Risk Assessments: The Hidden Key to Continuous Security Improvement

A Security Leader's Guide to Risk Assessments that Actually Work

CRITICALSTART®

Table Of Contents

Introduction

Do I have the right tools in place to keep my organization safe? How does my security program measure up to my competitors? How can I prioritize security investments?

These are just a few of the questions keeping security professionals up at night. Making informed security investment decisions is both time- and labor-intensive. And security isn't the only issue; there's also consolidating tech stacks and keeping staff and budgets as lean as possible.

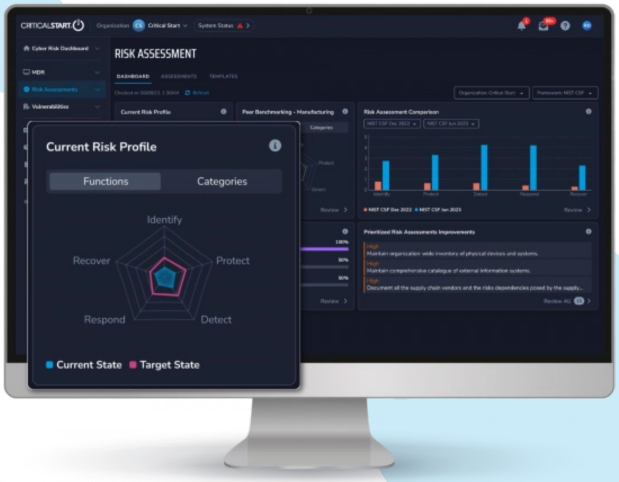
What if there was a way to:

1) Assess and reduce risk in measurable and trackable ways, and

2) Defend budgets and investment decisions with data?

Now, with Critical Start's Risk Assessments, you can.

With guided, framework-aligned questionnaires, prioritized Risk Ranked Recommendations, and intuitive dashboards and reporting that offer real-time and comparative analysis, Critical Start Risk Assessments deliver the tools you need to establish a cycle of continuous security improvement that's risk-aware and data-driven.



High
Maintain organization-wide inventory of physical devices and systems.

High
Maintain comprehensive catalogue of external information systems.

High
Document all the supply chain vendors and the risks dependencies posed by the supply...

Re-thinking Cyber Risk Assessments

Traditional risk assessments gather information to gauge an organization's security posture at a particular point in time. Most of the time, the data is used once, then stored in spreadsheets or documents for months or even years, limiting its value.

Unlike periodic, non-standardized risk assessments that are little more than check-box and audit exercises, a modern risk assessment platform helps you proactively evaluate your organization's cyber risk posture and track risk reduction over time by:

- **Easy-to-use web interface to execute and manage framework-based assessments, with no limits to the number of users or assessments that can be taken or re-taken.**
- **Ability to import existing assessments to gain greater insights and build upon previous work.**
- **Attach evidence of compliance or attainment to each assessment questionnaire.**
- **Visual tracking of security improvements over time.**
- **Industry peer benchmarking and security maturity comparison to more than 1,000 organizations across more than a dozen industries.**
- **Easy-to-follow, ranked, and justified recommendations for making immediate improvements.**
- **Continual reassessment to show progress and keep ahead of changing frameworks, standards, and peer organization advancements.**
- **Track the lifecycle of each assessment including reviewers, approvers, due dates, and overdue status.**

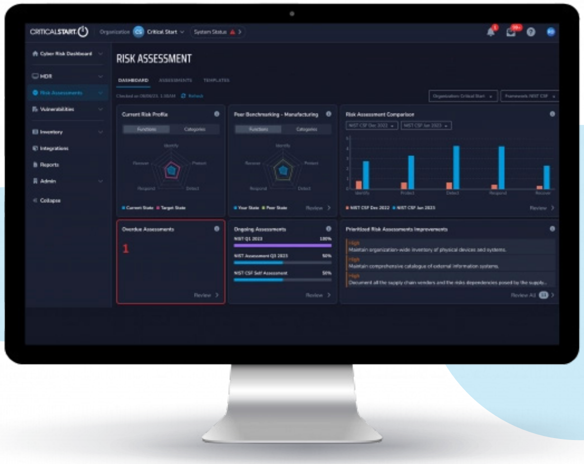
Plus, a platform that couples risk assessment data with additional tools, such as asset visibility, endpoint monitoring, and vulnerability monitoring, further enhances assessment data value. These combined capabilities provide evidence-based, real-time strategic insights that empower organizations to move toward real-time risk monitoring and remediation efforts that deliver the greatest risk reduction impact.

Re-thinking Cyber Risk Assessments (continued)

	Periodic, Non-standardized Risk Assessments	Cyber Risk Assessment Platform
Definition	Exercises "National Institute of Standards and Technology **(NIST CSF)"** used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.	A tool that offers guided and standardized organization of risk assessments and provides insights into evolving security posture. It helps maintain ongoing awareness of cyber risks so that organizational leadership can make data-informed risk management decisions.
Frequency of data updates	Periodic, with manual update frequency, typically based on audit requirements.	Scheduled and regular, with triggered notifications.
Reporting	A static snapshot of security risks.	Snapshot and retrospective views that reflect an organization's response to changing risks, shifting threat landscapes, and emerging vulnerabilities.
Scope	Assesses the overall security posture and risks of technical controls, processes, and policies at a single point in time. Often related to specific audit standards or regulatory requirements.	Expands upon the scope of each risk assessment conducted by providing comparative analysis across cumulative data sets with peer benchmarking.
Data sources	Editable spreadsheet questionnaires that are prone to human error, omission, and editing during the data-gathering process.	Standardized, non-editable questionnaires that structure the data gathering and analysis processes and quickly identify missing or erroneous data points. Ability to import third-party and previously completed assessments. Additionally, platforms can include additional data points that can provide deeper analysis, such as peer benchmarking data, which would otherwise be out of reach.
Methodology	Uses pre-defined questionnaires that are aligned only to the current version of a risk assessment framework (e.g., NIST CSF, ISO 27001).	Frameworks like NIST CSF and CIS controls are used as foundational guides for data-gathering efforts. Platforms can adapt to changing frameworks and standards without complicating analysis and can be customized to organizational needs.
Effort	Intensive process that requires manual data input and analysis.	Less intensive due to standardization of data input and automation of analysis and report generation.
Cost	Often outsourced to expensive third-party vendors who specialize in audit reporting.	Reduces or eliminates the need for outsourcing by allowing internal staff to conduct regular risk assessments without incurring significant additional costs.

Critical Start Risk Assessments: Your Strategic Ace in the Hole

Many, or even most, organizations face challenges with visibility and insight into their cyber risk posture, leading the majority to seek help reducing cyber risk. Those organizations need help identifying security maturity measurements and aligning next steps to established frameworks like NIST CSF.



Maintain organization-wide inventory of physical devices and systems.

Maintain comprehensive catalogue of external information systems.

Document all the supply chain vendors and the risks dependencies posed by the supply...

Quick Start Risk Assessment	Essentials Risk Assessment
Our Quick Start Risk Assessment and Risk Assessments Essentials is a free **5-question guided survey** that delivers dashboards and reports that provide: • A quick understanding of security maturity • Peer benchmarking insights and comparisons • A list of prioritized risk-reduction recommendations • Ongoing tracking and reporting	Risk Assessment Essentials **helps measure and articulate the value of security** and provides: • Guided assessments that track alignment with frameworks (e.g., NIST CSF, CIC CSC v8, NIST 800-171, ISO 27001) • Automated analysis against target maturity and peer benchmarks • Normalization and analysis of existing/historical assessment data currently contained in disparate spreadsheets • The ability to attach evidence, assign owners, and track due dates

Risk Assessments and Framework Alignment

Our guided, data-driven Risk Assessment questionnaire identifies gaps in controls, policies, and procedures, and provides Risk-Ranked Recommendations for driving budget-aware resilience across your organization.

Our free Quick Start Risk Assessment makes it easy to set an organizational risk baseline. Essentials gives you access to multiple risk management and compliance frameworks for:

- Building a risk-driven security roadmap tied directly to frameworks.
- Highlighting control deficiencies across frameworks.

Align Your Organization's Cybersecurity with Industry Standard Frameworks

CRITICALSTART®

Quick Start Risk Assessment

CRITICALSTART®

NIST CSF Guided Assessment

CRITICALSTART®

Custom Assessment

Information Security Management System ISO 27001 Certified

2013
2022

ISO 27001

NIST

NIST CSF 2.0

NIST

NIST Special Publication 800-171

CIS. Center for Internet Security®

CIS Critical Security Controls v8

We're adding and updating frameworks to continually align with industry changes.

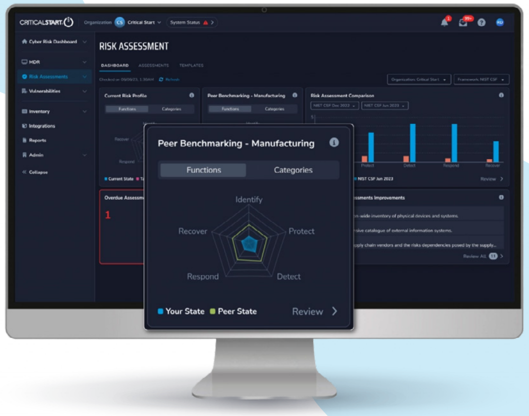
The Benefits of Peer Benchmarking

Peer benchmarking provides context that internal measures alone cannot. By comparing your organization's security posture against industry peers and standards, you can determine where your security posture aligns with sector norms and identify the areas that need improvement.

This information enables accurate peer comparisons and provides actionable insights into:

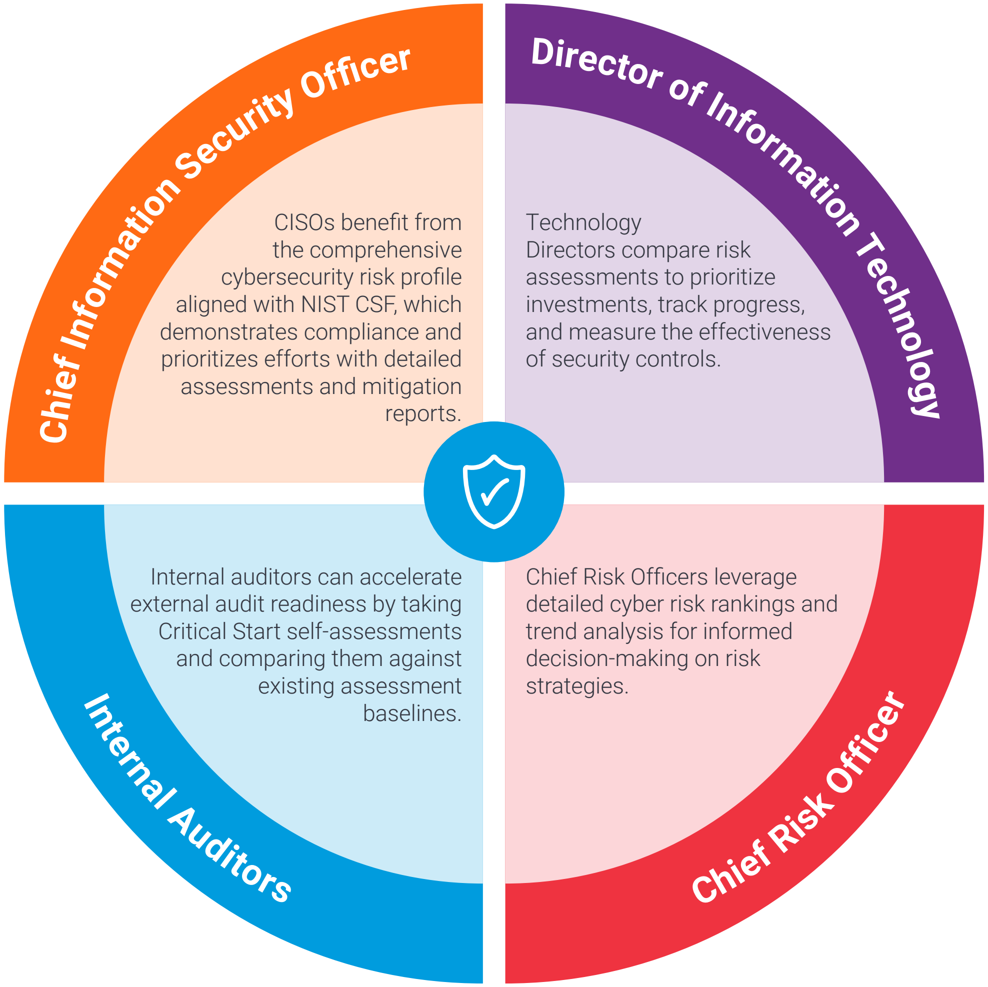
- Risk levels for various categories compared with competitors.
- Prioritized areas in need of remediation based on peer benchmarks.
- Program strengths and weaknesses against established benchmarks.
- Security budget needs and evidence-based justification backed by risk profiles compared with industry averages.
- Current investment validation and demonstration that security maturity meets expected standards.

This industry-based context for cyber risk is invaluable. It helps security leaders clearly and confidently present an organization's security hygiene and posture to business leaders and set objectives for measurable improvement. As a result, leaders are confident security resources are allocated appropriately, enabling data-driven decision-making on security investments, staffing, and activities.



Empowering Security Leadership with Actionable Insights

Critical Start Risk Assessments unify oversight across various compliance demands by delivering high-value insights. With contextualized data, key stakeholders gain the knowledge they need to make strategic decisions within their specific areas of responsibility.



Chief Information Security Officer

CISOs benefit from the comprehensive cybersecurity risk profile aligned with NIST CSF, which demonstrates compliance and prioritizes efforts with detailed assessments and mitigation reports.

Director of Information Technology

Technology Directors compare risk assessments to prioritize investments, track progress, and measure the effectiveness of security controls.

Internal Auditors

Internal auditors can accelerate external audit readiness by taking Critical Start self-assessments and comparing them against existing assessment baselines.

Chief Risk Officer

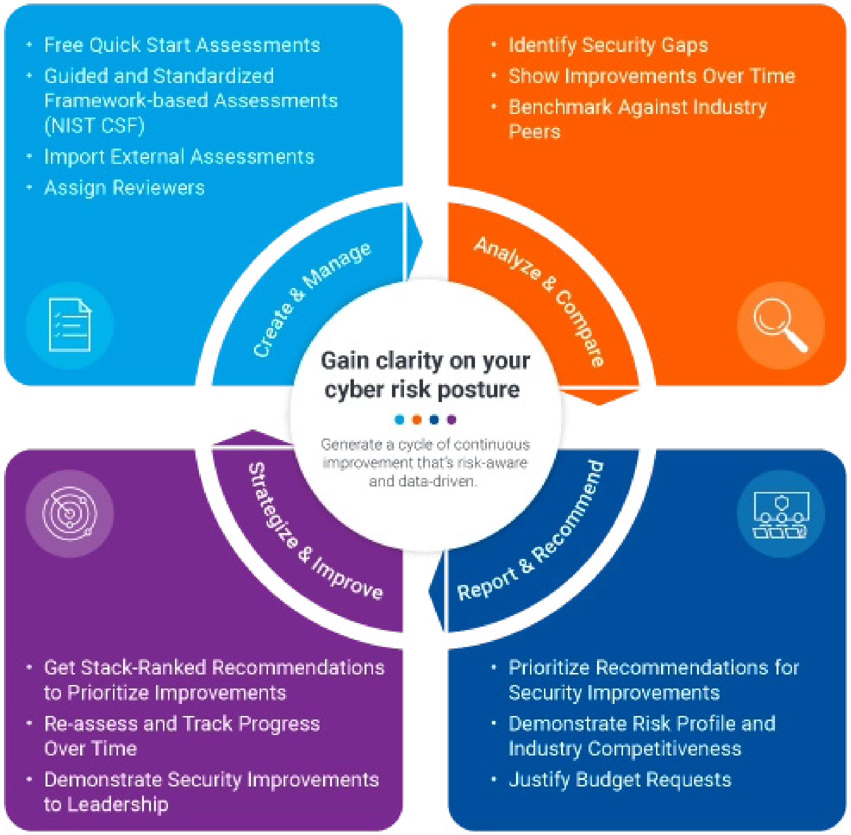
Chief Risk Officers leverage detailed cyber risk rankings and trend analysis for informed decision-making on risk strategies.

Integrating Risk Assessments into the Security Strategy

Critical Start Risk Assessments simplify risk management with a SaaS-based platform that records, tracks, and analyzes risk assessment data. Our Quick Start and Essentials Assessments let you import existing third-party assessment data for a seamless transition to a unified risk dashboard and reporting platform.

Assessment analysis includes peer benchmarking for greater visibility into your organization's risk posture versus competitors. Prioritized risk recommendations help you focus your security improvement efforts and budgets effectively. And comparisons across recurring internal assessments deliver critical tracking metrics and prove the value of your security improvements over time.

Start with our free Quick Start Risk Assessments based on the National Institute of Standards and Technology Cybersecurity Framework (**NIST CSF**) to get a baseline of your organization risk. Move to Essentials when you're ready to leverage our full-service module to access the multiple risk management and compliance frameworks your business needs for more in-depth, proactive insights. Both tiers are backed by data that is easily accessible through clear dashboards and reports, mapping progress to milestones over time.



- Free Quick Start Assessments
- Guided and Standardized Framework-based Assessments (NIST CSF)
- Import External Assessments
- Assign Reviewers

- Identify Security Gaps
- Show Improvements Over Time
- Benchmark Against Industry Peers

- Get Stack-Ranked Recommendations to Prioritize Improvements
- Re-assess and Track Progress Over Time
- Demonstrate Security Improvements to Leadership

- Prioritize Recommendations for Security Improvements
- Demonstrate Risk Profile and Industry Competitiveness
- Justify Budget Requests

Create & Manage
Analyze & Compare
Report & Recommend
Strategize & Improve
Gain clarity on your cyber risk posture
Generate a cycle of continuous improvement that's risk-aware and data-driven.

Achieving Cybersecurity Maturity with Critical Start

By making Critical Start's strategic cyber risk assessments a cornerstone of your path to cybersecurity maturity, you gain a lasting edge, empowering security, leadership, and executive teams to make data-driven decisions that continuously improve security posture and reduce risk exposure against evolving threats.

CISO (Chief Information Security Officer):

CISOs benefit from the comprehensive cybersecurity risk profile aligned with a wide range of frameworks, demonstrating compliance and prioritizing efforts with detailed assessments and mitigation reports.Assign reviewers and track progress

Director of Information Security:

Security Directors compare risk assessments to prioritize investments, track progress, and measure the effectiveness of security controls.

Chief Risk Officer:

Chief Risk Officers leverage detailed cyber risk rankings and trend analysis for informed decision making on risk strategies.

Internal Auditors:

Internal auditors can accelerate external audit readiness by taking Critical Start self-assessments and comparing against existing assessment baselines.

Achieving Cybersecurity Maturity with Critical Start (continued)

In addition to Risk Assessments, two other components of Critical Start's Managed Cyber Risk Reduction (**MCRR**)—**Risk-Ranked Recommendations and** CRITICAL**START**® **Cyber Risk Dashboard**—help enterprises focus on the areas with the greatest measurable security program impact.

Risk-Ranked Recommendations: Building on inputs from CRITICAL**START**® Asset Visibility, Risk Assessments, threat-based alert data, MITRE ATT&CK® Mitigations Recommendations, and more, Critical Start provides data-rich insights into security weaknesses and delivers prioritized and actionable Risk-Ranked Recommendations for driving budget-aware resilience across your IT estate. Our enhanced Risk-Ranked Recommendations system centralizes risk management, enables risk prioritization and ownership tracking, and integrates completion date tracking for improved oversight.

Cyber Risk Dashboard: The Critical Start Cyber Risk Dashboard uses data from Risk Assessments and Risk-Ranked Recommendations to create a dynamic and customizable dashboard that provides a snapshot of your organization's risk landscape. The Cyber Risk Dashboard provides both point-in-time snapshots and tracks changes for historical comparison and maturity analysis. This single source of truth streamlines risk lifecycle management by improving risk visibility, tracking, and accountability. It simplifies the documentation process, helping organizations manage identified risks along with their associated mitigation steps.

Key Takeaways and Recommended Reading

Security maturity is critical to earning and keeping customer trust, and knowing how well your security strategy stacks up against the competition is a game changer.

Now, with the Critical Start Quick Start Risk Assessments and Risk Assessments Essentials, it's easier than ever to:

- See insights that quickly and easily measure cyber security maturity grounded in the NIST CSF.
- Analyze results with visual graphs that show actual versus target maturity and assessment versus peer benchmarks.
- Act on prioritized recommendations and make data-informed strategic improvements.

Don't wait—get started now.

[Start Free Quick Start Risk Assessment]

Recommended Reading

Shifting Paradigms: Redefining Cyber Risk Assessments for Tangible Outcomes White Paper

Critical Start Risk Assessments Datasheet

Critical Start CIS Critical Security Controls v8 Risk Assessment Quick Card

Critical Start NIST 800-171 Rev. 2 Risk Assessment Quick Card

Cybersecurity Risk Assessments at CriticalStart.com

CRITICALSTART®

Don't Fear Risk. Manage It.

For more information, contact us at:
https://www.criticalstart.com/contact/