IBM Security

# Making the most of your risk management resources

How an effective security framework can help provide important protection

Let’s get started

# Contents

# The potential benefits of a security framework

As the volume and potential impact of cyber security risks continue to grow, today's organizations face mounting challenges in their efforts to manage them. But in the race to develop effective risk management programs and policies, it's become clear that one size does not fit all. While multiple organizations may be threatened by the same attacks, each organization's size, complexity, risk tolerance and threat management policies and processes contribute to a unique environment—with its own requirements and best practices for protection. And in each organization, risk will ultimately be defined by a set of complex calculations that attempt to balance costs with potential losses.

Virtually any discussion of risk needs to start by considering how an organization operates. That means understanding the data, technology and human resources it relies upon, knowing where information is stored and who has access to it, what needs to be protected.

A security framework functions as a structure designed to help shape and support the protection process. It provides a logical approach to digital risk management. And it lays a foundation for a flexible protection plan that can adapt over time to meet the maturity level of the threats it faces and the security capabilities it employs.

**Of course there are different types of security frameworks. Some, like the National Institute of Standards and Technology—or NIST—Cybersecurity Framework, offer a set of industry standards and best practices designed to help organizations manage cybersecurity risks. While others focus on ISO 27000 series sector-specific approaches or compliance regimes.**

# Different types of frameworks meet different types of needs

*With each organization needing to manage its own risks and managing vulnerabilities—as well as its own processes and technologies—the framework approach to risk management offers a structured way to identify and assess an organization's cyber security needs.*

It also provides a common language on addressing risk that others within their ecosystem and supply chain can readily understand.  The Framework approach can include everything from establishing general best practices and controlling the actions of people or applications, to complying with government mandates or industry security requirements.

Frameworks provide a step-by-step approach that lets an organization evolve from meeting its basic security requirements to developing a security-optimized environment that can easily adapt as its needs and capabilities mature. They make it possible for organizations to address gaps and shortcomings—and provide more effective protection over time. That's why framework-based digital risk management has emerged as an imperative for organizations of all types. And as many organizations continue to establish the position of chief information security officer (CISO), it's giving upper management direct involvement and engagement with security and more effectively supporting the use of sophisticated techniques, such as analytics, to help prevent security problems.

## What's right for your organization?

Creating a security framework tailored to your organization by—blending the capabilities of multiple frameworks to meet your organization's unique requirements—is a critical step in both meeting current challenges and anticipating future needs. It's important to start the selection process with an assessment of risks across your organization, along with an assessment of industry frameworks, standards, guidance and preferred practices that are either available or required for ensuring security.

In addition to the four security framework models discussed here, there are also new models making their way into the mix, some of which offer tools to combine some or all of these frameworks into a single, custom-designed security framework, such as the Unified Compliance Framework.

But regardless of the approach you choose, the result should be able to help tailor your move toward ensuring the right level of digital security for the risk your organization accepts against the threats it faces.

# Four security framework models support a range of risk management issues

## What security frameworks can do for you

Effective security frameworks can help your organization:

- Increase security awareness and accuracy—by detecting and preventing sophisticated threats, increasing visibility and awareness and conducting comprehensive incident investigations
- Ease the burden on IT administrators—by simplifying risk management and decision making, enabling fast deployment and enhancing auditing and access capabilities
- Improve line-of-business productivity—by instilling confidence that business operations are secure
- Reduce costs and complexity enterprise-wide, delivering increased value and lowering total cost of ownership

Each of the four common types of security framework discussed here addresses a set of key digital risk-management components—such as technology products and services, IT skills and regulatory compliance—along with such issues as stakeholder input, security metrics and threat measurement.

**An incident response—or process—framework** focuses on incident prevention and response. The US National Institute of Standards and Technology (NIST) released its Framework for Improving Critical Infrastructure Cybersecurity, which provides a common language, set of activities, best practices and standards for managing cybersecurity risk. IBM, along with many other industry stakeholders, contributed to the development of this NIST framework, demonstrating the importance of a public-private collaboration for improving cybersecurity.

Intended for government and business organizations alike, the NIST Cybersecurity Framework currently  describes five core functions:

- **Identification:** Developing the organizational understanding necessary to manage cybersecurity risk to systems, assets, data and capabilities, while creating an understanding of business context, resources and risks that will allow the organization to focus and prioritize its efforts.
- **Protection:** Developing and implementing safeguards to ensure the delivery of infrastructure services and to help limit or contain the impact of a cybersecurity event.
- **Detection:** Developing and implementing activities to identify the occurrence of a cybersecurity event.
- **Response:** Developing and implementing a specific set of activities following the detection of a cybersecurity event and providing the support necessary to contain its impact.
- **Recovery:** Developing and implementing activities to maintain resilience and restore any capabilities or services that may have been impaired as the result of a cybersecurity event, providing support for a timely recovery to normal operations.

While the five NIST core functions serve as reference points for an organization establishing security frameworks, it's important to recognize that the NIST framework is largely a process model for incident prevention and response that focuses on how to manage an incident. It provides attack-related processes and actions from prevention to post-exploitation. But it doesn't address specific security domains, compliance requirements, unique demands or circumstances, the need for measurability or the technology infrastructure—all of which are typically covered in a cyclical, iterative risk management plan for the full security lifecycle. That's where the following three security frameworks come into play.

# How IBM can help build and support your security frameworks

IBM® Security solutions offer a comprehensive portfolio that can help you address all four security frameworks discussed here, including NIST framework core categories and subcategories, implementation tiers and framework profiles. In doing so, we can help you meet your risk management goals and objectives for enhancing cost efficiency and simplifying management by providing scalability and flexibility to help you avoid perceived gaps in coverage as threats evolve and change.

For organizations with more mature security strategies and more complex and demanding protection needs, IBM Security solutions can provide comprehensive controls and integrated actions to support strict risk.

**A domain framework** reflects the ways in which information technology is built out around the Control Objectives for Information and Related Technologies (COBIT) and International Organization for Standardization (ISO) standards for security risk management. It aligns a set of domains with an organization's four key assets: protecting its infrastructure and networks, people, data and applications. And it provides situational awareness for senior management teams, offering them an understanding of how their organizations are meeting established requirements for cybersecurity. What's more, a domain framework is likely to offer the broadest view of risk among the framework options discussed here.

## An overview of IBM solutions for addressing NIST framework requirements

| | Security intelligence | Identity and access management | Data security | Infrastructure (mobile, network, endpoint, mainframe) | Application security | Intelligence analysis (i2) | Security services |
|---|---|---|---|---|---|---|---|
| Identify: Asset management | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Identify: Business environment | ■ | | ■ | | | | ■ |
| Identify: Governance | ■ | ■ | ■ | ■ | ■ | | ■ |
| Identify: Risk assessment | ■ | | ■ | ■ | ■ | ■ | ■ |
| Protect: Identity and access | ■ | ■ | ■ | ■ | | ■ | ■ |
| Protect: Awareness and training | ■ | ■ | | | | ■ | ■ |
| Protect: Data security | ■ | | ■ | ■ | | ■ | ■ |
| Protect: Information protection | ■ | ■ | ■ | ■ | | ■ | ■ |
| Protect: Maintence | ■ | ■ | ■ | ■ | | | ■ |
| Protect: Protective technology | ■ | ■ | ■ | ■ | | | ■ |
| Detect: Anomalies and events | ■ | | ■ | ■ | | ■ | ■ |
| Detect: Security continuous monitoring | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Detect: Detection processes | ■ | | ■ | ■ | | | ■ |
| Respond: Response planning | ■ | | | | | | ■ |
| Respond: Communications | ■ | | | ■ | | ■ | ■ |
| Respond: Analysis | ■ | | ■ | ■ | | ■ | ■ |
| Respond: Mitigation | ■ | ■ | ■ | ■ | | | ■ |
| Respond: Improvements | ■ | | | | | | ■ |
| Recover: Recovery planning | ■ | | | | | | ■ |
| Recover: Improvements | ■ | | ■ | | | | ■ |
| Recover: Communications | | | | | | | |

*This is a summary showing where IBM offers solutions related to specific NIST standards. For a more detailed listing, please see the appendix.*

**A sectoral framework** is designed to address the security concerns of specific vertical business sectors. It can be customized to provide granular management capabilities that are specific to meeting operational and regulatory regimens and compliance mandates. Energy and utilities organizations, for example, must adapt their frameworks to support compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. Similarly, financial services organizations must meet security standards established by the Federal Financial Institutions Examination Council (FFIEC) and other regulatory bodies. Sectoral frameworks provide these extended and specialized functions while continuing to meet the NIST Cybersecurity Framework voluntary goals for the latest security issues facing IT domains.

**An organizational framework** is typically tailored to meet the individual needs of an organization by adapting elements of the domain, incident response and sectoral approaches. It allows those organizations to create a customized framework that takes an even closer look at the overall risk the enterprise faces—by determining its unique security requirements, ensuring capabilities are in place to provide the necessary security, and aligning requirements and technologies with its internal policies and processes. In other words, an organizational framework is typically most focused on threats to the business itself. For example, an organizational framework might include evolving threats, changing business needs, economic volatility, increasing regulation, technology and process changes, and geographic or facilities changes.

As with sectoral frameworks, the organizational framework is designed to meet NIST and organizational domain guidelines. But it may also give special attention to a limited number of specific approaches for addressing risk and measuring the effectiveness of protection. According to its specific needs, an organization may or may not require that security be integrated across all business or operational functions. The fundamental role of an organizational framework is to adapt risk management to specific and often unique conditions, while building on the capabilities of the cross-industry domain framework. An organizational framework may also be used to address a specific portion of the business and its operating environment.

## Key framework issues

- **Evolving threats**—include increasingly sophisticated approaches, new attack methods and adaptation to the latest technologies and delivery methods.
- **Changing business needs**—include evolving lines of business, acquisitions and mergers, the integration of operations and the addition or elimination of business functions.
- **Volatile economics**—include changes in profitability, the market for the current goods and services, local and international economic trends and wholesale currency changes.
- **Increasing regulation**—include changes and additions to regulatory and compliance requirements issued by local, national or international governing bodies.
- **Technology and process changes**—include the addition of new technologies and the elimination of existing ones or the implementation of new technology-based programs.

# Why IBM

We know that approaching security frameworks and risk management is not a simple exercise. Cyber threats change all the time, as do your organization's business environment and the availability of  resources to respond to those changes. But your organization still needs to be able to apply new risk strategies as soon as the need arises—especially when those strategies are key to supporting business operations and reducing risk.

IBM offers a comprehensive set of solutions and services designed to help you develop and implement risk management strategies for your organization. Within that context, we deliver leading technology, best practices and, above all, flexibility.

When you collaborate with IBM, you gain access to a security team of 8,000 people supporting more than 12,000 customers in 133 countries. As a proven leader in enterprise security, we hold more than 3,500 security patents. And with an approach that includes advanced cognitive computing, we help organizations like yours continue to innovate while reducing risk. So you can continue to grow your business—while securing your most critical data and processes.

## For more information

To learn more about the IBM Security portfolio of solutions, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security

Additionally, IBM Global Financing offers numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit:
ibm.com/financing

# IBM Security solutions key

| Category | Full product name | Short name/abbreviation | Short description |
|---|---|---|---|
| **Security Intelligence** | IBM QRadar® Advisor with Watson | IBM QRadar Advisor with Watson | Combines the cognitive capabilities of Watson and QRadar Security Analytics Platform to uncover hidden threats and automate insights |
| | IBM Security QRadar Incident Forensics | QRIF | Reduce time to investigate incidents, and remediate more thoroughly |
| | IBM Security QRadar Log Manager | QRadar LM | Turn-key log management, SMB to enterprise (upgradeable to SIEM) |
| | IBM Security QRadar QFlow Collector | QFlow | Layer 7 application monitoring of physical network traffic (includes VFlow) |
| | IBM Security QRadar Network Insights | QNI | Enables attack prediction through real-time network traffic analysis |
| | IBM Security QRadar SIEM | QRadar SIEM | Security intelligence & IBM Sense Analytics, protecting assets & information from advanced threats |
| | IBM QRadar on Cloud | QRoC | Outsources security intelligence deployment/support, by offering QRadar as a service |
| | IBM QRadar User Behavior Analytics | QRadar UBA | An app that provides early visibility to insider threats. |
| | IBM Security QRadar Vulnerability Manager | QVRM | Intelligent scanning - identifies and prioritizes vulnerabilities – integrates for prioritization insights |
| | i2® Intelligence Analysis Platform (including i2 Enterprise Insight Analysis and i2 Analyst's Notebook) | i2 | A system that facilitates the analysis, production, and reporting of security intelligence |
| | Resilient® Incident Response Platform | Resilient IRP | Allows security teams to easily configure incident response plans/technologies |
| **Advanced Fraud Protection** | IBM Security Trusteer® Fraud Protection Suite | Fraud Protection Suite | Designed to detect, enforce, investigate and remediate fraud fast and efficiently |
| | IBM Security Trusteer Pinpoint Detect | Pinpoint Detect | Real-time detection of Man-in-the-Browser malware infected devices |
| | IBM Security Trusteer Pinpoint Malware Detection | Pinpoint Malware Detection | Designed to provide conclusive detection of criminals and account takeover attempts |
| | IBM Security Trusteer Rapport | Rapport | Client-based endpoint detection, mitigation/remediation against financial malware/ phishing attacks |
| | IBM Security Trusteer Rapport for Mitigation | Rapport for Mitigation | Mitigation/remediation against financial malware |
| | IBM Security Trusteer Mobile SDK | Mobile SDK | Android/iOS library for native mobile apps detect compromised/vulnerable devices |
| | IBM Security Trusteer Mobile Browser | Mobile Browser | Secure mobile browser for safe web access |
| **Identity and Access Management (People)** | IBM Security Access Manager for ESSO | SAM ESSO | SSO, password management, session management, compliance and user productivity gains |
| | IBM Security Access Manager | SAM | All-in-one access appliance for web, mobile and cloud |
| | IBM Security Access Manager for DataPower | SAM for DataPower | Web access management software module for IBM DataPower Gateways |
| | IBM Cloud Identity Connect | CIC | Securely connect employees to cloud services |
| | IBM Cloud Identity Service | CIS | Multitenant identity and access management service offered from the public cloud |
| | IBM Security Identity and Access Assurance | IAA or SIAA | Discounted bundle - SAM, IGI Lifecycle, Directory Suite, QRadar Log Manager |
| | IBM Security Identity and Access Manager | SIAM | Discounted bundle - SAM base appliance and IGI Lifecycle |
| | IBM Security Identity Governance and Intelligence | IGI | Govern access and evaluate regulatory compliance – bring IT and LoBs together |
| | IBM Security Identity Manager | SIM | Creates, modifies and terminates user privileges throughout users' lifecycles |
| | IBM Security Privileged Identity Manager | PIM | Keeps admin (privileged user) ID usage tracked and under control |
| | IBM Security Directory Suite | SDS | Real-time, event-driven, general-purpose data integration environment (includes Directory Server) |

Return to How IBM can help

Next page

| Category | Full product name | Short name/abbreviation | Short description |
|---|---|---|---|
| **Data Security** | IBM Guardium® Activity Monitor for Databases | Guardium DAM | Real time data activity monitoring with blocking/masking capabilities |
| | IBM Guardium Activity Monitor for Files | Guardium FAM | Discover/track/control sensitive file access (local/networked file systems) |
| | IBM Guardium Vulnerability Assessment | Guardium VA | Vulnerability assessment for databases |
| | IBM Guardium Data Encryption | Guardium DES | DBMS encryption (Oracle, SQL Server, DB2, IMS, …) and file encryption |
| | IBM Guardium Data Encryption for DB2 and IMS Databases | Guardium DES for z/OS | Data encryption for both DB2 and IMS databases on z/OS |
| | IBM Guardium Data Redaction | Guardium Data Redaction | Designed to protect sensitive data in documents and forms from unintentional disclosure |
| | IBM Multi-Cloud Data Encryption | MDE | Designed to protect databases, file shares, data warehouses, and big data implementations in private/hybrid/public clouds |
| | IBM Multi-Cloud Data Protection | Multi-Cloud Data Protection | Designed to safeguard critical data where it resides, with cloud-based capabilities |
| | Agile® 3 GRC Command & Control Center | Agile 3 | A dashboard designed to provide visibility to identify potential risks to sensitive assets |
| | IBM Security Key Lifecycle Manager | SKLM | Enterprise management of encryption keys (key server on distributed platforms) |
| | IBM Security Key Lifecycle Manager for z/OS | SKLM for z/OS | Enterprise management of encryption keys (key server on mainframe) |
| | IBM Key Protect | Key Protect | Manages the lifecycle of encryption keys for apps across Bluemix® |
| **Application Security** | IBM Application Security on Cloud | ASoC | Designed to provide static, dynamic and interactive application security testing on cloud apps |
| | IBM Security AppScan® Enterprise | AppScan Enterprise | Enterprise dynamic (unattended, parallel) app scanning and reporting |
| | IBM Security AppScan Source | AppScan Source | Static testing of application source code for vulnerabilities |
| | IBM Security AppScan Standard | AppScan Standard | Dynamic testing of running web applications for vulnerabilities |
| **Infrastructure Security (Mobile, Network, Server and Endpoint)** | IBM MaaS360® | MaaS360 | Enterprise mobile platform - security/management for applications/documents/devices |
| | IBM X-Force® Exchange Commercial API | X-Force Exchange Comm API | API that makes a wide range of IBM Security Threat Intelligence available |
| | IBM BigFix® Compliance | BigFix Compliance | Designed to protect endpoints. Better meet security compliance. Designed to reduce costs and enhance agility |
| | IBM BigFix Patch | BigFix Patch | Server management – lifecycle management; security and compliance and server automation |
| | IBM BigFix Inventory | BigFix Inventory | Software asset management - designed to discover all licensed/unlicensed software for all devices |
| | IBM BigFix Detect | BigFix Detect | Integrates attack detection with remediation capabilities for endpoint security |
| | IBM BigFix Lifecycle | BigFix Lifecycle | Find/fix endpoint problems - connected or not, fixed or mobile, virtual or physical |
| | IBM Security zSecure® Admin | zSecure Admin | Solution to improve administration, audit, and compliance for System z |
| | IBM Security zSecure Audit | zSecure Audit | Provides highly customizable reporting and analysis of audit records |
| | IBM Security zSecure Alert | zSecure Alert | Real-time threat monitoring extending RACF/ACF2 real-time notification capabilities |
| | IBM Security zSecure Command Verifier | zSecure CV | Designed to control compliance by preventing erroneous or out-of-policy RACF commands |
| **Security Services** | Security Strategy, Risk and Compliance | SSRC | Assess, evaluate, and recommend to improve security risk management |
| | Security Intelligence and Operations Consulting | SIOC | Advise for the development of intelligence-driven security operations |
| | Infrastructure and Endpoint Security | IES | Managed security services for network, web, and messaging security |
| | Data and Application Security | DAS | Consulting and managed services for data security, including encryption |
| | X-Force Red Offensive Security | XFP | Security testing program focused on vulnerability management, rapid testing, and analytics |
| | X-Force Incident Response and Intelligence Services | XF IRIS | Prepare clients to respond to threats and incidents across the entire incident lifecycle |
| | Identity and Access Management | IAM | Consulting services recommending and integrating IAM components |
| | IT Risk Management Services | ITRMS | Create an IAM strategy and assist in deploying appropriate IAM solutions |

Return to How IBM can help

Next page

# How NIST framework requirements map to IBM solutions

This table shows which IBM solutions map to specific NIST standards.

| Function | Category | Subcategory | IBM Offerings |
|---|---|---|---|
| **IDENTIFY (ID)** | Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. | ID.AM-1: Physical devices and systems within the organization are inventoried | QVRM, BigFix Inventory, Resilient IRP, MaaS360 |
| | | ID.AM-2: Software platforms and applications within the organization are inventoried | QVRM, BigFix Inventory, AppScan Enterprise, DAS, Guardium VA (Discovery), MaaS360 |
| | | ID.AM-3: Organizational communication and data flows are mapped | QFlow, QNI, QRIF, QRadar SIEM, IBM QRadar Advisor with Watson, SSRC, SIOC, DAS, i2 |
| | | ID.AM-4: External information systems are catalogued | i2, SSRC |
| | | ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value | QRadar SIEM, IBM QRadar Advisor with Watson, QVRM, BigFix Inventory, Guardium VA (Discovery and Classification), MaaS360, i2 |
| | | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | Resilient IRP, PIM, zSecure Admin, SSRC, ITRMS, Guardium VA (Entitlement Reporting) |
| | Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities and risk management decisions. | ID.BE-1: The organization's role in the supply chain is identified and communicated | SSRC |
| | | ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated | SSRC |
| | | ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated | SSRC, Guardium Data Protection |
| | | ID.BE-4: Dependencies and critical functions for delivery of critical services are established | QRadar SIEM, IBM QRadar Advisor with Watson, QVRM, Resilient IRP, SSRC, XFP, Guardium Data Protection |
| | | ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) | QRadar SIEM, IBM QRadar Advisor with Watson, QVRM, Resilient IRP, SSRC, XFP, Guardium Data Protection |
| | Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and inform the management of cybersecurity risk. | ID.GV-1: Organizational information security policy is established | QRadar SIEM, IBM QRadar Advisor with Watson, QVRM, SIOC, ITRMS, Guardium Data Protection, MaaS360 |
| | | ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | zSecure Admin, ITRMS, Guardium Data Protection, Guardium VA (Entitlement Reporting), IGI |
| | | ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | ITRMS, Guardium Data Protection |
| | | ID.GV-4: Governance and risk management processes address cybersecurity risks | QRadar SIEM, IBM QRadar Advisor with Watson, QVRM, AppScan Enterprise, zSecure Admin, XFP, ITRMS, Guardium VA (Vulnerability Assessment), IGI,D33 MaaS360 |
| | Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals. | ID.RA-1: Asset vulnerabilities are identified and documented | QRadar SIEM, QVRM, AppScan Enterprise, Guardium VA (Vulnerability Assessment), XFP, Resilient IRP, MaaS360 |
| | | ID.RA-2: Cyber threat intelligence and vulnerability information is received from information sharing forums and sources | QRadar SIEM, QVRM, ASoC, SIOC, XFP, Guardium VA (Vulnerability Assessment), i2 |
| | | ID.RA-3: Threats, both internal and external, are identified and documented | QRadar SIEM, QRadar UBA, SSRC, SIOC, XFP, XF IRIS, Guardium VA (Vulnerability Assessment), Guardium Data Protection, i2 |
| | | ID.RA-4: Potential business impacts and likelihoods are identified | SSRC, XFP, XF IRIS, Agile 3, Guardium VA (Vulnerability Assessment) |
| | | ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | QRadar SIEM, QVRM, XFP, XF IRIS, Resilient IRP, Guardium VA (Vulnerability Assessment), MaaS360, i2 |
| | | ID.RA-6: Risk responses are identified and prioritized | AppScan Enterprise, XFP, XF IRIS, Resilient IRP, Guardium VA (Vulnerability Assessment) |
| | Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions. | ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders | Resilient IRP , SSRC, Agile 3, Guardium VA (Vulnerability Assessment) |
| | | ID.RM-2: Organizational risk tolerance is determined and clearly expressed | Resilient IRP , Agile 3, SSRC, Agile 3, Guardium VA (Vulnerability Assessment), Guardium Data Protection, i2 |
| | | ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | SSRC, Agile 3, Guardium VA (Vulnerability Assessment), Guardium Data Protection |

Return to How IBM can help

Next page

| Function | Category | Subcategory | IBM Offerings |
|---|---|---|---|
| PROTECT (PR) | Identity Management and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes and devices, and is managed consistent with the assessed risk of unauthorized access. | PR.AC-1: Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes | QRadar SIEM, QRadar UBA, SAM ESSO , SAM, CIS, SIM, PIM, zSecure Admin, IGI, Resilient IRP, Guardium Data Protection, MaaS360 |
| | | PR.AC-2: Physical access to assets is managed and protected | IAM, Resilient IRP, MaaS360, i2 |
| | | PR.AC-3: Remote access is managed | SAM ESSO, SAM, CIS, Resilient IRP, MaaS360 |
| | | PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | QRadar UBA, SAM ESSO , SAM, CIS, PIM, zSecure Admin, IGI, Resilient IRP, Guardium Data Protection, MaaS360 |
| | | PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate | IAM, Resilient IRP, MaaS360 |
| | | PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate | QRadar UBA, SAM ESSO , zSecure Admin, IGI, Resilient IRP, Guardium Data Protection, MaaS360 |
| | Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures and agreements. | PR.AT-1: All users are informed and trained | XF IRIS, Resilient IRP |
| | | PR.AT-2: Privileged users understand roles & responsibilities | PIM, XF IRIS, Resilient IRP |
| | | PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | Resilient IRP |
| | | PR.AT-4: Senior executives understand roles & responsibilities | XF IRIS, Resilient IRP, i2 |
| | | PR.AT-5: Physical and information security personnel understand roles & responsibilities | i2, XF IRIS, Resilient IRP |
| | Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity and availability of information. | PR.DS-1: Data-at-rest is protected | Guardium GDE, MDE, Guardium VA, MaaS360, Guardium Data Protection, SKLM, DAS |
| | | PR.DS-2: Data-in-transit is protected | Guardium Data Protection, SKLM, DAS, SAM, CIS, MaaS360 |
| | | PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition | Guardium Data Protection, BigFix Inventory, zSecure Admin , DAS, MaaS360 |
| | | PR.DS-4: Adequate capacity to ensure availability is maintained | DAS, Resilient IRP |
| | | PR.DS-5: Protections against data leaks are implemented | Guardium Data Protection, Guardium Redaction, Guardium GDE, DAS, MaaS360, i2 |
| | | PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity | QRadar SIEM, Guardium DAM , SKLM, BigFix Inventory, DAS, MaaS360 |
| | | PR.DS-7: The development and testing environment(s) are separate from the production environment | DAS, Resilient IRP |
| | | PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity | DAS, Resilient IRP |
| | Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment and coordination among organizational entities), processes and procedures are maintained and used to manage protection of information systems and assets. | PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g. concept of least functionality) | QRadar SIEM, IBM QRadar Advisor with Watson, QRadar UBA, Guardium FAM , BigFix Inventory, BigFix Lifecycle, BigFix Compliance, zSecure Admin , SSRC, IES, Resilient IRP, Guardium VA, Guardium Data Protection, MaaS360 |
| | | PR.IP-2: A System Development Life Cycle to manage systems is implemented | Guardium FAM , BigFix Lifecycle, BigFix Compliance, BigFix Inventory, DAS, Resilient IRP, MaaS360 |
| | | PR.IP-3: Configuration change control processes are in place | QRadar SIEM, IBM QRadar Advisor with Watson, Guardium FAM, Guardium VA, Guardium Data Protection, BigFix Inventory, BigFix Lifecycle, BigFix Compliance, IES, DAS, Resilient IRP, MaaS360 |

Return to How IBM can help

Next page

| Function | Category | Subcategory | IBM Offerings |
|---|---|---|---|
| **PROTECT (PR)** *(continued)* | Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment and coordination among organizational entities), processes and procedures are maintained and used to manage protection of information systems and assets. | PR.IP-4: Backups of information are conducted, maintained, and tested periodically | IES, DAS, Resilient IRP |
| | | PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met | zSecure Admin , DAS, Resilient IRP, Guardium Data Protection, MaaS360 |
| | | PR.IP-6: Data is destroyed according to policy | Guardium Data Redaction, DAS, Resilient IRP |
| | | PR.IP-7: Protection processes are continuously improved | IES, DAS, XF IRIS, Resilient IRP, Guardium Data Protection, IBM Security AppExchange |
| | | PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties | IES, DAS |
| | | PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | XF IRIS, Resilient IRP |
| | | PR.IP-10: Response and recovery plans are tested | QRadar SIEM, IBM QRadar Advisor with Watson, Guardium FAM , BigFix Inventory, BigFix Lifecycle, SSRC, IES |
| | | PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | QRadar SIEM, IBM QRadar Advisor with Watson, Guardium FAM, zSecure Admin , SSRC, IES, Resilient IRP, IGI, MaaS360, i2 |
| | | PR.IP-12: A vulnerability management plan is developed and implemented | QRadar SIEM, QVRM, IBM QRadar Advisor with Watson, Guardium FAM, Guardium VA, BigFix Patch, BigFix Compliance, SSRC, IES, Resilient IRP, MaaS360 |
| | Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. | PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | MaaS360, BigFix Patch, BigFix Lifecycle, zSecure Audit, IES, Resilient IRP, Guardium Data Protection, IBM Security AppExchange |
| | | PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | SAM, CIS, MaaS360, BigFix Lifecycle, BigFix Patch, zSecure Audit, IES, Resilient IRP, Guardium Data Protection, IBM Security AppExchange, QRadar SIEM |
| | Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures and agreements. | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | QRadar SIEM, IBM QRadar Advisor with Watson, QVRM, zSecure Audit , IES, Resilient IRP, Guardium Data Protection |
| | | PR.PT-2: Removable media is protected and its use restricted according to policy | DAS, Resilient IRP |
| | | PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | QVRM, QRadar SIEM, QFlow, ,QNI, QRIF, PIM, zSecure Command Verifier, Resilient IRP |
| | | PR.PT-4: Communications and control networks are protected | QRadar SIEM, Qflow, QNI, QRIF, QVRM, IES, MaaS360 |
| | | PR.PT-5: Systems operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations). | QVRM, QRadar SIEM, QROC, IES |
| **DETECT (DE)** | Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood. | DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed | QRadar SIEM, IBM QRadar Advisor with Watson, QRadar UBA, QFlow, QNI, QRIF, Agile 3, BigFix Detect, zSecure Command Verifier , SIOC, Resilient IRP, MaaS360 |
| | | DE.AE-2: Detected events are analyzed to understand attack targets and methods | QRIF, QRadar SIEM, QRadar UBA, QFlow, QNI, QRIF, X-Force Exchange API, BigFix Detect, zSecure Alert, MaaS360, i2 |
| | | DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors | QRadar SIEM, QVRM, IBM QRadar Advisor with Watson, X-Force Exchange API, zSecure Alert , SIOC, Resilient IRP, BigFix Detect, i2 |
| | | DE.AE-4: Impact of events is determined | QRadar SIEM, IBM QRadar Advisor with Watson, QVRM, QFlow, QNI, QRIF, Agile 3, BigFix Detect, Resilient IRP, i2 |
| | | DE.AE-5: Incident alert thresholds are established | QRadar SIEM, IBM QRadar Advisor with Watson, Agile 3, X-Force Exchange API, BigFix Detect, zSecure Alert, MaaS360 |

Return to How IBM can help

Next page

| Function | Category | Subcategory | IBM Offerings |
|---|---|---|---|
| **DETECT (DE)** ***(continued)*** | Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. | DE.CM-1: The network is monitored to detect potential cybersecurity event | QRadar SIEM, QFlow, QNI, QRIF, QVRM, zSecure Alert, SIOC, IES, Guardium Data Protection |
| | | DE.CM-2: The physical environment is monitored to detect potential cybersecurity events | QRadar SIEM, Guardium FAM , SIOC, IES, Resilient IRP, i2 |
| | | DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events | QRadar SIEM, IBM QRadar Advisor with Watson, QRadar UBA, PIM, Guardium FAM, Guardium Data Protection, zSecure CV , SIOC, IES, Resilient IRP, BigFix Detect, i2 |
| | | DE.CM-4: Malicious code is detected | QRadar SIEM, IBM QRadar Advisor with Watson, Rapport, BigFix Detect, SIOC, IES, Resilient IRP, MaaS360 |
| | | DE.CM-5: Unauthorized mobile code is detected | QRadar SIEM, QFlow, QNI, QRIF, QRadar Watson Advisor Advisor, MaaS360, IES, Mobile SDK |
| | | DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events | QRadar SIEM, QFlow, QNI, QRIF, QVRM, PIM, Guardium FAM, Guardium Data Protection,  IES |
| | | DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed | QRadar SIEM, IBM QRadar Advisor with Watson, QRadar UBA, PIM, Guardium FAM, Guardium Data Protection, zSecure CV, IES, SAM, CIS, MaaS360, i2 |
| | | DE.CM-8: Vulnerability scans are performed | QVRM, Guardium VA, AppScan Enterprise, AppScan Source, AppScan Standard, IES, Resilient IRP |
| | Detection Processes (DE.Data Protection): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. | DE.Data Protection-1: Roles and responsibilities for detection are well defined to ensure accountability | QRadar SIEM, IBM QRadar Advisor with Watson, QRadar UBA, IES, Guardium Data Protection |
| | | DE.Data Protection-2: Detection activities comply with all applicable requirements | IES |
| | | DE.Data Protection-3: Detection processes are tested | QRadar SIEM, IBM QRadar Advisor with Watson, IES, XF IRIS |
| | | DE.Data Protection-4: Event detection information is communicated to appropriate parties | QRadar SIEM, IBM QRadar Advisor with Watson, QRadar UBA, BigFix Detect, zSecure Alert , SIOC, IES |
| | | DE.Data Protection-5: Detection processes are continuously improved | BigFix Detect, SIOC, IES |
| **RESPOND (RS)** | Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events. | RS.RP-1: Response plan is executed during or after an event | QRadar  SIEM, XF IRIS, Resilient IRP |
| | Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. | RS.CO-1: Personnel know their roles and order of operations when a response is needed | QRadar  SIEM, DAS |
| | | RS.CO-2: Events are reported consistent with established criteria | QRadar  SIEM, zSecure Audit , SIOC, IES, DAS, i2 |
| | | RS.CO-3: Information is shared consistent with response plans | QRadar  SIEM, SIOC, IES, DAS |
| | | RS.CO-4: Coordination with stakeholders occurs consistent with response plans | QRadar  SIEM, IES, DAS |
| | | RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | QRadar  SIEM, X-Force Exchange API, SIOC |
| | Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities. | RS.AN-1: Notifications from detection systems are investigated | QRadar  SIEM, i2, XF IRIS, Resilient IRP |
| | | RS.AN-2: The impact of the incident is understood | QRadar  SIEM, i2, Resilient IRP , Agile 3, XF IRIS, BigFix Detect |
| | | RS.AN-3: Forensics are performed | QRIF, XF IRIS, Resilient IRP |
| | | RS.AN-4: Incidents are categorized consistent with response plans | QRadar  SIEM, Agile 3, zSecure Audit , XF IRIS |

Return to How IBM can help

Next page

| Function | Category | Subcategory | IBM Offerings |
|---|---|---|---|
| **RESPOND (RS)** *(continued)* | Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects and eradicate the incident. | RS.MI-1: Incidents are contained | QRadar SIEM, QRIF, Rapport , MaaS360, IES, BigFix Detect |
| | | RS.MI-2: Incidents are mitigated | QRadar SIEM, QRIF, MaaS360, BigFix Compliance, BigFix Detect, zSecure CV , IES, SAM, CIS, IGI |
| | | RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks | IES, Resilient IRP, Guardium VA, BigFix Detect, QVRM |
| | Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | RS.IM-1: Response plans incorporate lessons learned | Resilient IRP, SSRC, XF IRIS |
| | | RS.IM-2: Response strategies are updated | Resilient IRP , SSRC, XF IRIS |
| **RECOVER (RC)** | Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events. | RC.RP-1: Recovery plan is executed during or after an event | Resilient IRP , XF IRIS |
| | Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities. | RC.IM-1: Recovery plans incorporate lessons learned | Resilient IRP , Agile 3, XF IRIS |
| | | RC.IM-2: Recovery strategies are updated | Resilient IRP , Agile 3, XF IRIS |
| | Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs and vendors. | RC.CO-1: Public relations are managed | THIS CELL OF THE EXCEL DOC IS EMPTY |
| | | RC.CO-2: Reputation after an event is repaired | THIS CELL OF THE EXCEL DOC IS EMPTY |
| | | RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams | THIS CELL OF THE EXCEL DOC IS EMPTY |

Return to How IBM can help

Legal

IBM Security

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
September 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

WGB03045-USEN-00