JEFF PIKE

Foreword by
Sumedh Thakar

LEFT of BOOM

Introducing the ROC

Risk
Operations
Center

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a leading provider of disruptive cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings.

The Qualys Enterprise TruRisk Platform leverages a single agent to continuously deliver critical security intelligence while enabling enterprises to automate the full spectrum of vulnerability detection, compliance, and protection for IT systems, workloads and web applications across on premises, endpoints, servers, public and private clouds, containers, and mobile devices. Founded in 1999 as one of the first SaaS security companies, Qualys has strategic partnerships and seamlessly integrates its vulnerability management capabilities into security offerings from cloud service providers, including Oracle Cloud Infrastructure, Amazon Web Services, the Google Cloud Platform and Microsoft Azure, along with a number of leading managed service providers and global consulting organizations. For more information, please visit **http://www.qualys.com**.

LEFT of BOOM

Introducing the ROC

Risk Operations Center

BY JEFF PIKE

Foreword by Sumedh Thakar

Left of Boom: Introducing the ROC | Risk Operations Center

Published by:
CyberEdge Group, LLC
501 E. Las Olas Boulevard
Suite 300
Fort Lauderdale, FL 33301
(800) 327-8711
www.cyberedgegroup.com

ISBN: 978-1-948939-53-9 (Paperback)
ISBN: 978-1-948939-54-6 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Designer: Colleen R. Abel

Table of Contents

Foreword

Today, security teams identify more cyber risks than ever before across an ever-expanding attack surface that includes on-premises and cloud infrastructures, internally developed and SaaS applications, operational technology, and IoT networks.

However, the more vulnerabilities, misconfigurations, and exposed user identities security teams find, the more they need to fix. There's simply not enough bandwidth to eliminate every potential exposure.

Within the cybersecurity industry, this trend has elevated the vulnerability management discussion to a risk management discussion. Enterprise security teams need to evolve from simply managing attack surfaces to operationalizing risk surface management.

This approach stands in stark contrast to the situation I encountered at Qualys more than 20 years ago. Back then, clients scanned their environments only once a quarter and gave IT teams a full 90 days to fix cyber risks.

Today's cybercriminals have greatly expanded their attack capabilities by leveraging AI. Given the frequency at which malware is unleashed by using AI technologies, our clients now scan their environments every four hours. Their security teams need to mitigate vulnerabilities and misconfigurations at the speed of detection.

To prioritize and remediate risks quickly and efficiently, enterprises must turn risk management into a business conversation based on the anticipated monetary impact of attacks on the organization. This will enable management to allocate resources where they are needed most.

Security teams then need to operationalize their processes so they can mitigate risks before the bad guys exploit them. Everyone on the security team should focus on reducing risk. This effort requires understanding how the business operates and what it needs to maintain and optimize those operations.

Only then can enterprises make smart decisions on what to spend and where to reduce risk.

To understand these business needs in terms of cyber risks, CISOs and their security teams need to collaborate with the CEO, the CFO, and the board of directors. However, reporting on the number of vulnerabilities and the number of applied patches—along with the types of security controls—won't resonate with business leadership. Conversations must pivot to defining risks in dollar terms:

- What's the value at risk?
- What will it cost the company if a risk is exploited?
- How will spending X million dollars on cybersecurity reduce the likelihood of a breach?

Answering these questions is paramount. Not every risk matters. But it's vital to fix the 1% that matter most to reduce the likelihood of a major financial loss.

That's the essence of risk surface management and the concept upon which the Risk Operations Center (ROC) was launched. The ROC is the future of cyber risk management. It aligns technical risk factors to business risks and uses agentic AI to efficiently remediate the riskiest exposures "left of boom," before bad actors launch attacks.

As you will discover in this book, a ROC enables executives and security teams to determine what each risk factor means to the business. The organization can then evolve to an operationalized process for risk management that provides focused findings and identifies what to fix first—through repeatable and well-defined processes.

In a world with millions of fragmented cyber threat exposures, a ROC identifies risks, applies threat intelligence and business context to prioritize mitigation, and then facilitates measuring, communicating, and eliminating major risks. You can't fix everything. But you can de-risk your business by defining the value at risk and determining how much to spend on mitigating, accepting, and transferring risk.

Sumedh Thakar
CEO of Qualys

Introduction

This guide introduces the Risk Operations Center (ROC). A ROC enables enterprises to compare information about digital assets and compile relevant risk factors. From there, the ROC brings in business context for each asset to quantify and prioritize risks. This allows security teams to prioritize and orchestrate mitigation while communicating compliance and risk reduction to executives.

By quantifying the potential impact of security vulnerabilities and cyber threats, a ROC enables organizations to build an effective cyber risk management program that minimizes negative business outcomes. It empowers enterprises to accurately prioritize risk mitigation and invest resources in activities that efficiently protect critical digital assets and business processes "left of boom," that is, before cyberattacks occur.

Chapters at a Glance

Chapter 1, "A New Era in Managing Cyber Risk," the challenges and importance of cyber risk management.

Chapter 2, "Introducing the Risk Operations Center," the ROC concept and how it enhances continuous threat exposure management.

Chapter 3, "Unified Asset Inventory," discovering all assets and visualizing the entire attack surface.

Chapter 4, "Risk Factor Aggregation," consolidating and correlating risk factors from diverse assets.

Chapter 5, "Threat Intelligence Enrichment," leveraging threat intelligence to enrich asset/risk data and layer in exploit availability and targeted geographies.

Chapter 6, "Adding Business Context," quantifying cyber risk and adjusting scores based on business context.

Chapter 7, "Risk Prioritization for Security Teams," how a ROC prioritizes risk mitigation.

Chapter 8, "Risk Prioritization for CISOs and Security Executives," basing cybersecurity investments on the monetary value of business entities.

Chapter 9, "Risk Response Orchestration," automating remediation and collaborating on risk acceptance.

Chapter 10, "Compliance and Executive Reporting," how a ROC ensures compliance readiness with audit trails while providing executives with IT asset risk summaries.

Chapter 11, "Future-proofing Your ROC with Agentic AI," how agentic AI supports the ROC process.

Chapter 12, "Embracing the ROC Concept," why now is the time to deploy a ROC and the steps to develop a plan.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Want to learn more? Follow the corresponding URL to discover additional content available on the web.

Chapter 1

A New Era in Managing Cyber Risk

In this chapter

- Understand the importance of cyber risk management
- Review the challenges hindering successful cyber risk management

The Importance of Cyber Risk Management

The objective of a cyber risk management program is to align cyber risk with business risk in order to minimize negative business outcomes.

A successful cyber risk management program:

- ☑ Enables cybersecurity teams to quantify the impact of security vulnerabilities and threats on the business, so they can prioritize mitigation based on business outcomes rather than technical metrics
- ☑ Empowers security leaders to invest in the activities that best protect the information assets and business processes most critical to their organization's success
- ☑ Allows cybersecurity and IT teams, executives, and business unit leaders to reach consensus on the value of cybersecurity activities and collaborate on risk reduction initiatives
- ☑ Improves and automates processes for detecting and remediating vulnerabilities and security weaknesses to prevent their being exploited

But effective cyber risk management is not simple. It involves multiple elements, as shown in Figure 1-1.

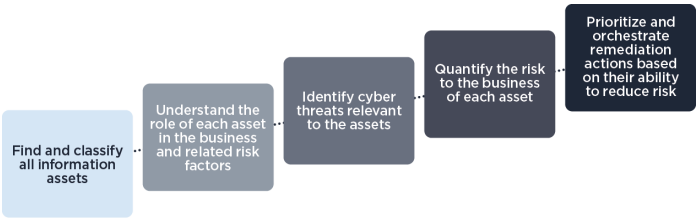

Figure 1-1: The elements of risk management.

Cyber risk management involves gathering and comparing information about assets from across the enterprise, compiling the risk factors relevant to each of them, tying in business context, quantifying and prioritizing the risks, and orchestrating mitigation and other responses. It can also involve communicating about compliance and risk reduction over time to management and other interested parties.

Today's Cyber Risk Management Challenges

Today, most enterprises face difficult challenges when establishing and operating an effective cyber risk management program. They include barriers to collaboration, a dauntingly complex IT environment, business constraints, and, until now, the absence of a systematic process for cyber risk management.

Lack of collaboration across the enterprise

Traditional initiatives to measure, prioritize, and reduce cyber risk frequently fail due to a combination of factors that inhibit collaboration among IT and business functions:

- ☑ Poor communication
- ☑ Lack of resources
- ☑ Unclear objectives
- ☑ Inadequate expertise

Often, cybersecurity teams focus on technical risk management. They ignore operational and financial risks and never reach out to business managers who could provide input on those. In turn, most non-technical managers aren't even aware that they could play an important role in assessing and quantifying the impact of cyber threats on the business.

Also, most efforts at cyber risk management operate in silos. That's because there are no mechanisms to share information and insights across business or functional units, much less to assess and prioritize risks from an enterprise-wide perspective.

The lack of unified risk management and cross-functional collaboration comes at a high cost. These issues:

- ☑ Lead security teams to spend too much time on tasks that have a relatively minor effect on risk
- ☑ Prevent organizations from prioritizing mitigation activities based on risk and investing in security controls and processes with the most impact on reducing risk
- ☑ Make it impossible to develop mitigation and risk reduction metrics that are meaningful for business operations
- ☑ Cause CISOs, CFOs, risk officers, and other business leaders to pursue different risk mitigation goals

To learn more about the cyber risks faced by enterprises, read The Future of Cybersecurity Risk Management white paper.

Complexity and security tool sprawl

According to research by Qualys, large enterprises typically deploy 70 or more security tools. Figure 1-2 lists some of the main categories. These tools usually operate in silos, generating isolated sets of risk metrics and alerts. Without integration, the tools produce conflicting priorities and cannot create a cohesive picture of the organization's overall risk.

Figure 1-2: Fragmented tools add to the complexity of managing cyber risks.

Risk warnings from this multitude of tools can overwhelm security teams as they investigate:

- ☑ Cloud vulnerabilities such as insecure APIs
- ☑ Visibility gaps in operational technology (OT)
- ☑ Third-party integrations with outdated software

Even with so many tools in use, critical data can remain undetected. For example, as Qualys research shows, typical network scans miss 30% of digital assets. Obviously, security teams can't protect what they don't know about.

Don't try to mitigate vulnerabilities without understanding which risks are priorities. Otherwise, security teams will focus on the vulnerabilities that are easiest to find and fix rather than the ones that actually put the organization at financial or operational risk.

Business constraints

Even when business leaders understand the value of cyber risk management, they are often held back by business constraints related to resources, organizational structure, and mindset. Typical issues include:

Limited resources and overloaded teams

Few organizations have the workforce, budget, or time to remediate every risk. Manually reviewing thousands of user and service accounts is impractical. Without a way to quantify which risks matter most—and without automation that unifies identity and asset telemetry to orchestrate responses—security efforts remain scattered, with siloed teams chasing symptoms instead of eliminating root causes.

Reactive vs. strategic decision making

The lack of a unified platform leaves security teams juggling multiple dashboards and operating based on fragmented information. Constant, reactive firefighting leaves little time or bandwidth to prioritize risks based on their impact on business outcomes.

Lack of financial context

The biggest gap in understanding risk is the lack of a connection or link between financial impact and security posture. The absence of risk quantification reduces cybersecurity investments to mere compliance exercises. Risk management solutions may lack the business value required to drive informed decision-making.

Disconnected risk management

As business units operate in isolation—using separate tools, data sources, and prioritization protocols—an incoherent view of the organization's overall risk posture emerges. Executives may have visibility into select areas but lack a comprehensive view to manage risks that span business operations and cybersecurity domains. In addition, identity systems often sit outside this picture, even though they underpin every business process.

Lack of an enterprise perspective.

Without a unified approach to risk management, CFOs may lack integrated cybersecurity insights, leading to mismatched cyber insurance coverage and misallocated budgets. Similarly, CISOs sometimes focus on cybersecurity threats that fail to address the most business-critical risks.

Absence of a Systematic Process for Cyber Risk Management

It is extremely difficult to overcome the challenges described here without a systematic process for assessing and managing cyber risks across a complex enterprise. Unfortunately, until recently, few such processes existed.

This book is designed to fill that need by helping organizations manage cyber risks efficiently and effectively, using the concept of a Risk Operations Center (ROC). This concept integrates asset, vulnerability, configuration, and identity telemetry into a unified process that measures, prioritizes, and orchestrates risk reduction.

The next chapter explains the Risk Operations Center, a function within a cybersecurity organization, and how a ROC platform can operationalize IT asset risk reduction by aligning cyber risk management with business outcomes.

Chapter 2

Introducing the Risk Operations Center

In this chapter

- Understand the concept of a Risk Operations Center (ROC)
- Discover how a ROC enhances Continuous Threat Exposure Management (CTEM)
- Review the key capabilities and benefits of a ROC platform

SOCs Are For "Right of Boom" Security

Today, almost every enterprise of any size employs a security operations center, or SOC, a centralized function that unifies activities for cybersecurity incident detection and response. Typically, a SOC team collects and aggregates alerts and data from a wide range of security tools. They also analyze and prioritize (triage) alerts, initiate and monitor attack containment and mitigation measures, and report activity levels and results to management.

However, SOCs are concerned almost exclusively with what are sometimes called "right of boom" activities; that is, actions that occur after a cyberattack has been detected. Until now, there has never been an equivalent function to help manage "left of boom" activities related to strengthening cyber defenses before attacks occur.

Just as critically, SOCs rarely monitor the conditions that make attacks possible in the first place. These include misconfigured systems, unpatched vulnerabilities, and the expanding identity

attack surface of privileged and service accounts that adversaries routinely exploit.

ROCs: Guiding "Left of Boom" Security

To address these SOC shortfalls, this book introduces the idea of a Risk Operations Center, or ROC, a centralized function to guide activities that strengthen cyber defenses left of boom—before attacks occur and after they have been contained.

Like SOCs, ROCs collect and aggregate security data, analyze and prioritize threats, initiate remediation measures, and provide critical insights and reports to management. But ROCs differ from SOCs in several respects. For example, ROCs:

- ☑ Collect and aggregate data on vulnerabilities and existing security issues, rather than indicators of attacks
- ☑ Focus on analyzing and prioritizing risks to the organization rather than alerts
- ☑ Correlate asset, configuration, and identity risk factors into a single risk score to guide mitigation priorities
- ☑ Provide recommendations and insights on how to patch vulnerabilities, improve security controls, and strengthen the organization's security risk posture—rather than on how to contain ongoing attacks
- ☑ Quantify how improving identity posture and access governance directly reduces risk and overall exposure
- ☑ Guide management on how to invest in cybersecurity staffing and technology to minimize risk and maximize business outcomes

We often visualize a SOC as a large room filled with oversized monitors, with beeping alarms and hushed but urgent conversations among analysts. And many are like that. But a ROC (and indeed a SOC) can be highly distributed, with people participating from remote locations and home offices. Furthermore, a ROC does not need to be a single organizational entity reporting to one manager. The important attributes are a common mindset and a ROC platform (discussed below) to integrate risk management processes across the enterprise.

Speaking the Language of Business

Executives and non-technical managers typically don't comprehend the business value of cybersecurity metrics. It's not enough to tell them that security operations teams found and patched hundreds of vulnerabilities and protected thousands of IT assets.

But executives and managers do understand risk and cost. So, to facilitate communications, security teams need to translate security issues into two metrics:

1. Consistent, enterprise-wide risk scores for IT assets that can be used to compare, rank order, and prioritize business risks associated with each asset.
2. Monetary risk values based on the financial impact of cybersecurity events on key business units and business functions.

An enterprise-wide set of risk scores for both IT assets and identities allows security teams to monitor and protect the assets that are most at risk. Defining risk in monetary terms based on projected business outcomes— complemented by technical risk measurements—enables IT and business managers to work together to find cost-effective ways to reduce risk and set cybersecurity budget priorities.

The goals of a ROC include the ability to ask and answer questions like:

- ☑ Which IT assets are most exposed to attack?
- ☑ Which assets include vulnerabilities that are currently being exploited by threat actors?
- ☑ Which assets are associated with high-value, mission-critical business processes?
- ☑ Which assets support processes that cannot tolerate interruptions?
- ☑ How much money will the enterprise lose each hour a critical business process remains offline?
- ☑ What are the direct and indirect costs if a data breach exfiltrates customer information?

- ☑ What would be the impact of a competitor stealing intellectual property?
- ☑ How much would it cost to reduce or eliminate the risk of events like interruptions, breaches, and data thefts?
- ☑ Which identities—human or machine—have over-privileged access to assets with high business value?
- ☑ How do exposures amplify the risks of lateral movement or ransomware attacks?

By determining a risk score for each IT asset and calculating the monetary risk associated with entities such as business functions and business units, CISOs can communicate in terms familiar to executives and boards of directors, including business risks and the likelihood of financial loss. A single chart, such as the one shown in Figure 2.1, can allow executives and boards to compare the value at risk for assets across key business entities, as well as comparing risk scores and risk appetites (the amount of risk the organization is willing to tolerate) for those entities. (This chart is discussed in more depth in Chapter 8).

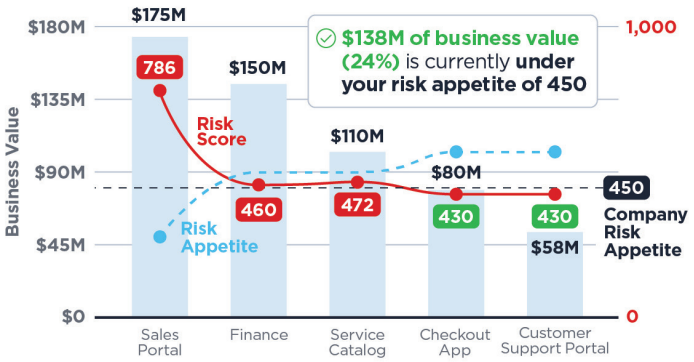

Figure 2-1: A chart for executives and board members showing value at risk, risk score, and risk tolerance for an organization's key business entities.

Finally, with a ROC, security leaders can compare risks defined in monetary terms with the costs of alternative mitigation strategies to make informed decisions about which risks:

- ☑ Should be mitigated with technology
- ☑ Should be transferred to other parties (such as cyber insurance companies)
- ☑ Should be accepted, because the probable impact is less than the cost of mitigation.

Some experts maintain that risk management is about three things: risk mitigation, risk acceptance, and risk transfer. When you evaluate a cyber risk, don't automatically leap on the first technical mitigation strategy that comes to mind. Investigate whether there are alternative technical approaches, if cyber insurance might be the most cost-effective form of mitigation, and if the best course of action might be to accept the risk. A ROC can provide data to help you make the best decision. For example, if the risk score for a business entity falls below the organization's tolerance level, you might want to focus your mitigation activities on other areas.

ROC Activities as a Seven-step Process

At a high level, a ROC organizes and manages four types of activities:

1. Automating security data collection and risk identification
2. Enriching security data with real-time threat intelligence and business context
3. Prioritizing risks based on their potential business impact as well as technical severity
4. Orchestrating risk mitigation actions

At a more granular level, a ROC operationalizes risk reduction by integrating seven sets of activities into a unified process that aligns cyber risk management with business outcomes, as shown in Figure 2-2.

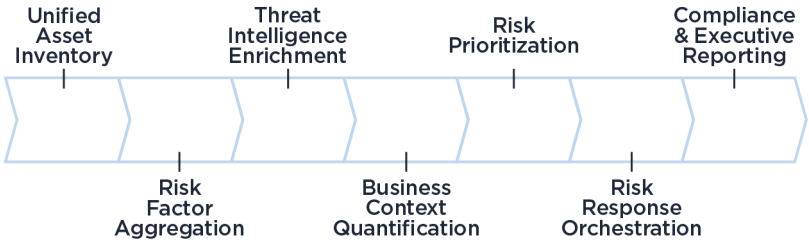

Figure 2-2: The seven steps of a ROC process.

We discuss the seven steps in detail in the chapters that follow. By unifying the security, operational, and financial consequences of cyber risk into one framework, ROCs allow organizations to adopt a holistic risk management strategy. Security teams can quantify business impact, prioritize risks based on criticality, and allocate resources where needed most.

Also, security teams can use the data generated by a ROC to report to executives on their progress in risk reduction and produce audit trails to facilitate compliance with security regulations.

The ROC Platform

We have discussed a ROC in conceptual terms as a function within the cybersecurity organization that helps organizations understand and reduce risk based on business value. But what is the best way to operationalize this idea?

In theory, you could string together a series of standalone security and analytics tools to implement the ROC concept. However, in practice, it makes far more sense to deploy a **ROC platform,** a software solution, to unify, streamline, and automate the data collection, analysis, and orchestration activities we have been discussing.

ROC platform benefits

A ROC platform helps organizations make decisions driven by data and informed by business and financial context. It also enables security teams to continuously monitor and respond to changes in the attack surface. Plus, a ROC can provide proactive risk management capabilities that shift security teams away from reactive firefighting.

By streamlining the management of risk factors—conditions affecting the likelihood that an IT risk will occur or worsen—security teams can cut through the noise of thousands of vulnerability and threat alerts and act on the ones that matter most. And by combining cybersecurity, operational, and financial risks into a single platform, enterprises can synchronize risk management strategies across all departments to prioritize and mitigate risks based on their business impact.

For more insights into how a ROC helps enterprises solve cyber risk management challenges, check out this webinar: the 2025 State of Cyber Risk: Insights, Challenges & the Path Forward.

ROC Business Benefits

Focus resources on high-impact risks
A ROC centralizes and normalizes risk data from across the entire enterprise, enabling organizations to concentrate resources on mitigating risks with the most significant impact on business operations.

Align risk mitigation with business goals
By factoring in business context and quantifying risks with financial metrics, a ROC aligns risk management with business goals. This alignment helps inform decisions about risk mitigation and resource allocation.

Facilitate cross-functional collaboration
By providing data-driven insights and breaking down silos among CISOs, CFOs, risk officers, and other business stakeholders, a ROC helps decision makers collaborate. This collaboration synchronizes enterprise risk mitigation, technology budgeting, and cyber insurance strategies.

Improve security posture and business resilience
With continuous monitoring and risk prioritization capabilities provided by a ROC, security teams can strategically harden the organization's attack surface to improve its security posture and business resilience.

How a ROC Enhances Continuous Threat Exposure Management

The ROC concept also supports Continuous Threat Exposure Management, an attack surface management framework developed by the analyst firm Gartner. CTEM is an integrated, iterative approach to prioritizing and refining security posture improvements. It enables organizations to develop consistent and actionable security plans that business executives can understand and security teams can act upon.

A CTEM program is governed by five core stages (Source: Gartner):

- ☑ Scoping external attack surfaces, SaaS security postures, digital risk protections, and potential threats to critical assets
- ☑ Discovering assets within that scope and their risk profiles
- ☑ Prioritizing mitigation based on the urgency, severity, ability to remediate, and level of risk posed to the organization
- ☑ Validating by using controlled attack simulations to understand how malicious actors could execute on cybersecurity threats
- ☑ Mobilizing to streamline approvals for mitigations by defining communication standards and documenting cross-team approval workflows

A major challenge of operationalizing CTEM is that each stage can require additional tools to properly execute the framework. In contrast, a ROC platform helps implement CTEM by operationalizing the five core stages described by Gartner and unifying risk management activities into a single platform. A ROC also enhances CTEM by assigning monetary values to risks and helping enterprises prepare for audits.

The chapters that follow provide details on the seven steps of the ROC process and how they align cyber risk management with business outcomes.

Chapter 3

Unified Asset Inventory

In this chapter

- Understand the role of unified asset inventory in cyber risk management
- Appreciate the importance of discovering all assets across the enterprise
- See why it's critical to visualize the entire attack surface

Cybercriminals Target Untracked Assets

This chapter and the next seven explore the steps of the ROC process. The chapters demonstrate how each set of activities enables organizations to operationalize risk reduction and align risk management to business priorities.

The first step in the ROC process addresses the challenge of discovering ALL assets across ALL enterprise networks (on premises and in the cloud). With attack surfaces expanding exponentially, security teams often lack full visibility into the many and varied assets running on corporate networks and in siloed environments, including:

- ☑ Public cloud platforms
- ☑ SaaS applications
- ☑ Remote offices
- ☑ Production facilities

- ☑ IoT networks
- ☑ Operational technology (OT) systems
- ☑ Identity management environments

In addition, business units may spin up cloud infrastructures and applications on their own, and local IT teams may expand remote networks with devices that are unknown to security teams. All these untracked assets may have security issues that increase risk to the enterprise.

Even known and managed assets can represent hidden risks when viewed in isolation. Unless security teams have access to the full business context for each asset, such as its users, owner, and role in company operations, they cannot assess the asset's criticality and the business impact if it is compromised.

In other words, for risk management purposes, an asset inventory should show not only the existence of all assets in the enterprise, but also the key context for each of them.

The ROC Approach to Unified Asset Inventory

As shown in Figure 3-1, the first step of the Risk Operations Center process, **unified asset inventory**, discovers assets across all internal and external IT environments. These include corporate headquarters, regional offices, failover data centers, operational technology, and remote worker locations.

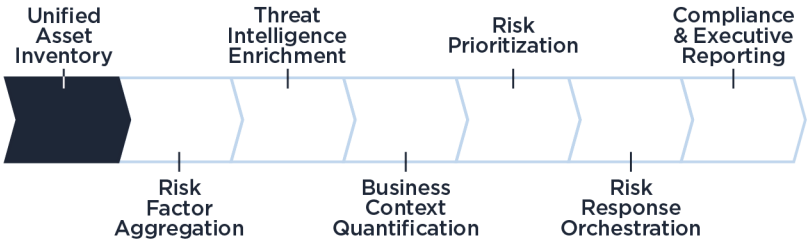

Figure 3-1: Unified asset inventory: The first step for operationalizing a ROC.

Discovery also uncovers assets in external IT environments hosted by third parties, such as cloud services and SaaS application providers, as well as customer-hosted and vendor-hosted infrastructures. Identifying and cataloging all assets allows organizations to view their entire attack surface. It is a prerequisite to mapping and assessing possible negative outcomes from external attacks.

Gain 100% visibility across the entire attack surface—both assets and identities—by building a foundational inventory for risk analysis. Security teams can then prioritize risk mitigation efforts with full confidence that they are focusing their efforts on the entities that matter most to the business.

Continuous Asset Discovery and Classification

A ROC platform enables organizations to solve their asset management challenges by continuously discovering and classifying internal and external IT assets and managing them in a central inventory database. To accomplish this, the ROC platform provides vital asset-tracking capabilities:

- ☑ **360° IT ecosystem discovery** enables security teams to see their organization from an attacker's point of view by identifying on-premises assets, assets functioning on OT and IoT networks, and assets in the cloud.
- ☑ **Credential and non-credential scanning** automatically finds and classifies known and previously unknown assets—ranging from instances to containers, repositories, devices, domains, subdomains, subsidiaries, and business partners.
- ☑ **Configuration management database integration** provides updated views on assets, enriched with business context data such as asset criticality and the data owner.
- ☑ **Tagging and grouping assets** locates security gaps and enables business impact analysis.
- ☑ **Tracking authorized and unauthorized software** proactively manages software lists based on type, location, criticality, and usage.

With these capabilities, enterprises can identify gaps in their asset inventories across their various IT environments. Tracking detailed asset information also facilitates flagging of configuration issues, security risks, IT policy violations, and regulatory noncompliance.

This blog provides more detail about how a ROC facilitates unified asset management: Introducing Cyber Asset Management 3.0 With Enhanced Security Assessment.

Once the security team has captured a complete inventory of IT assets, the next step of the ROC process is to aggregate risk factors for each asset. We discuss this in the next chapter.

Chapter 4

Risk Factor Aggregation

In this chapter

- Understand the need to consolidate risk factors from across diverse assets
- Explore the importance of normalizing and correlating risk factors
- Discover the benefits of generating a unified view of the organization's risk posture

The Top Three Risk Factors

After creating a unified inventory of digital assets, the next step is aggregating risk factors associated with each asset. Aggregation enables enterprises to address the challenge of acquiring and comparing large volumes of risk factor data for assets that live in a wide range of IT system silos.

Risk factors are characteristics of digital assets that increase the likelihood that they will be attacked successfully. These factors can stem from hardware and software issues, human configuration errors, external threats, and conditions in the IT environment. Top risk factors include:

- ☑ Vulnerabilities in software and hardware, especially those rated "critical" and "high"
- ☑ Misconfigurations in applications, infrastructure services, and security tools that make them susceptible to compromise
- ☑ User, admin, and non-human identity accounts that are unused, orphaned (lack a current owner), over-permissioned, or excessively shared

Asset criticality is also an important risk factor. Assets have high criticality when compromise could have a significant negative effect on business operations and performance.

Risk factors are typically obtained from security scanning and application management tools, such as:

- ☑ Vulnerability scanners
- ☑ Identity and access management (IAM) systems
- ☑ Misconfiguration scanning tools
- ☑ SaaS/cloud platform security and management tools
- ☑ Identity provider (IdP) posture assessment tools

However, with risk factor data coming from many sources in many formats, most enterprises are unable to assess and compare asset risk levels outside of their original silos.

To understand the importance of risk aggregation, check out this white paper: Risk Aggregation: How to Aggregate Your Risks and Dependencies.

The ROC Approach to Risk Factor Aggregation

ROC platforms are engineered to continuously aggregate and normalize risk signals from multiple security tools. In this context, normalizing means organizing data in a set of common formats so the information from disparate sources can be compared and analyzed together.

An effective ROC platform can acquire risk factor data from on-premises, cloud, SaaS, and website assets. These include virtual machines, OT and IoT devices, proprietary codebases, and repository codebases.

In addition, risk factors can flow into the platform from cloud agents, passive sensors, agent gateways, container sensors, IAM systems, threat feeds, configuration databases, and penetration testing systems.

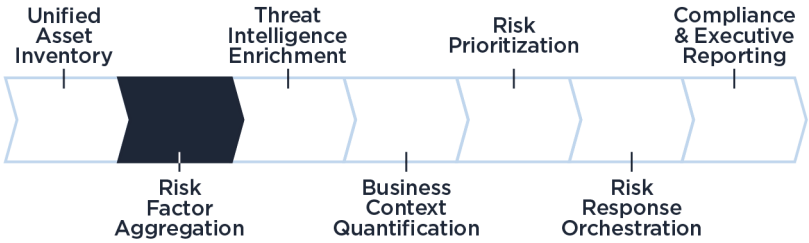

Figure 4-1: Risk factor aggregation: The second step for operationalizing a ROC.

The ROC platform then normalizes and correlates all the risk factor data so security teams can compare risks across internal and external enterprise environments. This process gives enterprises a complete picture of their vulnerability landscape and generates a unified view of risk posture through charts and graphs.

Compiling cloud and web application risk factors

Many organizations struggle to collect risk factor data from assets and resources running in public cloud environments. An advanced ROC platform can give security teams instant visibility across all cloud services and collect metadata from every cloud resource associated with those resources.

A ROC platform can also aggregate risk factor data from enterprise websites. With AI-assisted clustering, security teams reduce the time required to scan critical website areas. This includes scanning APIs to detect deviations from OpenAPI interoperability standards.

Through risk factor aggregation, security teams can identify sensitive data exposed on websites and detect efforts to collect personal information.

The Benefits of Risk Factor Aggregation for Cyber Risk Management

The risk factor aggregation capabilities of a ROC platform support cyber risk management programs by:

- **Revealing the exposure path** of every asset vulnerability to account for factors such as end-of-service software, risky ports associated with external assets, unauthorized software, and missing security agents
- **Identifying technical debt** (end-of-life software, hardware, and operating systems) to determine their associated risks and proactively plan mitigation steps
- **Expanding attack surface coverage** by using passive sensor agents to detect the risks of any network assets missed by scans and API discovery tools
- **Assessing external attack surfaces** to see immediate snapshots of unknown Internet-facing assets and associated risks
- **Identifying newly compromised assets** and network irregularities
- **Providing real-time alerts** on zero-day vulnerabilities
- **Highlighting toxic identity risk** to accelerate hardening of identity postures in alignment with the overall risk assets

The next chapter describes how adding threat intelligence to the ROC process can enrich risk factor data.

Chapter 5

Threat Intelligence Enrichment

In this chapter

- Learn how to leverage real-time, dynamic threat intelligence
- Explore how to enrich asset and risk data by layering in exploit availability and targeted geographies
- Understand the need to determine which vulnerabilities are likely to be exploited

The Role of Threat Intelligence in Cyber Risk Management

After creating a unified inventory of IT assets and aggregating risk factors, enterprises can enrich their analysis with threat intelligence. It's not enough to know that vulnerabilities exist and are associated with risk factors. Security teams also need to ask:

- ☑ Which vulnerabilities and security issues will cybercriminals most likely exploit?
- ☑ What vulnerabilities are no longer just theoretical risks but are currently being exploited in the wild?
- ☑ How do the threats against the organization's critical assets align with its risk tolerance?

Unfortunately, many organizations do not have the tools to answer questions like these.

To understand external threats, security teams have traditionally relied on the static information provided by multiple intelligence feeds. However, these feeds can't keep up with the ever-evolving AI-enhanced attack techniques.

Adding to these challenges, many organizations can't integrate threat intelligence feeds with internal risk models. This makes it nearly impossible to efficiently ingest and quickly analyze the threat information.

In the end, enterprises often cannot answer the critical question: Which threats will most likely hit us today?

The ROC Approach to Threat Intelligence Enrichment

To take on the challenge of static threat intelligence, the third step of the ROC process, **threat intelligence enrichment**, enhances asset and risk data by collecting real-time threat intelligence from multiple feeds.

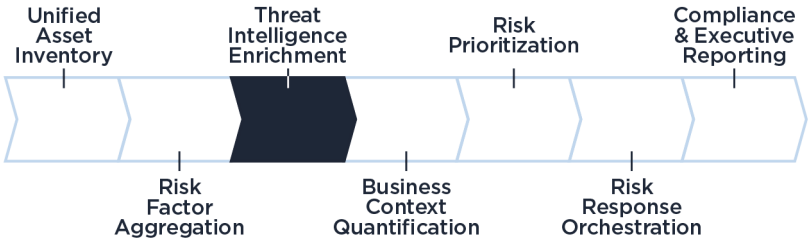

Figure 5-1: Threat intelligence enrichment: The third step for operationalizing the ROC concept.

In addition to alerting security teams about current threats, a ROC platform integrated with threat intelligence can provide information on exploits currently targeting similar enterprises and the geographies where they are being used.

A ROC platform can also correlate external threat data with vulnerabilities and the IT asset inventory. This helps security teams look for specific assets and vulnerabilities susceptible to threats by enabling ad hoc queries of threat intelligence data by using multiple variables and criteria.

In addition, security teams can filter and fine-tune query results and feed them into dashboards that display real-time trends. Even with the thousands of threats disclosed annually, the security team can easily grasp which ones pose the greatest risk to the organization at any given time.

To see what a ROC platform is capable of, examine its dashboards. You should find customizable graphs and charts that provide comprehensive views of the threat landscape in real time. You should also find out if the platform creates views for different roles and breaks down vulnerabilities by threat indicator types.

Preventing Breaches Before They Impact Business Operations

A ROC platform provides real-time threat intelligence capabilities that help security teams prevent breaches by:

- ☑ Validating and rating new threats from external intelligence feeds
- ☑ Displaying the latest vulnerability disclosures
- ☑ Mapping threats to specific IT assets
- ☑ Enriching identity risk posture with threat actor behaviors

With this information, security teams can see the number of assets affected by each threat and drill into the asset details.

Security teams can also use a ROC with embedded AI to surface predictive threat trends and forecast what cybercriminals will do. By continuously correlating external real-time threat intelligence with security gaps in the IT environment, this in-depth, actionable intelligence allows a proactive focus on active threats with known exploits.

For an example of the key role threat intelligence feeds play in reducing risk, read this blog: Responding to Zero-Day Vulnerabilities: Detection and Mitigation.

The Role of Threat Intelligence Enrichment in Cyber Risk Management

By tapping into threat intelligence feeds, a ROC can analyze real-time threat indicators, assess the danger levels of vulnerability types, and detect toxic combinations of risk factors. The information can include:

- Zero-day vulnerabilities susceptible to active attacks in the wild
- Public exploit vulnerabilities for which exploit code is available
- Vulnerabilities attackers can propagate laterally across a network
- Vulnerabilities attackers with few skills can target successfully
- Vulnerabilities that can lead to massive data losses if exploited
- Denial-of-service vulnerabilities that crash compromised systems
- No-patch vulnerabilities (the vendor does not offer a fix)
- Malware vulnerabilities associated with malware infection
- Vulnerabilities for which threat actors have made an exploit kit

Turning Risk Signals into Actionable Insights

The threat and misconfiguration analysis enabled by a ROC can simplify the detection of remotely exploitable vulnerabilities. Risk indicators include devices and software that have reached end of life/end of support, unauthorized or missing titles, and missing required software.

Security teams can also combine threat and vulnerability data with internal criteria, such as the role of an IT asset. This helps prioritize remediation by showing all threat indicators for vulnerabilities and allowing them to drill down into specific vulnerabilities behind a threat indicator.

Enriched, real-time threat intelligence turns risk signals (signs of a breach or a failed security control) into actionable, business-relevant insights. As security teams understand which vulnerabilities are being exploited, they can make informed decisions about remediation.

In the next chapter, the ROC platform quantifies risk by considering the business context of each IT asset.

Chapter 6

Adding Business Context

In this chapter

- Learn how a Risk Operations Center quantifies cyber risk for each IT asset by adding business context
- See how a ROC platform uses tagging to classify IT assets and adjust asset risk scores based on business context

Business Context: A Prerequisite for Prioritizing Risks Accurately

Within the realm of cyber risk management, business context refers to the role an IT asset plays within an enterprise. Business context includes information about the functions the asset performs and how critical those functions are to business operations.

Consider a server that hosts an online customer payment application, which allows customers to check out once they finish shopping. For an e-commerce company, an attack that disables that server for an hour would have a major impact on revenue. Therefore, the business risk associated with the asset is much greater than the technical characteristics of the server alone would imply.

A ROC should take the business context into account and give that server a high risk score relative to other, technically identical servers that are less critical to business operations. For example, the impact of losing an hour of processing from a back-office server managing employee profiles for the human resources department would be far less. This context must be quantified and scored—not assumed.

Without business context, security teams can't map risks to business outcomes or assess the actual impact of attacks. However, most organizations lack the ability to add meaningful business context to tens of thousands of assets in their IT asset inventory and maintain that information over time as new assets are added.

The difficulty of applying business context to assets

Most organizations today maintain an asset inventory database. Unfortunately, they have no practical means of applying business context to risk assessments of the thousands (or tens and even hundreds of thousands) of IT assets they manage. Doing that requires addressing the challenges in ways that are highly scalable and not burdensome to security and IT operations teams.

Those challenges include specifying how business context should be used to increase (or decrease) the risk scores of assets. Enterprises also need to map each user identity to business-critical systems, sensitive data, or privileged actions.

Without business context, risk scoring remains incomplete or biased toward what is easiest to measure rather than what matters most.

The ROC Approach to Prioritizing Risk Using Business Context

After enterprises identify IT assets, aggregate risk factors for each asset, and factor in threat intelligence, the next step in the ROC process is to capture business context relevant to each asset (see Figure 6-1).

How can enterprises add business context to the ROC process? By tagging and classifying IT assets and adjusting the risk scores of asset classes.

Tagging involves affixing unique identification labels to IT assets such as servers, desktops, network devices, and application containers. The tags record key technical attributes and business context information about each asset.

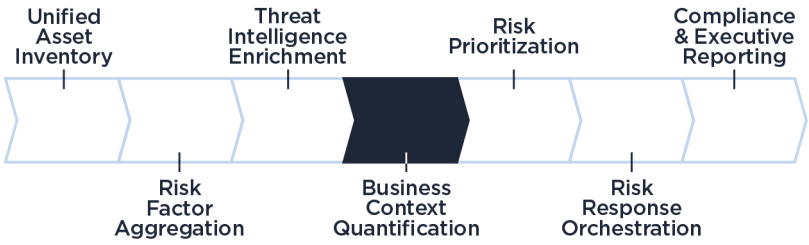

Figure 6-1: Adding business context, the fourth step in operationalizing the ROC process.

Technical attributes for hardware devices could include model number, operating system, IP address, and open ports. Software workloads might be the application name, version number, and known software vulnerabilities.

Business context attributes may indicate function, geo location, business unit, or asset owner. Additional attributes could describe characteristics, such as cloud agent, Internet-facing asset, or a passively sensed asset.

Enterprises can also create attributes to indicate the assets that belong to business entities, such as major applications or functions. Business entities and their use for risk assessment will be discussed in Chapter 8.

Using tags to associate context with assets

By using tags with attributes for technical attributes and business context, security teams can filter and group assets to create categories relevant to the organization's business. For example, they might want to create categories for:

- ☑ Specific-type hardware devices and software apps
- ☑ Assets used by business units
- ☑ Internet-facing assets containing specific types of sensitive data, or support key business processes
- ☑ Identities with weak security (e.g., no multi-factor authorization or default passwords)

Customizing risk scores based on business priorities

When asset tagging is complete, security teams can use a ROC to adjust the risk scores of assets based on business context. For example, they could increase the risk scores of:

- ☑ Assets belonging to the business unit(s) that produce the most revenue for the organization
- ☑ Assets in geographical regions subject to higher levels of attack
- ☑ Software applications supporting the organization's most critical business processes
- ☑ Asset types known to be under attack in similar organizations (e.g., SolarWinds Orion devices)
- ☑ Dormant identities with privileged access
- ☑ Service accounts of unknown ownership with production-level access

Security teams can also use tags to adjust asset risk scores based on industry- and technology-specific factors. While an e-commerce company would prioritize security for Internet-facing devices and applications, a manufacturing company might prioritize security for production and logistics entities. A technology company could focus on product development systems. In industries like healthcare or finance, identities tied to compliance (e.g., HIPAA, SOX) or fraud vectors might receive elevated scores.

In addition, a ROC gives security teams the flexibility to prioritize security for assets that meet multiple criteria, e.g., an exploitable vulnerability + Internet-facing + part of a critical business entity. The prioritization formula can be based on combined factors, as discussed in Chapter 7.

Make sure your ROC platform syncs with ITSM tools and configuration management databases. Synchronization allows asset tagging data to flow into your ROC in real time.

The next chapter examines how a ROC platform helps security teams prioritize day-to-day remediation based on the business criticality of each IT asset.

Chapter 7

Risk Prioritization for Security Teams

In this chapter

- Learn about the two primary use-cases for which enterprises require cyber risk prioritization
- Find out about the flaws of common risk scoring systems
- Understand how a ROC generates comprehensive risk scores to prioritize day-to-day risk mitigation

Prioritizing Cyber Risks Before Attackers Exploit Them

Prioritizing IT risks involves assessing and ranking risks based on the potential impact on operations and the likelihood of occurrence. Given the overwhelming potential threats and vulnerabilities, applying prioritization is vitally important—particularly for two use-cases:

1. To help security teams effectively manage day-to-day risk mitigation activities that address imminent threats to IT assets.
2. To help CISOs and business executives plan and manage technology investments and resources that will reduce long-term risk for the organization.

Prioritization in these two areas—based on risk factors, threat intelligence, and business context—ensures enterprises resolve the most critical cyber risks first. Otherwise, enterprises could waste capital and valuable resources on reducing IT asset vulnerabilities that don't play a critical role in business operations.

This chapter examines the challenges security teams face in managing risk mitigation and how a ROC can help them prioritize their activities. The next chapter covers the risk prioritization challenges that CISOs must contend with and how a ROC makes it easier to plan technology investments and manage resources.

Common scoring systems lack business context and priorities

To decide which IT assets need to be investigated or remediated first, many security teams rely on the Common Vulnerability Scoring System (CVSS). Created by the Forum of Incident Response and Security Teams, the framework rates the severity of vulnerabilities. The CVSS also provides information on ease of exploitability and the extent of vulnerabilities enterprises face from a technical standpoint.

However, these scores do not account for business context or the priorities of different organizations. In fact, technical scoring systems like CVSS can be extremely misleading. For instance, a vulnerability with a medium CVSS score on a mission-critical website server can represent a much greater risk to the organization than a vulnerability with a high score on a non-critical IT asset such as a printer.

True risk scoring needs to go beyond technical severity. Enterprises should rank risks by their potential business impact so assets that carry the highest financial and operational importance drive the risk mitigation agenda.

Varying alert protocols difficult to prioritize

With IT asset vulnerability and threat data coming from so many sources, it's difficult to reconcile the prioritization protocols of various security tools. Each system uses a different set of warning images.

If one tool labels an alert with a <Red> warning while another applies a <High> alert, how does the security team know which one is more critical?

This problem occurs even when multiple tools use the same <Red-Yellow-Green> or <High-Medium-Low> status ratings.

A <Yellow> or <Medium> warning for one tool may equate to a <Red> or <High> warning from another.

Another problem created by scoring systems like the CVSS is the overload of issues labeled as <Critical>. Security teams become overwhelmed by urgent alerts that may not matter all that much. Analysts and other security experts, whose skills and expertise could prevent high-impact attacks, end up wasting their time on low-impact issues.

The ROC Approach to Risk Prioritization for Security Teams

The fifth step in the ROC process, **risk prioritization**, measures the cyber risks of IT assets based on risk factors, threat intelligence, and business context.

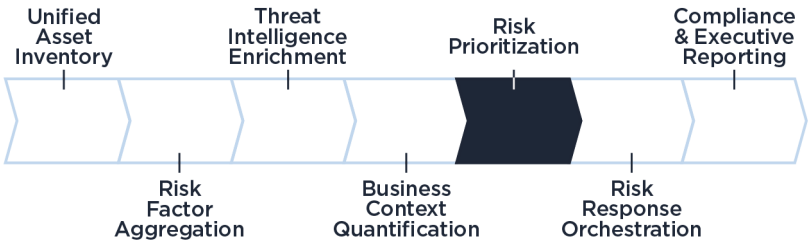

Figure 7-1: Risk prioritization: The fifth step for operationalizing a Risk Operations Center.

A ROC platform offers three capabilities that can dramatically improve security teams' ability to prioritize response and remediation activities based on business risk:

1. Generating risk scores for thousands of assets that are informed by a wide variety of internal and external risk factors
2. Allowing security teams to tailor risk scoring to reflect the situation and business priorities of their specific enterprise
3. Providing security teams with detailed context to understand the factors behind asset risk levels

Generating Comprehensive Risk Scores to Prioritize Assets

A ROC platform can automatically generate risk scores for thousands of IT assets, informed by the risk factors and data captured during the previous ROC phases.

These comprehensive risk scores provide a highly accurate reflection of the criticality of vulnerabilities and security issues. The scores also give security teams a single, consistent scale with which to rank the risks associated with every IT asset across the enterprise.

Internal technical information on risk factors

A ROC platform can pull in a wide variety of information from existing security, IT operations, and cloud management scanners and tools to assess the technical severity of risk factors applicable to IT assets. Risk factors associated with a specific asset might include data about potential vulnerabilities, malware, and misconfigurations that could lead to compromised devices and applications.

In addition, a ROC platform may be able to weigh many of these factors based on information about the presence or absence of mitigating controls. For example, a device susceptible to certain types of malware may represent a higher or lower risk depending on whether it is protected by an effective anti-malware solution.

Threat intelligence

ROC platforms can also incorporate threat intelligence into risk assessments. The classic example is adjusting the risk score of an asset subject to a potential vulnerability based on whether that vulnerability is theoretical (i.e., a researcher has identified the vulnerability), but there is no evidence that it has ever been exploited.

Other conditions that may warrant adjusting risk scores include exploit kits available on the web, evidence that a vulnerability has been exploited by threat actors, and attacks based on a vulnerability that are trending upward.

Business context

As discussed in Chapter 6, business context should have a major impact on the risk assessment of IT assets. In many cases, business context is organization-specific and needs to be determined by the security team, sometimes with assistance from business managers (a situation discussed below). However, a ROC platform can generate pre-defined rules that factor in some business context automatically, even without security team input.

Certain applications are almost always mission-critical and contain sensitive information: financial and accounting systems, human resources applications, order processing systems, and software code repositories. A ROC platform may be able to increase the risk scores of these systems or assets belonging to these systems, "out of the box."

Risk scores that enable prioritization across silos

One of the greatest limitations of most risk management programs is that prioritization can only be performed separately within individual technology silos. Not only does each domain have its own tools and metrics for risk scoring and prioritization, but the assessments are also based on a handful of risk factors familiar to practitioners in each area.

A compelling reason for creating a ROC and deploying a ROC platform is the ability to utilize a wide range of risk factors consistently in every domain—so the resulting risk scores can be used to create rankings and make comparisons across silos. For the first time, security and IT operations teams can feel comfortable moving from "let each domain take care of its own top risks" to "let's look across the enterprise and put more emphasis on risks that could have the biggest impact on the business as a whole."

Tailored Risk Scoring

There is value in creating and managing comprehensive risk scores for thousands of IT assets. But a ROC platform can go further by enabling security teams to adjust scores to reflect

the peculiarities and priorities of their enterprise, at scale, and with relatively little effort. This capability is provided by enabling security teams to adjust risk scores of IT assets up or down, based on attributes in their tags.

Case in point: a security team in healthcare needs to prioritize the security and availability of IT assets involved with protected health information (PHI) and other data covered by HIPAA. These assets must function continuously—interruptions could mean life-or-death, and they are essential for maintaining compliance with specific government regulations and industry standards.

If all these IT assets are stored in an database and tagged with attributes showing they belong to one or more of these categories, then a ROC platform can give security teams the ability to say, in effect: "Bump up the risk score of assets with a PHI tag by XX%, assets with a continuous operation tag by YY%, and those with a compliance tag by ZZ%."

Identifying toxic risk

Security teams can use a ROC to find and prioritize assets with multiple risky attributes. A system admin could ask the ROC to list assets containing exploitable vulnerabilities, exposing access to unauthorized users, and serving critical functions. If all three criteria are met, the admin can label assets as <toxic risk> and assign a top mitigation priority.

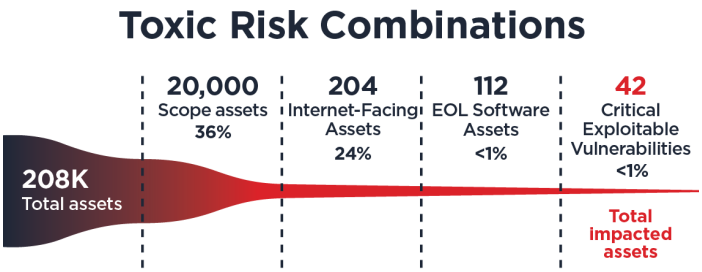

Figure 7-2: ROC dashboard showing toxic risk combinations.

Context and Comparisons

Obviously, the ability to rank and filter thousands of IT assets across an enterprise by risk score is extremely valuable. But advanced ROC platforms can build on that capability to help security teams even more—by providing context on the risk factors for each asset and the ability to aggregate and compare risks for groups of assets.

Drilling into risk factors assets

A ROC platform may be able to show security teams what assets pose the greatest risks to their organization. But the platform may also allow them to drill into why an asset is vulnerable and important. The ROC solution accomplishes this by presenting the risk factors underlying the risk score.

In this case, a security analyst might note an asset has a high risk score and want to know why. The answer might be that the asset is part of a mission-critical system, required to ensure PCI compliance, or subject to a vulnerability that has a high CVE score and is trending recently.

The ROC platform could provide additional context, such as which malware is being used to exploit a vulnerability and which threat actors are known to be attacking it. This information can help security teams decide not only what to prioritize for action, but also what investigative and remediation actions might yield the best results.

Detecting high-risk patterns

A ROC platform can identify patterns that will help determine what types of actions might have the greatest impact in reducing the risk for groups of high-risk assets. It may turn out that a high percentage of Linux servers with high risk scores have the same type of misconfiguration.

Or…many of the web servers in a specific business unit have old operating system versions and expired certificates. These findings would suggest that actions could substantially reduce the risk scores of many similar assets in critical areas of the organization.

Tracking trends

A ROC platform can allow security managers to track trends showing changes in security issues and risk scores over time. In addition to potential risk reduction opportunities (see Figure 7-3), a dashboard widget might show vulnerabilities appearing more (or less) frequently in various asset types, and how risk scores are falling (or rising) in different business units. Trend charts and data help security teams identify emerging threats and show progress over time, strengthening the organization's risk posture. In addition, spikes in new admin assignments or trust changes can signal heightened identity risk even before indicators of compromise appear in assets.

Name	Scope	Applied Filters	Potential Risk Reduction	Impacted Assets	Impacted Findings
Risk Reduction for Sales Portal	SP	8	811 → 700	1	202
Sales Portal Risk Workbench	SP	3	701 → 560	1	208
Cloud Infra	SP	3	701 → 560	1	210
Highest Risk Reduction	SP F +1	8	502 → 421	1	281
CISA KEV	SP F +1	4	478 → 328	2	158
Focus on Essentials (Demo)	SP	5	885 → 682	4	1.01K

Figure 7-3: ROC screenshot showing potential risk reduction opportunities for a sales portal and its cloud infrastructure.

Read this blog to learn more about How To Prioritize Vulnerabilities in a Modern IT Environment.

The next chapter demonstrates how the ROC platform enables CISOs to prioritize plans for investing in technologies and allocating security resources to reduce risks across the enterprise and its business entities.

Chapter 8

Risk Prioritization for CISOs and Security Managers

In this chapter

- Learn the importance of basing cybersecurity investments on the monetary value of business entities
- Find out how to prioritize risk reduction plans
- Understand the value of communicating projected risk reduction outcomes across the enterprise

Focusing Risk Reduction on Critical Business Entities

Prioritizing IT risks involves assessing and ranking them based on the potential impact on business operations and the likelihood of occurrence. This chapter examines how prioritization helps CISOs and other security executives allocate resources and plan investments to reduce risk for business entities and the organization as a whole.

Success in this mission ensures enterprises focus their capital and cybersecurity resources on reducing risks for IT assets that play a critical role in their business operations.

Making big decisions with less information about risk

CISOs make prioritization decisions at a level different from the security team members discussed in Chapter 7. Rather

than determining what individual assets or asset types need attention in the coming days or weeks, they primarily concentrate on allocating resources across security domains and business units over quarterly and annual timeframes.

While CISOs make fewer prioritization decisions than their security teams, many of the decisions have a profound impact on the risk posture of the enterprise. And CISOs typically have less information than their subordinates about the impact of their decisions on business outcomes.

Struggling to communicate

CISOs have bosses too, and they often struggle to communicate with the CEO and board of directors. Non-technical executives typically can't comprehend what it means to the business if firewalls block a million threats a day or if a security team installs 400,000 patches a month.

Executives certainly won't know if those stats signify the enterprise is managing cyber risks in line with company requirements. That makes it difficult for CISOs to obtain budgets to keep their enterprises safe from cyberattacks.

When CISOs want to explain cybersecurity activities, budgets, and proposed investments to the CEO and board members, they need metrics that are tied to concepts that the higher-ups understand and care about: the business impact of security spending on business risks, or, to put it another way, the likely reduction in monetary losses.

The ROC Approach to Prioritization Planning

One proven ROC methodology to facilitate the prioritization of cybersecurity spending options takes CISOs and other security executives through a process spanning six steps:

#1 – Define business entities

The process to prioritize cybersecurity spending options begins with defining business entities—IT systems, operational processes, functional units, geographical areas, or any organizational grouping of software and hardware assets.

This definition step includes listing all the valuable IT assets for each business entity, such as applications, application interfaces, databases, servers, networking gear, and other software and hardware components. It should include the identities (human and machine) with access to those assets, including their associated roles and entitlements. The definition process also identifies who "owns" the business entity and who manages its IT assets.

#2 – Set risk appetite thresholds

The second component in prioritizing cybersecurity spending options sets a risk appetite for each business entity—the threshold level of cyber risk that the organization is willing to accept. A ROC platform can provide prompts to help security executives define the boundaries of acceptable risk exposure.

Risk appetite levels can be established according to industry benchmarks. Security executives can then adjust these appetites through a combination of discussions with business unit leaders and consideration of what each business entity means to the operations of the organization.

#3 – Calculate risk scores

Next in the prioritization process is calculating risk scores for each business entity. The ROC platform automatically creates risk scores for a business entity by rolling up the risk scores of the IT assets supporting it. Security executives can customize the risk score of a business entity by adjusting the scores of the IT assets associated with it.

#4 – Generate monetary values

For the fourth step of the cybersecurity planning prioritization process, the ROC platform generates a monetary value for each business entity based on the business context of IT assets. The monetary valuation should account for operational downtime, data loss, and the potential impact of unauthorized identity access to these IT assets. The asset risk scores roll up into a dashboard view of the risk score for each business entity.

#5 – Compare risk scores to risk appetites

A ROC dashboard might also provide a comparison of risk scores to risk appetites so security executives can see where the biggest gaps are. Enterprises can see risk levels and risk appetites across the organization by business entity. As security executives plan technology investments and resource allocation, they can drill into data curated by a ROC to see top vulnerabilities and threats contributing to business entity risk scores and how risks trend over time.

#6 – Compare entity monetary values and risk profiles

One of the most powerful capabilities of a ROC platform is comparing monetary values, risk scores, and risk appetites for business entities. Charts like Figure 8-1 can answer questions that are especially important to executives and members of the board of directors, including "is the business value at risk across the organization within our acceptable tolerance level?"

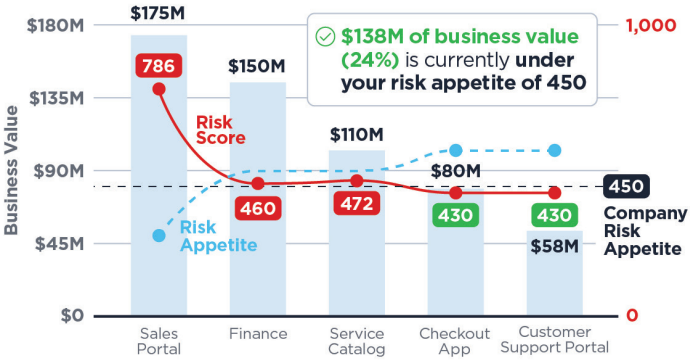

Figure 8-1: ROC dashboard view displaying the business value, risk score, and risk appetite of business entities.

For example, which entities have the greatest monetary value? Are the risk scores of the highest-value business entities high or low relative to others? For each business entity, how does the risk score compare to the risk appetite? The answers

to these questions have powerful implications for security planning and investment. All other things being equal, most security investments should be directed to the business entities with the highest monetary values.

However, a high-value business entity with a low risk score relative to its size (meaning it is comparatively well defended) may merit less additional investment than an entity with a lower business value but a higher risk score (meaning it has serious gaps in security). Risk appetites can also affect assessments. Entities with low risk appetites have less margin for error. They should be a higher priority than entities with high risk appetites.

Analyzing Which Assets and Risk Factors Contribute Most to Risk

Security executives may want more guidance on where to focus security activities. A ROC can present assets (hosts, databases, apps, servers) and risk factors (vulnerabilities, misconfigurations, weak credentials, exposure to the Internet, unsupported OS and software versions, toxic privilege combinations, inherited group access) that contribute most to risk scores, as shown in Figure 8-2:

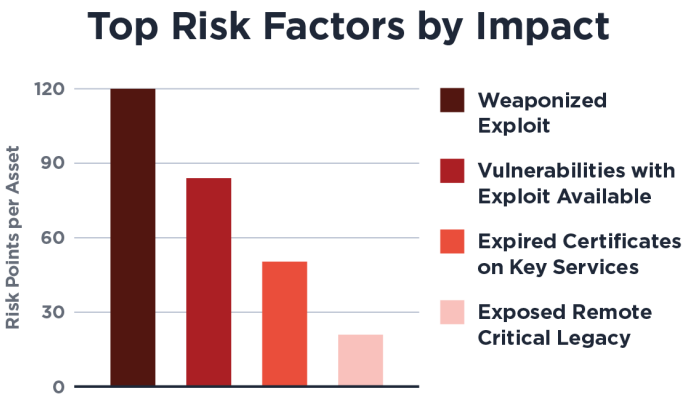

Figure 8-2: Screenshot of risk factors ranked according to their potential impact.

Exploring factors contributing to risk scores with business leaders, security executives can assess the potential risk consequences to guide decisions on mitigation strategies.

It is especially important that executives weigh the impact of identity security on business entity risk. If a critical business unit depends on identities that are misconfigured, overpermissioned, or stale, that entity's true exposure and risk level will be understated. Adding to the challenge, identity signals are often not readily visible to executives.

Transforming IT Risk into a Shared Business Challenge

When viewing risks in technical terms, organizations almost always assign mitigation to IT. This decision precludes non-IT approaches to risk reduction that are more cost-effective than investing in more security controls. This is especially true for identity risk, where remediation often requires input from application owners and business units to adjust permissions, retire accounts, or redesign access workflows.

Non-IT approaches to risk reduction include user training, cyber insurance, and transferring risks to third parties. Sometimes, the cost of mitigating risks may exceed the expected value of the reductions. In that case, the business units must agree to accept the risk.

Quantifying risks with a ROC allows stakeholders to understand the potential consequences for each risk. The ROC also provides insights into how to mitigate risks economically. Ultimately, this helps determine actions that balance the costs and benefits of risk reduction activities.

This approach also transforms IT risk into a shared challenge. Mutual understanding across cybersecurity, IT, and executive teams enables data-driven prioritization for reducing IT risks. Everyone gains awareness and agreement on where the greatest risks lie and what to do about them.

The next chapter demonstrates how the ROC platform enables security teams to orchestrate and automate their risk reduction workflows.

Chapter 9

Risk Response Orchestration

In this chapter

- Understand the challenges of remediating IT assets
- Learn how automation and connected tools accelerate remediation workflows
- Discover how security teams can collaborate with business leaders on risk acceptance

The Key Elements of Orchestrating Risk Response

Orchestration refers to the automated coordination and management of processes. In the context of risk operations, orchestration streamlines remediation. This is the process of reducing potential security risks by patching software, removing vulnerabilities, fixing misconfigurations, applying new security controls, and mitigating other security issues.

Orchestrating risk reduction processes allows security teams to work more quickly with less effort. They can use the actual risk of IT assets as a guide to prioritize activities.

Orchestration also allows a ROC to bring remediation processes together while integrating multiple systems and tools. This allows enterprises to quickly remediate vulnerabilities and reduce or eliminate the time available to threat actors to launch attacks.

The Challenges of Remediation

Remediation presents multiple challenges. Given the speed at which threat actors unleash attacks, manual remediation takes too long.

In addition, remediation processes typically require coordination among multiple security and IT operations tools. These tools need to pass data and process status information to each other. This places a burden on either the enterprise or its security solution vendors to integrate the tools and maintain the integration over time.

Identity remediation presents additional challenges. Privileges are often accumulated slowly, over time, not through a single configuration change. In addition, service accounts may inherit access they no longer require, and when users change roles, their entitlements are rarely reduced.

This identity drift is rarely patched in the traditional sense. In addition, if remediation processes are not well-defined, their effectiveness can degrade. Without documented flows and clear objectives, teams often default to patching and nothing more—ignoring other types of remediation.

The ROC Approach to Risk Response Orchestration

With the sixth process step, **risk response orchestration**, the ROC resolves the challenges of remediation by supporting two types of orchestration. This includes day-to-day risk mitigation activities as well as processes for gathering data and identifying alternatives for planning, resource allocation, and investment in security technologies and staff, and for analyzing and documenting compliance.

The orchestration of day-to-day mitigation activities primarily involves supplying accurate risk scores to patch management tools, IT service management (ITSM) systems, DevOps pipeline tools, and other remediation solutions. These scores allow security teams to prioritize remediation activities based on actual risk to the organization.

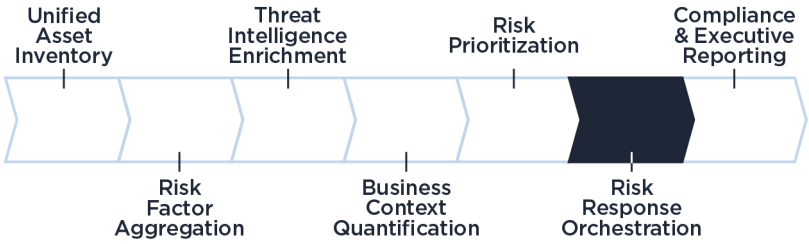

Figure 9-1: Risk response orchestration: The sixth step for operationalizing a Risk Operations Center.

We discuss this type of orchestration in this chapter. We cover orchestration of processes that support executive reporting, planning, and compliance in the next chapter.

The power of orchestration

All orchestration solutions are designed to replace manual tasks with automated processes that are faster, more reliable, and less susceptible to human error. Orchestration tools provided by a ROC platform deliver those benefits.

In addition, using a platform designed for ROC operations offers unique opportunities to employ comprehensive risk scores and asset risk rankings to prioritize remediation activities. A ROC platform can also provide asset attributes and vulnerability context to systems and security team members to facilitate better remediation decisions. With these capabilities, security teams can implement remediation plans to achieve management objectives or systematically reduce business risk in certain areas.

Orchestration Playbooks

A ROC platform integrates prioritized risk scores with remediation workflows. This ensures orchestrated processes first address vulnerabilities and threats that pose the greatest risk to the organization.

The key to this form of orchestration is automated playbooks—pre-defined, machine-driven workflows that execute steps to detect, analyze, contain, and remediate security incidents. In addition to enabling more efficient responses, playbooks reduce human errors and workloads.

Within a ROC, orchestration playbooks typically specify conditions that trigger remediation workflows and the data to be passed between tools. The playbooks also specify actions to be taken by the tools, and the results and status information to be reported by the tools.

Let's examine how some risk orchestration processes might be organized by playbooks.

Workflow triggers

A security team might want remediation workflows to be triggered by events such as:

- ☑ Detection of assets with risk scores exceeding a specified threshold
- ☑ Detection of assets with certain risk factors (e.g., a specific vulnerability or misconfiguration)
- ☑ Planned remediation activities (e.g., a weekly patching run)
- ☑ An alert that a type of asset or mission-critical system has been compromised or is under attack somewhere in the enterprise
- ☑ Input by a security or IT operations team member
- ☑ A request to execute a remediation plan (discussed below)
- ☑ Detection of identities with privilege levels that exceed policy for the business entity they support

Data and actions

A ROC playbook typically specifies data to be passed to remediation tools and the actions those tools are expected to perform. This data might include:

- ☑ A list of assets to be patched during the next patching cycle and the patches to be used
- ☑ ITSM tickets with information about assets to remediate, specific actions to take, and the priority level of the requests
- ☑ Messages to security and network tools to isolate a server or block traffic to specific IP addresses

Using the playbook, ROC workflows can be created to send alerts and contextual information to asset owners and SOC teams when assets with unusually high risk scores are detected. This guidance allows them to step up monitoring of assets whose compromise would be particularly damaging to the organization.

Results and status Information

A ROC playbook can also specify actions to be taken at the end of the remediation process.

Examples might include reporting the successful completion of a requested action, or reporting unsuccessful attempts and reasons for the failure (e.g., no patches available for a vulnerability).

Other examples are creating alerts to notify appropriate team members and sending data for auditing and reporting purposes.

Orchestration dashboards

To support orchestration playbooks, some ROC platforms include dashboards with information such as the assets in the scope of each remediation plan, sorted by type.

Security teams can drill into the findings, including the number and type of high-severity vulnerabilities and CISA-known exploited vulnerabilities. A dashboard might also display the causes of risk scores for assets and business entities, and the number at high risk due to those causes.

Generating Remediation Plans Based on Key Objectives

Security teams can use a ROC platform to generate and execute remediation plans tailored to business and technical objectives that might include workflow plans that:

- ☑ **Produce quick wins** by targeting a large number of assets that can be fixed in a short time
- ☑ **Have high risk reduction potential**, focusing on assets with risk scores that can be reduced the most
- ☑ **Support existing remediation processes**, for example, Microsoft Patch Tuesdays
- ☑ **Assist incident response** by accelerating remediation of asset types attacked within the organization or at other enterprises
- ☑ **Strengthen protection for key business entities** by prioritizing remediation for assets that support applications critical to the enterprise
- ☑ **Reduce identity-driven attack paths** by prioritizing orphaned accounts, privilege chains, and admin roles that enable lateral movement

For more on how a ROC handles remediation response orchestration, check out: How to Quickly Prioritize Risks.

Up next is Chapter 10, covering the final step of the ROC—executive reporting and compliance.

Chapter 10

Compliance and Executive Reporting

In this chapter

- Learn how the Risk Operations Center helps ensure compliance readiness with detailed audit trails
- Understand how the ROC helps maintain compliance with various regulations
- See how the ROC provides executives with risk summaries for IT assets and business entities

The ROC Approach to Compliance and Executive Reporting

The seventh component of the Risk Operations Center process, **compliance and executive reporting**, solves the challenge of communicating IT risks and compliance information with business stakeholders.

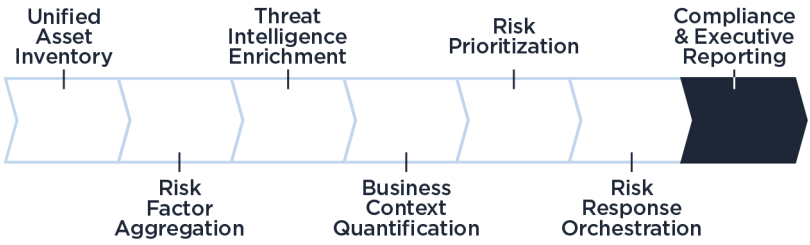

Figure 10-1: Compliance and executive reporting: The seventh component for operationalizing a Risk Operations Center.

This guide outlines many types of risk-related data a ROC can capture and analyze. The guide also shows how the data can be utilized to prioritize response and remediation activities and direct security planning and investment.

However, risk data can be organized in many other ways in dashboards and reports to drive actions and help organizations make better decisions. Along these lines, we will explore reporting for regulatory compliance, security program management, and communication with executives.

Reporting for Compliance

Remember those asset tags we in Chapter 6 that record business context for IT assets? To facilitate regulatory compliance, tags for an asset can indicate that it supports:

- ☑ Specific regulations and industry standards such as PCI DSS, HIPAA, GDPR, NIST, and OSI
- ☑ Controls important for compliance with standards for access control, data encryption, and privacy

A ROC platform can use these tags to aggregate, monitor, and track risk scores for all assets related to specific regulations and controls, and for combinations, say, for PCI and data encryption. A ROC platform can also be used for analysis of combinations within specific settings—say, for assets involved with PCI compliance and data encryption that are hosted on cloud platforms for the South Asia region.

Through these capabilities, a ROC platform can be a key tool for:

- ☑ Identifying compliance gaps between current practices and required standards and regulations
- ☑ Providing data for compliance reports
- ☑ Documenting good faith efforts to improve compliance over time
- ☑ Demonstrating identity governance

A ROC platform can help organizations accomplish some of these goals. Dashboard reports not only rate the overall level of

readinessfor a NIST 800-53 audit, they also provide information on how many assets have compliance gaps so they can be targeted for remediation.

Some ROC platforms also provide pre-designed reports in standard formats for audits, relieving compliance teams from collecting data and creating those reports.

Reporting for Security Programs

A ROC can provide metrics that enable security executives to improve the effectiveness of their activities. For example, ROC dashboards and reports can organize data to show:

- ☑ The asset types and business entities with the *highest* risk
- ☑ Business entities that have experienced the *biggest increases* in risk
- ☑ Business entities that have experienced the *biggest decreases* in risk
- ☑ Remediation options that will produce the *fastest reductions* in risk
- ☑ Remediation options that will produce the *largest reductions* in risk
- ☑ *Differences* in risk levels among business units, assets, or business entities of the same type

This information provides insights into issues needing more attention and successes that can be replicated. It can also help security executives monitor progress in risk reduction.

The risk metrics can be used to:

- ☑ Create objectives for security teams
- ☑ Measure (and reward) the performance of the most effective teams
- ☑ Assess whether investments in security controls and staff achieve expected results
- ☑ Measure the progress over time of individual elements of the security program and the program as a whole

Reporting for Executives

ROC dashboards and reports can play a unique role in communication with executives and boards of directors. Even managers with no technology background can immediately grasp the implications of ranking assets and business entities by risk score.

From there, managers can address assets with the highest risk scores first and use business risk as a metric to set goals, compare alternatives, and measure results.

Business unit executives

ROC dashboards and reports can help security leaders work effectively with the leaders of business functions, such as finance, human resources, marketing, and manufacturing, as well as business units and subsidiaries. Not only do they provide information in terms all businesspeople can understand, they can also be customized to display information tailored to the function or business unit, and even to subdivisions within those entities.

For example, a CISO could sit down with a CFO and discuss the risk profile of:

- ☑ The financial function as a whole
- ☑ Business entities within the function, such as accounting, treasury, tax, and investor relations
- ☑ Financial operations for each business unit and subsidiary

ROC data and analysis might also help the CISO and CFO conduct an informed conversation about cyber insurance options as they assess the risk appetite of the organization.

CIOs and CEOs

Risk scores and monetary values associated with risk provide a simple but powerful way to summarize key security program information for CIOs, CEOs, and other top executives, and to drill down into details when appropriate.

ROC dashboards and reports can be used to:

- ☑ Explain the current allocation of security resources and their alignment with business strategy
- ☑ Create objectives for the security program as a whole and for its major components
- ☑ Set and justify goals for security investments and initiatives
- ☑ Measure progress toward those objectives

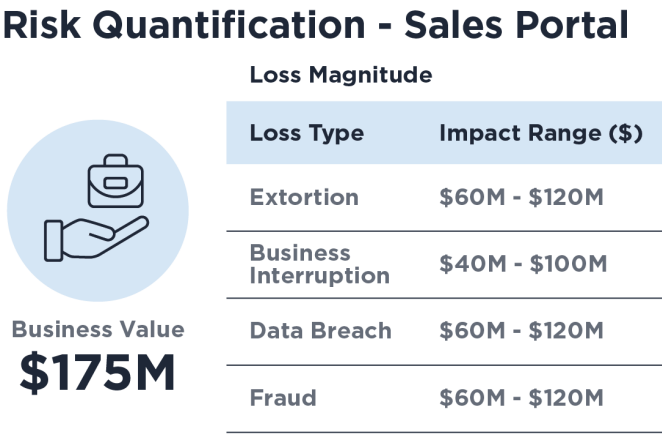

Figure 10-2: ROC dashboard view of the monetary value of a sales portal and the loss potential of various cyberattacks.

Boards of Directors

CISOs and other security leaders are increasingly asked to interact directly with boards of directors. They must demonstrate that they understand the business as a whole and are working effectively to support strategic initiatives and minimize business risk.

Information generated by a ROC can help security executives communicate by:

- ☑ Clarifying misunderstandings about actual risks to the organization
- ☑ Demonstrating that security resources are being allocated to optimize business outcomes
- ☑ Justifying budgets and new investments

By bolstering cyber risk management capabilities, enterprises can turn security and compliance into competitive advantages.

The next chapter demonstrates how an agentic AI framework accelerates and future-proofs the seven core steps of the ROC process.

Chapter 11

Future-Proofing a ROC with Agentic AI

In this chapter

- Discover the benefits of a ROC that leverages agentic AI
- Learn how an agentic AI framework accelerates the seven core steps of the ROC process
- See how integrating agentic AI works better in a phased deployment rather than a "big bang" rollout

For years, security teams used automation to execute tasks such as patching and ticket creation. Unfortunately, existing automation technologies still require significant human effort to define rules, anticipate scenarios, and update the logic as the environment changes.

Agentic AI represents a significant leap forward. Instead of following a rigid script, an AI agent can perceive its environment, create a plan, and execute actions using available security and IT management tools. As part of a Risk Operations Center, an AI agent can be tasked with a high-level goal, such as "reduce the risk score for the PCI environment" and autonomously take action to achieve it.

This capability moves beyond simple automation. Agentic AI introduces a dynamic approach—where the system can adapt to new information, handle exceptions, and sequence complex actions without step-by-step human direction.

Mapping Agentic AI to the ROC Process

An agentic AI framework accelerates each of the seven core steps of the ROC process. By delegating specific goals to AI agents, security teams can transform semi-automated workflows into a more autonomous, continuous operation. Here's a sampling of what AI agents can do in different steps of the ROC process:

Inventory All Assets

Discover and classify assets for a cloud subsidiary by selecting discovery tools, querying cloud APIs, analyzing network traffic, parsing procurement records, and reconciling results in the central inventory.

Aggregate Risk Factors

Identify critical risk factors for production servers by orchestrating scans, reviewing IAM for orphaned accounts, checking configurations against benchmarks, and correlating signals to surface compound risks.

Enrich Threat Intelligence

Determine immediate threat exposure for e-commerce platforms by monitoring threat feeds and bulletins, detecting relevant exploits, and enriching affected asset records with contextual indicators.

Add Business Context

Streamline business tagging by interfacing with CMDB, ITSM, and financial systems to infer relationships and criticality, flagging inconsistencies for human review.

Prioritize Risks

Continuously prioritize top risks by weighing technical severity, live threat intel, and business criticality, and elevating toxic combinations to the front of the queue.

Orchestrate Risk Response

Remediate defined vulnerabilities by generating a plan, selecting the right tool, validating impact, executing fixes, and verifying risk reduction.

Produce Compliance and Executive Reports

Generate weekly compliance gap reports by querying assets, comparing controls, summarizing findings, visualizing trends, and drafting executive-ready outputs.

In addition to enhancing each step of your ROC process, AI agents can work across different steps to coordinate actions among security functions. With sufficient training and parameters, an AI agent can monitor threat actor activity related to a particular exploit, identify at-risk assets, and prioritize risk reduction actions based on business impact—while keeping humans in the loop for review and approval.

Top Agentic AI Benefits

A ROC using agentic AI agents offers compelling benefits:

- ☑ **Speed**—operates at machine speed, reducing the duration between risk detection and remediation from days or weeks to minutes
- ☑ **Scale**—manages thousands of assets and analyzes millions of risk signals simultaneously, far exceeding human capacity
- ☑ **Consistency**—removes manual variability to ensure risk management processes are executed uniformly and in line with established policies

The Need for Governance

Agentic AI also introduces a few new risks into ROC processes. However, these can be addressed through robust governance practices that include:

Goal Alignment

The highest risk is an agent pursuing a poorly defined goal. An instruction to <patch all servers> could cause widespread outages if business context is ignored. Goals must be specific, contextual, and include clear constraints.

Operational Guardrails

Agents must operate within strict boundaries, including which tools they can use, what actions they are permitted to take (e.g., read-only vs. read-write), and which systems are off limits.

Human-in-the-Loop

For high-stakes actions, a human-in-the-loop approval workflow is essential. An agent can formulate and propose a remediation plan, but a human expert should provide the final authorization before execution.

Auditability

Every action taken by an AI agent must be logged in a clear, understandable format. Security teams need a complete audit trail to understand why agents make particular decisions and to investigate any unintended consequences.

A Pragmatic Path to Adoption

Successfully leveraging agentic AI within a ROC requires a thoughtful, phased approach, not a "big bang" rollout:

1. **Start Small—**Begin with a well-defined, low-risk use-case, such as discovering assets in a development environment or generating compliance reports for a single standard.
2. **Define Clear KPIs—**Establish metrics to measure success before deployment: time-to-remediate, percentage of assets with complete business context, or hours saved on manual reporting.
3. **Iterate and Expand—**Use the learnings from initial projects to gradually expand the scope of agentic operations, moving from monitoring and reporting to orchestrated response in controlled environments, and eventually to more autonomous operations with proven guardrails.

By treating agentic AI as a powerful capability to be governed and guided, organizations can safely harness its potential to build a faster, smarter, and more resilient ROC.

The next chapter concludes this book, presenting how the ROC will drive the future of cyber risk management.

Chapter 12

Embracing the ROC

In this chapter

- Understand why now is the time to deploy a risk operations center
- Realize why enterprises can never achieve zero risk—the goal is to minimize financial loss
- Learn about developing a plan to build a ROC

The Risk Operations Center Arrives Just in Time

CISOs are under unprecedented pressure to connect the security posture of their enterprise to business performance. Doing so enables buy-in from CEOs, CFOs, and corporate boards to invest in the technologies necessary to reduce IT risks.

Given these developments, the ROC concept has arrived just in time to facilitate the mission to achieve "left of boom" to reduce risks for business operations and maintain continuous threat exposure management.

As noted by Gartner, 75% of organizations are moving towards unified platforms (like a ROC) so they can evolve from fragmented tools to orchestrated risk management. They can do this through a ROC platform that continuously ingests all the data required to assess, prioritize, and mitigate risks in real time, through contextualized risk management.

To realize the full potential of a ROC, organizations need more than just concepts. They need a solution that prioritizes risk signals based on business impact and automates risk

response. The emergence of the ROC platform fills this need. By integrating tools and processes for collecting, correlating, and analyzing data about IT assets and their risks, the ROC can help deliver real-time risk assessments, prioritized remediation plans, and actionable insights.

A ROC essentially advances cyber risk management from a concept to a fully operational system that delivers real-time, actionable insights and transcends the traditional, reactive approach of a SOC.

Enterprises can never achieve zero risk. Instead, their goal should be to minimize financial loss associated with risk. As noted by Richard Seiersen, Chief Risk Technology Officer for Qualys, "Risk Management is the mitigation or transfer of risk for the most plausible losses that could impact the business."

Deploying a ROC: The Big Picture

When you are ready to deploy a ROC platform, consider developing a plan based on these five steps:

1. **Assess the risk surface**—Understand the full scope of risk across on-premises data centers, cloud platforms, endpoints, APIs, and third-party SaaS applications, including identity risks.
2. **Align stakeholders**—Get buy-in from IT, security, executive teams, and the board of directors by focusing on business impacts.
3. **Establish the foundation**—Consolidate risk signals with the platform's unified visibility across asset identities, vulnerabilities, and exploitability.
4. **Prioritize with business context**—Use risk surface management to focus resources on what matters most to the business.
5. **Automate and act**—Streamline remediation with orchestration, automation, and patchless risk elimination.

It's also helpful to collaborate with a managed services provider, particularly for organizations without in-house expertise. These experts can implement risk management

services quickly to accelerate time to value while reducing the burden on internal security teams.

As enterprises begin the ROC journey, they can set the table for success by starting small—focusing on a business-critical area to demonstrate value quickly. Just as important, enterprises need to ensure cybersecurity outcomes map to operational and financial goals. Maintaining alignment between the ROC program and business goals keeps the organization on the path to continuous threat exposure management and reduction of IT risks.

Recap: The Quest to Minimize Risk and Negative Outcomes

In the quest for **left of boom** to minimize cyber risks in complex IT environments, enterprises must contend with overwhelming volumes of data pertaining to vulnerabilities and cyber threats. Security teams have developed a function to collect, aggregate, analyze, prioritize, and report the copious data needed for incident detection and response—the security operations center, or SOC.

However, until recently, there has never been a comparable function to collect, aggregate, analyze, prioritize, and report disparate data to guide the remediation of security issues and strengthen cyber defenses before attacks occur.

A ROC can help security teams create a complete inventory of IT assets, identify associated risk factors, tie in threat intelligence about the assets, their vulnerabilities, and the threats against them, and then tag each asset with business context that influences its value and exposure to compromise or disruption.

At that point, a ROC platform can evaluate risk factors, threat intelligence, and business context related to every IT asset and generate comprehensive risk scores. The ROC can also compare and rank those risk scores within and across security domains and business entities.

This ranking enables security teams to understand which remediation activities appear to have the greatest impact in reducing the frequency and consequences of cyberattacks.

Security teams can also aggregate and analyze those same risk scores to identify the business functions and business entities that pose the greatest risk to the enterprise and to track progress toward reducing risk.

In addition, a ROC platform can magnify the productivity and effectiveness of security teams by orchestrating remediation workflows and compliance reporting. From there, a ROC can boost the influence of CISOs and security executives by allowing them to analyze the potential value of security investments in monetary terms—so they can allocate security resources and plan security investments to minimize business risk.

Ultimately, the ROC platform helps CISOs communicate their plans in terms that are meaningful to CEOs, business function executives, and other non-technical stakeholders. Effective communication is key in the face of escalating cybersecurity challenges and innovative new security technologies. Now is the right time for leveraging the ROC to ramp up the quest to minimize cyber risk and maximize business protection.

LEFT of BOOM

Introducing The Risk Operations Center

Learn how a Risk Operations Center aligns technical risk factors and business context to remediate vulnerabilities quickly—before the bad guys can exploit them.

Security operations centers (SOCs) do a great job organizing "right of boom" security activities that occur after a cyberattack has been detected. But until now, there hasn't been an equivalent resource to systematically manage "left of boom" security processes. Introducing the Risk Operations Center (ROC), a centralized function to guide activities that strengthen cyber defenses before attacks occur and to prioritize actions based on monetary risk values.

- **Unified asset inventory** — learn how a ROC addresses the challenge of discovering all assets across the enterprise
- **Threat intelligence enrichment** — find out how a ROC leverages real-time threat intelligence to enrich asset and risk data
- **Adding business context** — see how a ROC quantifies cyber risk for IT assets by adjusting risk scores based on business context
- **Risk prioritization** — understand how a ROC helps security teams prioritize remediation and lets CISOs allocate resources based on the monetary value of risks to business entities
- **Exploitability validation** — grasp how identifying valid attack paths can prevent attackers from slipping past security controls
- **Orchestration** — discover how a ROC automates and accelerates remediation workflows
- **Agentic AI** — explore how agentic AI supports and streamlines ROC processes

About the Author

Jeff Pike has worked in cybersecurity since 1999, collaborating with 75+ firms. With the unique ability to translate technical concepts into business-value messaging, Jeff has helped clients generate customer success stories, white papers, e-books, and full-length books. He earned his BS in Journalism from Northeastern University.

ISBN 978-1-948939-54-6

Qualys.

CYBEREDGE PRESS™