

2025 CISOs' Guide to Automate Security, Privacy, and AI Risk Assessments

TABLE OF CONTENTS

- 3 Introduction**
- 4 Chapter 1. Why Continuous Control Assurance and Risk Assessments are Critical**
- 5 Chapter 2. Addressing CISOs' Top Frustrations**
- 7 Chapter 3. Key Benefits of Continuous Control Assurance and Risk Assessments**
- 8 Chapter 4. How To Transform Security, Privacy, and AI Risk Assessments**
- 11 Chapter 5. Building the Business Case for Continuous Testing**
- 12 Chapter 6. Case Study: Enhancing Security for a Global Pharmaceutical Giant**
- 13 Chapter 7. Conclusion: Building Resilience Through Continuous Control Assurance and Risk Assessments**
- 14 References**

INTRODUCTION: REDEFINING HOW TO CONTINUOUSLY TEST APPLICATIONS, DATA, AND INFRASTRUCTURE FOR SECURITY, PRIVACY, AND AI RISK

CISOs have one primary responsibility: protecting their organization's critical assets — applications, data, and infrastructure — from evolving cyber threats while driving business growth. Security is no longer just about protection; it's about building trust with regulators, auditors, and customers while creating operational efficiencies.

The irony is that despite investing millions in security tools, many still can't confidently say their applications meet their security, privacy, and AI governance requirements at all times. This is a universal issue but there's a way forward to provide CISOs with the assurance needed over security measures. This guide highlights these measures.

The truth is that traditional risk assessment approaches, such as annual audits or quarterly manual assessments, are no longer enough. With sprawling IT environments and increasing regulatory scrutiny, spreadsheet-based cybersecurity assessments and point-in-time workflows are insufficient for today's fast-paced threat landscape.



Sravish Sridhar
CEO of TrustCloud

CHAPTER 1: WHY CONTINUOUS CONTROL ASSURANCE AND RISK ASSESSMENTS ARE CRITICAL

Continuous control testing and risk assessments ensure CISOs can extract maximum value from their existing security investments. By identifying redundancies, inefficiencies, gaps, and underutilized tools, organizations can optimize their resources while enhancing security outcomes.

The Evolving Threat Landscape

1. The Sophistication of Cyber Threats

Cybercriminals now use AI-powered malware, exploit zero-day vulnerabilities, and deploy sophisticated phishing campaigns.



2. Hybrid and Third-Party Risks

Organizations increasingly rely on SaaS tools and third-party vendors, creating vulnerabilities outside their direct control. **60% of data breaches involve third-party vendors.** (Ponemon Institute)

3. Increased Regulatory Scrutiny

Boards and regulators demand more visibility into breach disclosures and security measures. **In October 2024, four companies were fined by the SEC for inadequate breach responses.**

4. AI Governance Complexity

Enterprises must ensure ethical and secure AI usage internally and with vendors. **"Every enterprise is forming AI governance committees to manage internal AI usage and evaluate vendor practices responsibly."**

5. Technology Sprawl

Hybrid environments, cloud adoption, and third-party tools complicate visibility. **"CISOs face a sprawling landscape of on-prem and cloud systems, making it nearly impossible to get a clear picture of their security posture."**

"Our processes were functional but disconnected. We needed a unified system to improve collaboration and ensure transparency."

Lori Kevin VP of Information Security, IMO Health

CHAPTER 2: ADDRESSING CISOS' TOP FRUSTRATIONS

Frustration 1: Lack of Actionable Insights and Prioritization

Problem: Enterprises invest in hundreds of security tools but lack a unified view of risk. Security signals are overwhelming, with no clear prioritization.

Solution: Integrate control testing, mapped to business, financial, and regulatory compliance objectives to determine which failures to address first. AI-powered workflows prioritize risks based on business impact. Sravish Sridhar says ***“You’ve bought the smoke alarms—now you need a system that tells you where the fire is, which fire is most important to put out first.”***

“The ability to see how risks, controls, and systems connect has been really transformative. It’s not just a tool—it’s a framework for decision-making.”

Lori Kevin
VP of Information Security, IMO Health

Frustration 2: Manual Processes

Problem: Static assessments require significant time and resources while missing evolving risks.

Solution: Automating tasks like access reviews and patch management ensures faster, error-free compliance.

***“Vendor risk management used to feel like guesswork.
Now, it’s a structured process we trust.”***

Lori Kevin
VP of Information Security, IMO Health

Frustration 3:

Lack of accuracy, cannot trust the results

Problem: Subjective risk assessments with spreadsheet-based workflows makes it really hard to believe the results

Solution: Programmatic assessments based on data from systems of record.

Frustration 4:

ROI from security program and where to reduce or apply new budget

Problem: There are always new requirements, needing a new budget. How do I ensure my existing budget is optimized, and how to justify what to spend on next.

Solution: AI-powered workflows prioritize risks based on business impact to drive prioritization and get rid of or consolidate ineffective tools



“The bigger you are, the harder it is to ensure your tools are configured correctly to protect your most critical assets.”

Dixon Wright
VP GRC Transformation of TrustCloud

CHAPTER 3: KEY BENEFITS OF CONTINUOUS CONTROL ASSURANCE AND RISK ASSESSMENTS

▪ **Proactive Risk Management:**

Identifies vulnerabilities before they can be exploited. Sravish Sridhar says *“Think of continuous testing as your Apple Watch—it tells you when something is wrong before it becomes critical.”*

▪ **Incident Prevention and Response:**

Prevents incidents and ensures rapid containment when breaches occur.

Dixon Wright says *“The number one priority for CISOs is preventing incidents. If I do have an event, can I actually respond appropriately?”*

▪ **Continuous Regulatory Compliance Readiness:**

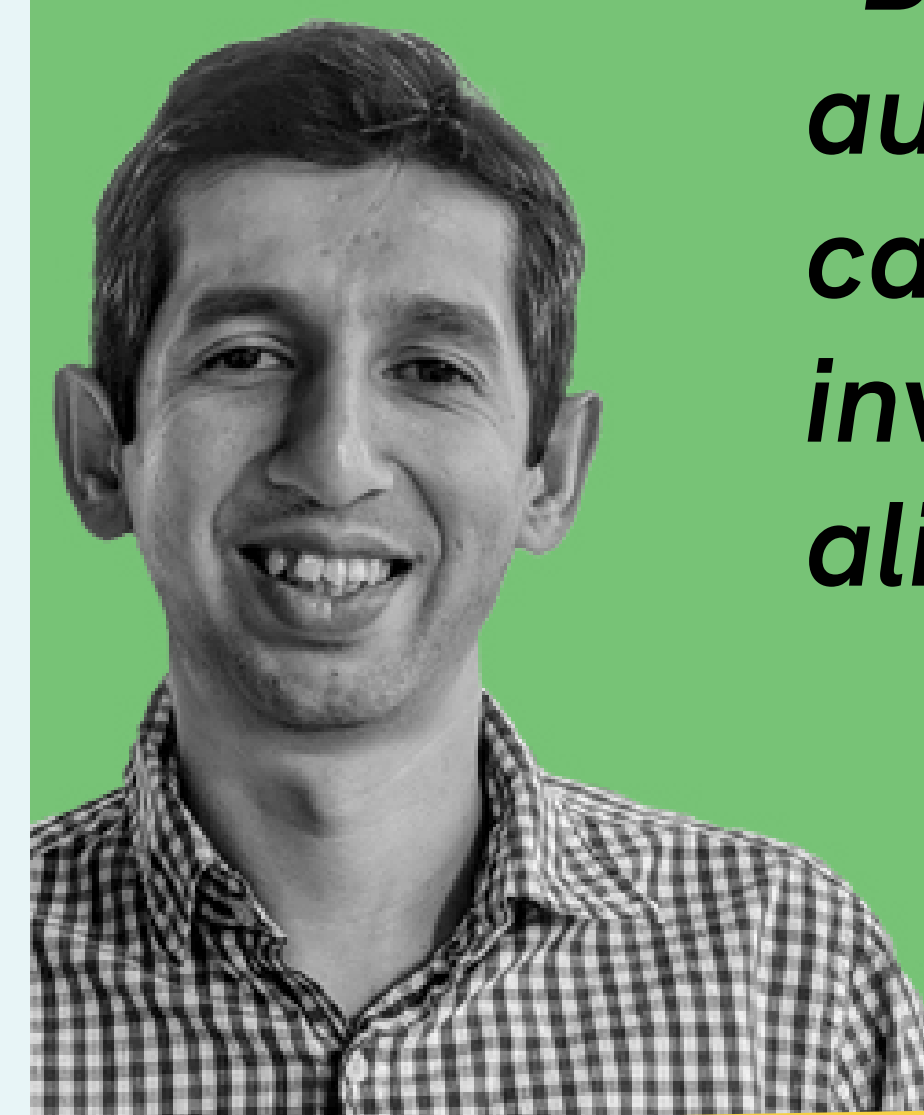
Automates reporting for frameworks like SOC 2, ISO 27001, and GDPR. Reduces audit preparation time by 40%. Operational Efficiency: Frees teams to focus on high-priority threats by automating repetitive tasks. Tejas Ranade: *“The time and cost required to get full visibility manually are prohibitively high. Automation is the only solution.”*

▪ **Maximized ROI on Security Investments:**

Continuous testing ensures that every dollar spent on security tools is optimized for performance and outcomes.

▪ **Business Growth Enablement:**

Continuous testing fosters trust with regulators and customers, creating opportunities for business expansion. Lori Kevin has this to say *“This alignment has been a game-changer for our organization.”*



“By centralizing visibility and automating key processes, CISOs can maximize their existing security investments, reducing waste and aligning with business priorities.”

Tejas Ranade
Chief Product Officer of TrustCloud

“Security isn’t just about protection; it’s about enabling growth by demonstrating resilience and reliability.”

Tejas Ranade
Chief Product Officer of TrustCloud

CHAPTER 4: HOW TO TRANSFORM SECURITY, PRIVACY, AND AI RISK ASSESSMENTS

Transforming Security, Privacy, and AI risk assessments requires CISOs to adopt a programmatic approach to risk management. This involves implementing tools and workflows that provide real-time visibility into risks, automate critical processes, and align security programs with broader business goals.

Implementation Timeline: 30 Days to Continuous Control Monitoring

- **Day 1-10:** Integrate with existing tech stacks and APIs to establish seamless data flows across tools.
- **Day 11-20:** Map controls and prioritize risks using a control framework tailored to the organization's regulatory and business needs.
- **Day 21-30:** Activate real-time monitoring and set up automated reporting dashboards to track progress and identify vulnerabilities.

Key Elements of Effective Risk Assessment Automation

- **Data Aggregation and Noise Reduction:**
Integrate data from diverse sources to reduce noise and focus on actionable risks.
- **Control Frameworks:**
Establish clear mappings between risks, policies, assets, and compliance standards for better visibility.
- **Automated Workflows:**
Use automation to validate controls and processes across complex systems, freeing up resources for high-priority tasks.
- **Business Context Insights:**
Align security metrics with organizational objectives, enabling better communication with leadership.



Real-World Applications

- **Maximizing Security Investments:**

By centralizing visibility, organizations can reduce redundancies and optimize their existing security tools. For example, a financial services firm streamlined their security stack, cutting duplicative costs by 15%.

- **Facilitating Business Growth:**

Automated compliance and improved risk management enable businesses to expand into new markets confidently. For instance, an enterprise SaaS company achieved ISO 27001 certification, unlocking partnerships with global clients.

Dashboards Every CISO Should Use

1. Top Risks and Business Impact Dashboard:

- The CISO's reporting dashboard for the leadership team that summarizes:
 - i. The overall security, privacy, and AI risk posture
 - ii. Top risks, and how they have trended over time
 - iii. The business impact of risk, and the investment and budget required to lower the business impact

2. First-party and third-party application risk posture:

- Provides a real-time view of which applications and vendors have the highest risk to my organization, prioritized by the application and vendor risk surface.

3. Compliance and customer assurance dashboard:

- Presents a picture of how well the security program is enabling business growth:
 - i. By delivering on compliance objectives to help the business expand into new verticals and geographies
 - ii. By meeting customer expectations around security and privacy posture

4. Team Ownership and Accountability:

- Summarizes the functioning of internal teams and spotlights areas that require investment and focus, such as:
 - i. What teams in the organization have the highest ownership of risk and compliance gaps
 - ii. How well is the security and GRC function delivering on its commitments to the rest of the org, how has efficiency and level of automation improved over time

5. Security Posture Dashboard:

- Provides a real-time view of critical vulnerabilities and remediation status.

6. Compliance Dashboard:

- Tracks adherence to regulatory frameworks and highlights gaps in compliance readiness.

7. Incident Response Dashboard:

- Centralizes alerts and response activities for rapid action.

“A good dashboard doesn’t just show data—it tells you what to do next,”

Sravish Sridhar
CEO of TrustCloud

CHAPTER 5: BUILDING THE BUSINESS CASE FOR CONTINUOUS TESTING

Continuous testing isn't just a security measure—it's an investment in the organization's future resilience and growth. By reducing inefficiencies, lowering risks, and simplifying compliance, CISOs can demonstrate measurable returns on security investments.

Cost Savings

According to Forrester, automation saves enterprises an average of \$1.4 million annually. By identifying redundant tools and underperforming processes, organizations can redirect resources to high-impact areas and achieve better outcomes.

Risk Mitigation

Continuous testing lowers the probability and impact of breaches by providing real-time visibility into control gaps and vulnerabilities. This proactive approach reduces the likelihood of incidents and strengthens organizational resilience.

Compliance Confidence

Automated compliance simplifies regulatory reporting and reduces penalties. Meeting regulatory requirements seamlessly fosters trust with auditors and stakeholders, while ensuring alignment with global standards.

Efficiency Gains

Optimized workflows free up resources for strategic initiatives by automating repetitive tasks and centralizing operations. This enables teams to focus on innovation and growth while maintaining robust security practices.

“At the end of the day, it's about making risk management everyone's responsibility. TrustCloud supports us with this, and our team makes it happen.”

Lori Kevin
VP of Information Security, IMO Health

CHAPTER 6: CASE STUDY: ENHANCING SECURITY FOR A GLOBAL PHARMACEUTICAL GIANT

Overview:

A leading pharmaceutical and biotechnology company headquartered in London needed to secure critical applications supporting clinical trial data management and IP protection.

Challenge:

- Apply critical controls to 50 high-priority applications.
- Continuously monitor controls in real time.
- Reduce reliance on manual processes.

Solution:

- Control framework integrated and scoped to applications, infrastructure, and data.
- Automated validation of controls using data from 20+ cloud and on-prem systems of record.
- Continuous monitoring and AI-powered insights for prioritizing risks and findings.

Outcomes:

- Over 80% of technical controls are automatically monitored within 6 months.
- Identified 12 critical gaps and vulnerabilities within the first month.
- Enhanced compliance and stakeholder confidence.

CHAPTER 7: CONCLUSION: BUILDING RESILIENCE THROUGH CONTINUOUS CONTROL ASSURANCE AND RISK ASSESSMENTS

CISOs must embrace continuous testing to stay ahead of evolving threats and regulatory demands. By implementing real-time monitoring, automating controls, and aligning security with business priorities, organizations can build resilience and gain stakeholder trust.

“Continuous control assurance and risk assessments is about trust—internally and externally. It’s how you build a resilient organization that can adapt to any challenge.”

Sravish Sridhar
CEO of TrustCloud

REFERENCES

Cybersecurity Ventures. (2023). Cybercrime report.

Retrieved from <https://cybersecurityventures.com>

Compliance.ai. (2024). 2024 predictions: Expected regulatory compliance focus trends.

Retrieved from <https://www.compliance.ai>

Forrester. (2023). The total economic impact of automation in cybersecurity.

Retrieved from <https://www.forrester.com>

Hyperproof. (n.d.). The importance of security assurance.

Retrieved from <https://hyperproof.io/resource/importance-of-security-assurance>

Kevin, L. (2025). Personal interview. TrustCloud.

Ponemon Institute. (2022). Cost of a data breach report.

Retrieved from <https://www.ponemon.org>

Ponemon Institute. (2023). Third-party risk management benchmark report.

Retrieved from <https://www.ponemon.org>

Ranade, T. (2024). Personal interview. TrustCloud.

Sridhar, S. (2024). Personal interview. TrustCloud.

TrustCloud. (2024a). Building trust and delivering insights with TrustCloud.

Retrieved from <https://www.trustcloud.ai/case-study/atscale-building-trust-and-delivering-insights-with-trustcloud>

TrustCloud. (2024b). Evisort achieves ISO 42001 certification: Pioneering the responsible use of AI.

Retrieved from <https://www.trustcloud.ai/trustcloud-news/trustcloud-customer-evisort-achieves-iso-42001-certification-pioneering-the-responsible-use-of-ai>

TrustCloud. (2024c). TrustCloud platform overview.

Retrieved from <https://www.trustcloud.ai/trustcloud>

Wright, D. (2024). Personal interview. TrustCloud.

