Example: Establish criteria for escalating cybersecurity risks within enterprise risk management.	The Qualys Enterprise TruRisk™ Platform provides risk management and management process dashboard and reports to help with this requirement.	The Qualys Enterprise TruRisk™ Platform apps
	GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated. Example: Specify criteria for accepting and avoiding cybersecurity risk for various classifications of data.	The Qualys Enterprise TruRisk™ Platform allows you to go beyond just enumerating your cyber risk with the ability to clearly define it and articulate your complete cyber risk posture throughout your organization.	The Qualys Enterprise TruRisk™ Platform apps
	GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated. Examples: Establish criteria for using a quantitative approach to cybersecurity risk analysis, and specify probability and exposure formulas. Create and use templates (e.g., a risk register) to document cybersecurity risk information (e.g., risk description, exposure, treatment, and ownership). Establish criteria for risk prioritization at the appropriate levels within the enterprise. Use a consistent list of risk categories to support integrating, aggregating, and comparing cybersecurity risks.	The Qualys Enterprise TruRisk™ Platform allows for documenting, categorizing and prioritizing cybersecurity risks, and reports and dashboards ensure proper communication.	The Qualys Enterprise TruRisk™ Platform apps
	GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions. Example: Calculate, document, and prioritize positive risks alongside negative risks.	The Qualys Enterprise TruRisk™ Platform helps ensure opportunities for risk discussions are based on TruRisk to the organization.	The Qualys Enterprise TruRisk™ Platform apps
Policy (GV.PO): Organizational cybersecurity policy is established,	GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and	The Qualys Enterprise TruRisk™ Platform provides dynamic CISO dashboards that capture TruRisk across your entire environment.	The Qualys Enterprise TruRisk™ Platform apps

communicated, and enforced	priorities and is communicated and enforced. Example: Communicate cybersecurity risk management policy and supporting processes and procedures across the organization.		
	GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission. Examples: Update policy based on periodic reviews of cybersecurity risk management results to ensure that policy and supporting processes and procedures adequately maintain risk at an acceptable level. Provide a timeline for reviewing changes to the organization's risk environment (e.g., changes in risk or in the organization's mission objectives), and communicate recommended policy updates. Update policy to reflect changes in technology (e.g., adoption of artificial intelligence) and changes to the business (e.g., acquisition of a new business, new contract requirements).	The Qualys Enterprise TruRisk™ Platform provide business unit and compliance reports that pinpoint the most critical risks to your business.	The Qualys Enterprise TruRisk™ Platform apps
Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy	GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed. Examples: Review key risk indicators (KRIs) to identify risks the organization faces, including likelihood and potential impact. Collect and communicate metrics on cybersecurity risk management with senior leadership.	The Qualys Enterprise TruRisk™ Platform lets you prioritize risk by overall business impact and remediate efficiently with risk-based patching, AI-powered adaptive mitigation, and an integrated workflow across teams.	The Qualys Enterprise TruRisk™ Platform apps Qualys VMDR
Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders	GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.	The Qualys Enterprise TruRisk™ Platform offers integrations with CMDB and third-party vendors to keep IT, security, and GRC teams in lockstep on the most critical priorities, including supply chain risk management.	The Qualys Enterprise TruRisk™ Platform apps Qualys VMDR

	Example: Establish a strategy that expresses the objectives of the cybersecurity supply chain risk management program.		
	GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes. Examples: Identify areas of alignment and overlap with cybersecurity and enterprise risk management. Establish integrated control sets for cybersecurity risk management and cybersecurity supply chain risk management.	The Qualys Enterprise TruRisk™ Platform covers you for supply chain risk management based on TruRisk.	The Qualys Enterprise TruRisk™ Platform apps
	GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship. Examples: Monitor critical suppliers to ensure that they are fulfilling their security obligations throughout the supplier relationship lifecycle using a variety of methods and techniques, such as inspections, audits, tests, or other forms of evaluation. Monitor critical suppliers, services, and products for changes to their risk profiles, and reevaluate supplier criticality and risk impact accordingly.	The Qualys Enterprise TruRisk™ Platform provides dynamic dashboards that capture TruRisk across your entire environment, including third-party risks.	The Qualys Enterprise TruRisk™ Platform apps
	GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle. Examples: Policies and procedures require provenance records for all acquired technology products and services. Periodically provide risk reporting to leaders about	The Qualys Enterprise TruRisk™ Platform helps you monitor TruRisk to the organization across supply chains throughout the technology product and service life cycle.	The Qualys Enterprise TruRisk™ Platform apps

	how acquired components are proven to be untampered and authentic. Communicate regularly among cybersecurity risk managers and operations personnel about the need to acquire software patches, updates, and upgrades only from authenticated and trustworthy software providers.		
IDENTIFY			
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	ID.AM-01: Inventories of hardware managed by the organization are maintained. Examples: Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices. Constantly monitor networks to detect new hardware and automatically update inventories.	With Qualys CyberSecurity Asset Management (CSAM), you can gain comprehensive and continuous visibility across cloud, multi-cloud, on-premises, and IT/OT attack surfaces – all within one unified inventory that includes External Attack Surface Management (EASM). With Qualys VMDR, you can automatically discover and categorize known and unknown assets, internal and internet-exposed assets, continuously identify unmanaged assets. Qualys Global Asset View (GAV) provides visibility into all global assets.	Qualys VMDR Qualys CSAM / EASM Qualys SAQ Qualys GAV
	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained. Examples: Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services. Constantly monitor all platforms, including containers and virtual machines, for software and service inventory changes. Maintain an inventory of the organization's systems.	With Qualys CSAM you can find unmanaged IoT/OT internal assets, internet-facing digital assets (from mergers, acquisitions, and subsidiaries), and add business context with third-party connectors. CSAM is the only solution that combines native scanning, agent, passive discovery, and complements with API-based third-party connectors to provide the most comprehensive asset attack surface coverage. Qualys Web Application Scanning (WAS) provides full visibility and control of every web app and API - approved, unapproved, unknown or forgotten - in your environment, either cloud-native or on-prem. Custom tag your web assets for targeted reporting.	Qualys VMDR Qualys CSAM / EASM Qualys SAQ Qualys GAV Qualys WAS
	ID.AM-04 Inventories of services provided by suppliers are maintained. Examples: Inventory all external services used by the organization, including	Qualys CSAM and Qualys GAV can help provide supplier inventory visibility.	Qualys CSAM Qualys GAV Qualys WAS

	third-party infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings; APIs; and other externally hosted application services. Update the inventory when a new external service is going to be utilized to ensure adequate cybersecurity risk management monitoring of the organization's use of that service.		
	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission. Examples: Define criteria for prioritizing each class of assets. Apply the prioritization criteria to assets. Track the asset priorities and update them periodically or when significant changes to the organization occur.	With Qualys CSAM you can go beyond vulnerabilities to measure the TruRisk of every asset in your environment by uncovering key asset data. Add risk factors such as EoL/EoS software, missing agents and security tools, unsanctioned ports, and expired SSL certs to TruRisk Scoring to prioritize and eliminate business risk. Qualys PC ensures you don't miss databases and middleware, and Qualys WAS lets you include web apps and API in your assets prioritization. Qualys TotalCloud (TC) provides a comprehensive inventory of public cloud resources with Cloud Workload Protection to prioritize assets, including Kubernetes/containers, based on TruRisks.	Qualys VMDR Qualys CSAM / EASM Qualys PC Qualys WAS Qualys TC Qualys SAQ Qualys GAV
	ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained.	With Qualys CSAM you can add missing assets to your CMDB and enrich assets (CIs) with cyber risk context such as EoL/EoS software, expired certificates, and missing agents. Qualys File Integrity Monitoring (FIM) ensure you include monitoring for data contained in files that might be compromised.	Qualys VMDR Qualys CSAM / EASM Qualys FIM Qualys SAQ
	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles. Examples: Integrate cybersecurity considerations throughout the life cycles of systems, hardware, software, and services. Integrate cybersecurity considerations into product life cycles. Identify unofficial uses of technology to meet	With Qualys CSAM you can close tickets up to 50% faster with complete and accurate assets with required context shared between IT and Security teams. With Qualys VMDR you can create automated workflows and manage them effectively so you always know about every active asset across your global hybrid-IT environment. Qualys FIM, PC, WAS, and TotalCloud are important to ensure you're	Qualys VMDR Qualys CSAM / EASM Qualys SAQ Qualys GAV

	mission objectives (i.e., shadow IT). Periodically identify redundant systems, hardware, software, and services that unnecessarily increase the organization's attack surface. Properly configure and secure systems, hardware, software, and services prior to their deployment in production. Update inventories when systems, hardware, software, and services are moved or transferred within the organization.	covering all software and data.	
Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded. Examples: Use vulnerability management technologies to identify unpatched and misconfigured software. Assess network and system architectures for design and implementation weaknesses that affect cybersecurity. Review, analyze, or test organization-developed software to identify design, coding, and default configuration vulnerabilities. Assess facilities that house critical computing assets for physical vulnerabilities and resilience issues. Monitor sources of cyber threat intelligence for information on new vulnerabilities in products and services. Review processes and procedures for weaknesses that could be exploited to affect cybersecurity	Qualys Vulnerability Management, Detection & Response software helps you measure known and unknown risks, prioritize and communicate risk across vulnerabilities, and patch any device anywhere. Qualys TotalCloud lets you de-risk your IaaS and SaaS environments with one prioritized view of risk and vulnerabilities. Qualys PC can ensure you don't miss databases and middleware, and Qualys WAS covers you for webapps. Qualys Threat Protection (TP) pinpoints the most critical threats and prioritizes patching.	Qualys VMDR Qualys TC Qualys PC Qualys WAS Qualys SAQ Qualys TP
	ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources. Examples: Configure cybersecurity tools and technologies with detection or response capabilities to securely ingest cyber threat intelligence feeds. Receive and review advisories from reputable third parties on current threat actors and their tactics, techniques, and procedures (TTPs). Monitor sources of cyber threat intelligence for information on the types of vulnerabilities that	The Qualys Enterprise TruRisk™ Platform leverages 25+ threat intelligence feeds and 80k+ signatures to pinpoint what has been exploited, is likely to be exploited, or has evidence of exploitation. Sources should also include files, webapps, containers, databases, middleware, IaaS, SaaS and more. Qualys PC, WAS, TotalCloud and FIM can help with all these.	Qualys Enterprise TruRisk™ Platform Qualys VMDR Qualys CSAM / EASM Qualys PC Qualys WAS Qualys TC Qualys FIM Qualys SAQ Qualys TP

	emerging technologies may have.		
	ID.RA-03: Internal and external threats to the organization are identified and recorded. Examples: Use cyber threat intelligence to maintain awareness of the types of threat actors likely to target the organization and the TTPs they are likely to use. Perform threat hunting to look for signs of threat actors within the environment. Implement processes for identifying internal threat actors.	With Qualys VMDR you can detect threats up to 6x faster and identify your riskiest vulnerabilities to reduce your mean time to remediation (MTTR) by up to 4 hours. Internal threats should include files, databases, and middleware; and external threats should include webapps, cloud, containers, etc. Qualys PC, WAS, TotalCloud and FIM can help with all these. Qualys Endpoint Protection can help meet requirements for threat hunting.	Qualys Enterprise TruRisk™ Platform Qualys VMDR Qualys CSAM / EASM Qualys PC Qualys WAS Qualys TC Qualys FIM Qualys SAQ Qualys TP Qualys Endpoint Protection
	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded. Examples: Business leaders and cybersecurity risk management practitioners work together to estimate the likelihood and impact of risk scenarios and record them in risk registers. Enumerate the potential business impacts of unauthorized access to the organization's communications, systems, and data processed in or by those systems. Account for the potential impacts of cascading failures for systems of systems.	Qualys VMDR allows you to prioritize vulnerabilities and reduce risks using transparent risk scoring with Qualys TruRisk prioritization. Threats should include files, databases, and middleware, webapps, cloud, containers, etc. Qualys PC, WAS, TotalCloud and FIM can help with all these.	Qualys Enterprise TruRisk™ Platform Qualys VMDR Qualys CSAM / EASM Qualys PC Qualys WAS Qualys TC Qualys FIM Qualys SAQ
	ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization. Examples: Develop threat models to better understand risks to the data and identify appropriate risk responses. Prioritize cybersecurity resource allocations and investments based on estimated likelihoods and impacts.	Qualys VMDR ensures you can automatically prioritize the riskiest vulnerabilities of your most critical assets by reducing discovered vulnerabilities from thousands to only the few hundred that matter most. Threats should include files, databases, and middleware, webapps, cloud, containers, etc. Qualys PC, WAS, TotalCloud and FIM can help with all these.	Qualys Enterprise TruRisk™ Platform Qualys VMDR Qualys CSAM / EASM Qualys PC Qualys WAS Qualys TC Qualys FIM Qualys SAQ Qualys TP
	ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated. Examples: Apply the vulnerability management plan's criteria for deciding whether to accept, transfer, mitigate, or avoid risk.	With Qualys VMDR, you can prioritize based on evidence of exploitation in the wild and the likelihood of exploitation to quickly see which vulnerabilities, assets, and groups of assets are most at risk. Comprehensive dashboards and reports allow you to properly track	Qualys Enterprise TruRisk™ Platform Qualys VMDR Qualys CSAM / EASM Qualys PC Qualys WAS Qualys TC Qualys FIM Qualys SAQ

	Apply the vulnerability management plan's criteria for selecting compensating controls to mitigate risk. Track the progress of risk response implementation (e.g., plan of action and milestones [POA&M], risk register, risk detail report). Use risk assessment findings to inform risk response decisions and actions.	and communicate risks to stakeholders. Risk responses should include files, databases, and middleware, webapps, cloud, containers, etc. Qualys PC, WAS, TotalCloud and FIM can help with all these.	
	ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked. Examples: Implement and follow procedures for the formal documentation, review, testing, and approval of proposed changes and requested exceptions. Document the possible risks of making or not making each proposed change, and provide guidance on rolling back changes. Document the risks related to each requested exception and the plan for responding to those risks. Periodically review risks that were accepted based upon planned future actions or milestones.	Qualys VMDR allows you to monitor vulnerability changes and exceptions, manage and assess for risk impact and ensure reporting and tracking. Changes and exceptions should include files, databases, and middleware, webapps, cloud, containers, etc. Qualys PC, WAS, TotalCloud and FIM can help with all these. Qualys FIM includes File Access Monitoring (FAM) and support for agentless network devices to monitor for unauthorized changes.	Qualys Enterprise TruRisk™ Platform Qualys VMDR Qualys CSAM / EASM Qualys PC Qualys WAS Qualys TC Qualys FIM Qualys SAQ
	ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established. Examples: Conduct vulnerability information sharing between the organization and its suppliers following the rules and protocols defined in contracts. Assign responsibilities and verify the execution of procedures for processing, analyzing the impact of, and responding to cybersecurity threat, vulnerability, or incident disclosures by suppliers, customers, partners, and government cybersecurity organizations.	Qualys VMDR allows you to analyze your riskiest vulnerabilities and reduce your mean time to remediation (MTTR) by up to 4 hours. Analysis and response should include files, databases, and middleware, webapps, cloud, containers, etc. Qualys PC, WAS, TotalCloud and FIM can help with all these.	Qualys Enterprise TruRisk™ Platform Qualys VMDR Qualys CSAM / EASM Qualys PC Qualys WAS Qualys TC Qualys FIM Qualys SAQ
	ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use.	Qualys VMDR lets you continuously detect critical vulnerabilities and misconfigurations across mobile devices, operating systems, and applications per industry standard hardening CIS benchmarks. Qualys CSAM provides asset	Qualys VMDR Qualys CSAM / EASM Qualys PC Qualys WAS Qualys TC Qualys SAQ

		management, and Qualys Policy Compliance (PC) ensure you can discover and authenticate unknown databases and middleware missed by most solutions. Integrity should include databases, and middleware, webapps, cloud, containers, etc. Qualys PC, WAS, and TotalCloud can help with all these.	
Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions	ID.IM-01: Improvements are identified from evaluations. Examples: Perform self-assessments of critical services that take current threats and TTPs into consideration. Invest in third-party assessments or independent audits of the effectiveness of the organization's cybersecurity program to identify areas that need improvement. Constantly evaluate compliance with selected cybersecurity requirements through automated means.	With the Qualys Enterprise TruRisk Platform dashboards and reports you can identify and communicate security risk improvements to stakeholders. Qualys Policy Compliance provides a NIST CSF 2.0 dashboard to constantly evaluate compliance.	Qualys Enterprise TruRisk Platform Qualys SAQ Qualys PC
	ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties. Example: Collect and analyze performance metrics using security tools and services to inform improvements to the cybersecurity program.	With the Qualys Enterprise TruRisk Platform you can identify improvements including those relevant to third parties.	Qualys Enterprise TruRisk Platform Qualys SAQ
	ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities. Example: Use metrics to assess operational cybersecurity performance over time.	Qualys Enterprise TruRisk Platform identifies improvements needed for execution.	Qualys Enterprise TruRisk Platform Qualys SAQ
PROTECT			
Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization.	Qualys CSAM with EASM can find and help manage hardware such as unmanaged IoT/OT internal assets, internet-facing digital assets (from mergers, acquisitions, and subsidiaries), and add business context with third-party connectors. Qualys PC can discover and help manage databases and middleware. Qualys Custom Assessment and Remediation (CAR) software	Qualys CSAM / EASM Qualys CAR Qualys PC Qualys TC Qualys SAQ

		helps you measure known and unknown risks, prioritize and communicate risk across vulnerabilities, and patch any device. Qualys TotalCloud includes Cloud Security Posture Management (CSPM) to provide an inventory of public cloud resources.	
	PR.AA-03: Users, services, and hardware are authenticated. Example: Periodically reauthenticate users, services, and hardware based on risk (e.g., in zero trust architectures).	Qualys CSAM and Qualys PC can ensure hardware authentication. Qualys CAR helps you measure known and unknown risks. Qualys Endpoint Security monitors endpoints to detect suspicious activity in real time, hunt for sophisticated threat actors across your environment.	Qualys SAQ Qualys CAR Qualys Endpoint Security
	PR.AA-04 Identity assertions are protected, conveyed, and verified.	Qualys CAR helps you measure known and unknown risks. Qualys Endpoint Security monitors endpoints to detect suspicious activity.	Qualys SAQ Qualys CAR Qualys Endpoint Security
Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected.	Data at rest includes files. Qualys FIM can ensure the confidentiality, integrity, and availability of file data. Qualys PC can ensure this for database data. Qualys Endpoint Security monitors endpoints to detect suspicious activity. Qualys TotalCloud protects Cloud Infrastructure & SaaS apps up to 85% faster with a unified, prioritized view of risk.	Qualys SAQ Qualys FIM Qualys PC Qualys Endpoint Security Qualys TC
	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.	Data in transit includes files. Qualys FIM can ensure the confidentiality, integrity, and availability of file data. Qualys PC can ensure this for database data. Qualys Endpoint Security monitors endpoints to detect suspicious activity in real time. Qualys TotalCloud protects Cloud Infrastructure & SaaS apps.	Qualys SAQ Qualys FIM Qualys PC Qualys Endpoint Security Qualys TC
	PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected. Example: Protect data in use from access by other users and processes of the same platform.	Data in use includes files. Qualys FIM can ensure the confidentiality, integrity, and availability of file data. Qualys PC can ensure this for database data. Qualys Endpoint Security monitors endpoints to detect suspicious activity in real time. Qualys TotalCloud protects Cloud Infrastructure & SaaS apps.	Qualys SAQ Qualys FIM Qualys PC Qualys Endpoint Security Qualys TC
Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and	PR.PS-01: Configuration management practices are established and applied.	Misconfigurations are a primary attack vector. Qualys PC discovers and remediates misconfigurations missed	Qualys SAQ Qualys PC Qualys WAS Qualys TC Qualys CSAM

virtual platforms are managed consistent with the organization’s risk strategy to protect their confidentiality, integrity, and availability	Examples: Establish, test, deploy, and maintain hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality). Review all default configuration settings that may potentially impact cybersecurity when installing or upgrading software. Monitor implemented software for deviations from approved baselines	by VM and other solutions. Qualys WAS has discovered and rectified 8M+ misconfigurations. Qualys TotalCloud includes Cloud Security Posture Management (CSPM) to provide an inventory of public cloud resources with detection and remediation of misconfigurations. Qualys CSAM can help ensure configuration management.	
	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk. Examples: Perform routine and emergency patching within the timeframes specified in the vulnerability management plan. Update container images, and deploy new container instances to replace rather than update existing instances. Replace end-of-life software and service versions with supported, maintained versions. Uninstall and remove unauthorized software and services that pose undue risks. Uninstall and remove any unnecessary software components (e.g., operating system utilities) that attackers might misuse. Define and implement plans for software and service end-of-life maintenance support and obsolescence.	Software vulnerabilities, misconfigurations, and management can be helped with Qualys VMDR, Qualys CSAM/EASM, Qualys PC, Qualys WAS, and Qualys TotalCloud. Qualys Patch Management can ensure patching is completed on time per the plan.	Qualys SAQ Qualys VMDR Qualys CSAM / EASM Qualys PC Qualys WAS Qualys TC Qualys GA Qualys PM
	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk. Examples: Replace hardware when it lacks needed security capabilities or when it cannot support software with needed security capabilities. Define and implement plans for hardware end-of-life maintenance support and obsolescence. Perform hardware disposal in a secure, responsible, and auditable manner.	Hardware vulnerabilities, misconfigurations, and management can be helped with Qualys VMDR, Qualys CSAM/EASM, Qualys PC, and Qualys TotalCloud	Qualys SAQ Qualys VMDR Qualys CSAM / EASM Qualys PC Qualys TC

	PR.PS-04: Log records are generated and made available for continuous monitoring. Examples: Configure all operating systems, applications, and services (including cloud-based services) to generate log records. Configure log generators to securely share their logs with the organization's logging infrastructure systems and services. Configure log generators to record the data needed by zero-trust architectures.	Log records are provided by all Qualys Enterprise TruRisk Platform apps including Qualys TotalCloud and PC. Qualys WAS can help cover web applications.	Qualys Enterprise TruRisk Platform Qualys TC Qualys PC Qualys WAS
	PR.PS-05: Installation and execution of unauthorized software are prevented. Examples: When risk warrants it, restrict software execution to permitted products only or deny the execution of prohibited and unauthorized software. Verify the source of new software and the software's integrity before installing it. Configure platforms to use only approved DNS services that block access to known malicious domains. Configure platforms to allow the installation of organization-approved software only.	Qualys CSAM/EASM, Qualys WAS, and Qualys TotalCloud can help discover unauthorized software usage.	Qualys SAQ Qualys CSAM / EASM Qualys WAS Qualys TC
	PR.PS-06 Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle. Examples: Protect all components of organization-developed software from tampering and unauthorized access. Secure all software produced by the organization, with minimal vulnerabilities in their releases. Maintain the software used in production environments, and securely dispose of software once it is no longer needed.	Qualys CSAM, GAV, and PC can help with the monitoring required for this subcategory. Qualys WAS can help protect web applications, and Qualys TotalCloud can help protect cloud software.	Qualys CSAM Qualys GAV Qualys PC Qualys WAS Qualys TC
Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity,	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	Qualys WAS and Qualys TotalCloud can help discover unauthorized access and usage. Qualys FIM now includes FAM and	Qualys SAQ Qualys WAS Qualys TC Qualys FIM Qualys Endpoint Security

and availability, and organizational resilience	Examples: Implement zero trust architectures to restrict network access to each resource to the minimum necessary. Check the cyber health of endpoints before allowing them to access and use production resources.	support for agentless network devices. Qualys Endpoint Security protects network and device endpoints from unauthorized access.	
	PR.IR-03 Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	Qualys PC can help achieve resilience requirements for this subcategory.	Qualys PC
DETECT			
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	DE.CM-01: Networks and network services are monitored to find potentially adverse events. Monitor DNS, BGP, and other network services for adverse events. Monitor wired and wireless networks for connections from unauthorized endpoints. Monitor facilities for unauthorized or rogue wireless networks. Compare actual network flows against baselines to detect deviations. Monitor network communications to identify changes in security postures for zero trust purposes.	Qualys WAS can help discover unauthorized access and usage. Qualys TotalCloud detects malware with up to 99% accuracy using AI-powered deep learning threat detection. Qualys FIM now includes FAM and support for agentless network devices. Qualys Continuous Monitoring (CM) alerts you in real time about network irregularities.	Qualys SAQ Qualys TotalCloud Qualys FIM Qualys CM
	DE.CM-02 The physical environment is monitored to find potentially adverse events.	Qualys Endpoint Security, including endpoint protection and extended detection & response (XDR) provides endpoint monitoring to detect adverse events.	Qualys Endpoint Security
	DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events. Examples: Monitor logs from logical access control systems to find unusual access patterns and failed access attempts. Continuously monitor deception technology, including user accounts, for any usage.	This includes file and software usage. Qualys FIM provides this for files. Qualys WAS provides this for web apps. Qualys TotalCloud includes SaaS Security Posture Management (SSPM) for cloud security. Qualys Endpoint Security and Qualys Continuous Monitoring can help monitor for adverse events.	Qualys SAQ Qualys WAS Qualys TotalCloud Qualys FIM Qualys Endpoint Security Qualys CM
	DE.CM-06: External service provider activities and services are monitored to find potentially adverse events. Example: Monitor activity from cloud-based services, internet service providers, and other service providers	External service providers interacting with files, web apps, cloud, etc. are covered by Qualys FIM, Qualys WAS, and Qualys Total Cloud	Qualys SAQ Qualys WAS Qualys TotalCloud Qualys FIM

	for deviations from expected behavior.		
	DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events. Examples: Monitor email, web, file sharing, collaboration services, and other common attack vectors to detect malware, phishing, data leaks and exfiltration, and other adverse events. Monitor authentication attempts to identify attacks against credentials and unauthorized credential reuse. Monitor software configurations for deviations from security baselines. Monitor hardware and software for signs of tampering. Use technologies with a presence on endpoints to detect cyber health issues (e.g., missing patches, malware infections, unauthorized software), and redirect the endpoints to a remediation environment before access is authorized.	Qualys VMDR monitors for vulnerabilities and Qualys PC and Qualys WAS discovers misconfigurations. Runtime environments include cloud and containers, covered by Qualys TotalCloud. Qualys CM and Endpoint Security can also provide continuous monitoring. Qualys FIM can provide monitoring for agentless network devices and file changes.	Qualys SAQ Qualys VMDR Qualys PC Qualys WAS Qualys TotalCloud Qualys CM Qualys Endpoint Security Qualys FIM
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents	DE.AE-02: Potentially adverse events are analyzed to better understand associated activities. Examples: Utilize up-to-date cyber threat intelligence in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise. Regularly conduct manual reviews of log events for technologies that cannot be sufficiently monitored through automation. Use log analysis tools to generate reports on their findings.	Qualys VMDR, Qualys PC, Qualys WAS, Qualys FIM, Qualys Endpoint Security, and Qualys TotalCloud can help detect potentially adverse events.	Qualys SAQ Qualys VMDR Qualys PC Qualys WAS Qualys FIM Qualys Endpoint Security Qualys TC
	DE.AE-03: Information is correlated from multiple sources. Example: Utilize cyber threat intelligence to help correlate events among log sources.	Qualys Enterprise TruRisk is the industry standard on how to apply risk-based prioritization to your cyber security program. While EPSS and CVSS are foundational metrics for severity, they can miss real threats and fail to filter out non-critical risk without complete business context	Qualys SAQ Qualys Enterprise TruRisk Platform Qualys Endpoint Security

		of the environment. TruRisk aggregates ALL risk-factors from 73,000 vulnerability signatures, 25+ sources of threat intel, and integrations with third-party solutions. Qualys Endpoint Security correlates data from multiple sources including other Qualys apps.	
	DE.AE-04: The estimated impact and scope of adverse events are understood. Example: Use tools to estimate impact and scope, and review and refine the estimates.	The Qualys Enterprise TruRisk Platform lets you prioritize risk by overall business impact and remediate efficiently with risk-based patching, AI-powered adaptive mitigation, and an integrated workflow across teams. Qualys Endpoint Security can provide impact estimation for adverse events.	Qualys SAQ Qualys Enterprise TruRisk Platform Qualys Endpoint Security
	DE.AE-06: Information on adverse events is provided to authorized staff and tools. Examples: Use cybersecurity software to generate alerts and provide them to the security operations center (SOC), incident responders, and incident response tools. Incident responders and other authorized personnel can access log analysis findings at all times. Automatically create and assign tickets in the organization's ticketing system when certain types of alerts occur. Manually create and assign tickets in the organization's ticketing system when technical staff discover indicators of compromise.	The Qualys Enterprise TruRisk Platform and apps provide numerous dashboards and reports to facilitate this. Qualys Endpoint Security can provide information and alters for adverse events. ITSM automation for support ticketing can help reduce manual efforts. Qualys FIM includes noise cancellation to reduce false alerts by 90%+.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps Qualys Endpoint Security Qualys FIM
	DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis. Examples: Securely provide cyber threat intelligence feeds to detection technologies, processes, and personnel. Securely provide information from asset inventories to detection technologies, processes, and personnel. Rapidly acquire and analyze vulnerability disclosures for the organization's technologies from suppliers, vendors,	The Qualys Enterprise TruRisk Platform and apps integrate contextual information across numerous dashboards and reports including Qualys CSAM, GAV, VMDR, PC, TC Endpoint Security, FIM, WAS.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps Qualys VMDR Qualys PC Qualys WAS Qualys FIM Qualys Endpoint Security Qualys TC

	and third-party security advisories.		
	DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria. Examples: Apply incident criteria to known and assumed characteristics of activity in order to determine whether an incident should be declared. Take known false positives into account when applying incident criteria.	The Qualys Enterprise TruRisk Platform and apps provides scores and alerts to help meet this requirement, including Qualys Endpoint Security and Qualys FIM, both which include technologies to reduce false positives.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps Qualys Endpoint Security Qualys FIM
RESPOND			
Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed	RS.MA-01 The incident response plan is executed in coordination with relevant third parties once an incident is declared. Example: Detection technologies automatically report confirmed incidents.	The Qualys Enterprise TruRisk Platform and apps provides customizable reports to help meet this requirement, including Qualys VMDR, Patch Management, Endpoint Security, TotalCloud, and Policy Compliance.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps Qualys VMDR Qualys PC Qualys Endpoint Security Qualys TC Qualys PM
	RS.MA-02: Incident reports are triaged and validated. Example: Preliminarily review incident reports to confirm that they are cybersecurity-related and necessitate incident response activities. Apply criteria to estimate the severity of an incident.	The Qualys Enterprise TruRisk Platform and apps provides customizable reports to help meet this requirement, including Qualys VMDR, Patch Management, Endpoint Security, TotalCloud, and Policy Compliance.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps Qualys VMDR Qualys PC Qualys Endpoint Security Qualys TC Qualys PM
	RS.MA-03: Incidents are categorized and prioritized. Examples: Further review and categorize incidents based on the type of incident (e.g., data breach, ransomware, DDoS, account compromise). Prioritize incidents based on their scope, likely impact, and time-critical nature.	The Qualys Enterprise TruRisk Platform and apps provide for categorization and prioritization based on TruRisk to the business to help meet this requirement, including Qualys VMDR and Endpoint Security.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps Qualys VMDR Qualys Endpoint Security
	RS.MA-04: Incidents are escalated or elevated as needed. Example: Track and validate the status of all ongoing incidents.	The Qualys Enterprise TruRisk Platform and apps provide for escalation based on TruRisk to the business to help meet this requirement, including Qualys VMDR, Qualys TotalCloud, and Qualys Policy Compliance	Qualys SAQ Qualys Enterprise TruRisk Platform and apps Qualys VMDR Qualys PC Qualys TC
	RS.MA-05: The criteria for initiating incident recovery are applied.	The Qualys Enterprise TruRisk Platform and apps offer automated remediation based on TruRisk criteria to help meet this requirement.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps
Incident Analysis (RS.AN): Investigations are	RS.AN-03: Analysis is performed to establish	The Qualys Enterprise TruRisk Platform and many	Qualys SAQ

conducted to ensure effective response and support forensics and recovery activities	what has taken place during an incident and the root cause of the incident. Attempt to determine what vulnerabilities, threats, and threat actors were directly or indirectly involved in the incident. Analyze the incident to find the underlying, systemic root causes. Check any cyber deception technology for additional information on attacker behavior.	apps offer analysts vulnerability and threat scores mapped to MITRE ATT&CK data to understand root causes. Qualys VMDR and Endpoint Security that can help identity root causes.	Qualys Enterprise TruRisk Platform and apps Qualys VMDR
	RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved. Example: Collect, preserve, and safeguard the integrity of all pertinent incident data and metadata (e.g., data source, date/time of collection) based on evidence preservation and chain-of-custody procedures.	The Qualys Enterprise TruRisk Platform and collective data and metadata to meet this requirement.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps
	RS.AN-08: An incident's magnitude is estimated and validated. Example: Review other potential targets of the incident to search for indicators of compromise and evidence of persistence. Automatically run tools on targets to look for indicators of compromise and evidence of persistence.	The Qualys Enterprise TruRisk Platform and apps offer based on TruRisk scores and threat data mapped to MITRE ATT&CK to help meet this requirement.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps
Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects	RS.MI-01: Incidents are contained. Cybersecurity technologies (e.g., antivirus software) and cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) automatically perform containment actions.	The Qualys Enterprise TruRisk Platform and apps offer automated remediation based on TruRisk criteria to help meet this requirement. Qualys Endpoint Security offers automated remediation via Qualys PC to reduce time, effort, and mistakes. Qualys VMDR provides vulnerability remediation response capabilities.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps Qualys Endpoint Security Qualys PC Qualys VMDR
	RS.MI-02: Incidents are eradicated. Example: Cybersecurity technologies and cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) automatically	The Qualys Enterprise TruRisk Platform and apps offer automated remediation based on TruRisk criteria to help meet this requirement. Qualys Endpoint Security offers automated remediation via Qualys PC to reduce time, effort, and mistakes. Qualys	Qualys SAQ Qualys Enterprise TruRisk Platform and apps Qualys Endpoint Security Qualys PC Qualys VMDR

	perform eradication actions.	VMDR provides vulnerability response eradication.	
RECOVER			
Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed. Example: Select recovery actions based on the criteria defined in the incident response plan and available resources.	The Qualys Enterprise TruRisk Platform and apps offer automated remediation/recovery based on TruRisk criteria to help meet this requirement. Qualys Endpoint Security offers automated remediation/recovery via Qualys PC to reduce time, effort, and mistakes. Qualys VMDR with Qualys Patch Management (PM), which detects open vulnerabilities and missing patches across assets on-premises, in the cloud, and at remote endpoints. Efficiently schedule patch deployment jobs tailored to specific asset types or swiftly deploy emergency patches as needed.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps Qualys Endpoint Security Qualys PC Qualys VMDR Qualys PM
	RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration. Example: Check restoration assets for indicators of compromise, file corruption, and other integrity issues before use.	The Qualys Enterprise TruRisk Platform and apps such Qualys VMDR and Qualys WAS can be used to scan assets for restoration verification. Qualys Policy Compliance can provide visibility into asset integrity. Qualys FIM can help check for file corruption.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps Qualys VMDR Qualys WAS Qualys PC Qualys FIM
	RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms. Example: Monitor the performance of restored systems to verify the adequacy of the restoration.	Qualys Enterprise TruRisk is the industry standard on how to apply risk-based prioritization to your cyber security program. While EPSS and CVSS are foundational metrics for severity, they can miss real threats and fail to filter out non-critical risk without complete business context of the environment	Qualys SAQ Qualys Enterprise TruRisk Platform
	RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed. Examples: Check restored assets for indicators of compromise and remediation of root causes of the incident before production use. Verify the correctness and adequacy of the restoration actions taken before putting a restored system online.	The Qualys Enterprise TruRisk Platform and apps can be used to verify the integrity of restored assets. Qualys VMDR, PC, CSAM, Endpoint Security, and other apps can help check restored assets for IOCs.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps Qualys VMDR Qualys PC Qualys CSAM Qualys Endpoint Security
	RC.RP-06: The end of incident recovery is declared based on criteria,	The Qualys Enterprise TruRisk Platform and apps provide customizable	Qualys SAQ Qualys Enterprise TruRisk Platform and apps

	and incident-related documentation is completed. Example: Prepare an after-action report that documents the incident itself, the response and recovery actions taken, and lessons learned.	dashboards and reports to provide incident-related documentation.	
Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties	RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders. Example: Prepare an after-action report that documents the incident itself, the response and recovery actions taken, and lessons learned.	The Qualys Enterprise TruRisk Platform and apps provide customizable dashboards and reports to facilitate communications to internal and external stakeholders.	Qualys SAQ Qualys Enterprise TruRisk Platform and apps

Conclusion

NIST CSF 2.0 has taken a decade to get here, but rather than view this as an additional burden and constraint on your organization, covering the requirements in the right way with the right solutions can help bolster your firm's overall security posture and reduce risks for cybersecurity breaches, brand damage, and litigation.

The Qualys Enterprise TruRisk Platform provides you with a unified view of your entire cyber risk posture so you can efficiently aggregate and measure all Qualys and non-Qualys risk factors in a unified view, communicate cyber risk with context to your business, and go beyond patching to eliminate the risk that threatens the business in any area of your attack surface.

The Enterprise TruRisk platform supports dozens of apps, including CSAM, VMDR, PC, Endpoint Security, TotalCloud, WAS, FIM, and many others, that can help you address requirements across all six CSF 2.0 functions. With Qualys, attaining top tier Adaptive status is not only achievable, but can help you reduce overall costs and efforts along the way. Contact Qualys today to learn more.
For more information and to start your free trial, visit Qualys.com.

Contributors:

Bill Reed, Qualys Product Marketing