MSECB

○ Webinar Power Point

Security's Secret Weapon: Compliance as a Security Accelerator

Transforming SOC 2 and ISO 27001 into Real-World Defense

Hosted by MSECB

Trevor Horwitz, TrustNet

Rishi Bhatia, Calendly

Disclaimer

This presentation is intended solely for educational purposes and should not be considered as a substitute for independent professional judgment. The views and opinions expressed by the speakers are their own and do not necessarily represent the positions of their employers, MSECB, or any other co-sponsors. MSECB does not endorse, approve, or assume responsibility for the accuracy or completeness of the information presented.

This session may be recorded and distributed in various formats, including audio, video, and print, without further notice. All content, including presentation materials and media captures, is protected by copyright.

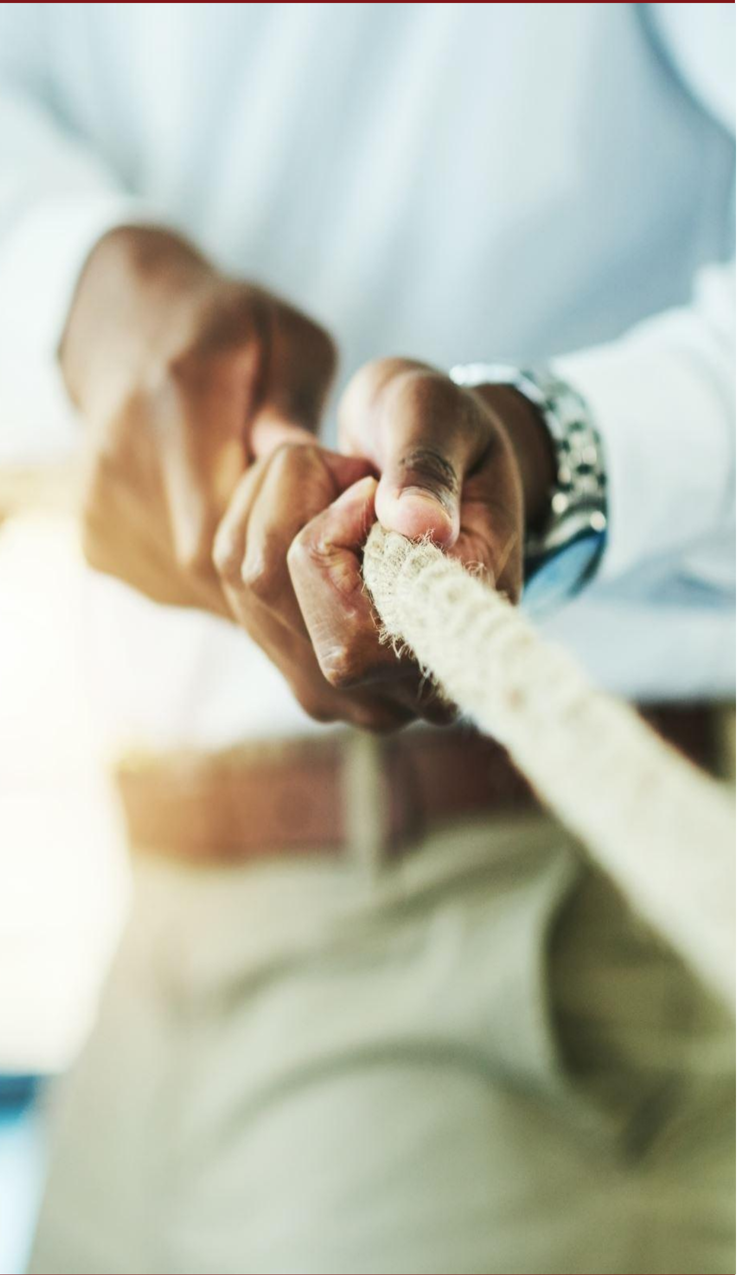
Attendees are advised to use the information provided herein for informational purposes only and not as legal, regulatory, or security advice.

Rishi Bhatia

- 20 years in cybersecurity, risk, and compliance
- Leads security & GRC at Calendly
- Expert in scaling security programs
- Ex-Ripple, PWC, Deloitte
- Focus: security operations, risk management & compliance automation
- Advisor to Fintech, Healthcare, SaaS, including Zip, Whistic, and Drata

Trevor Horwitz

- 20+ years in cybersecurity and assurance
- Founder/CEO of TrustNet
- Built and sold multiple tech companies
- Speaker at RSAC, SPIN, InfraGard, TAG, ISACA
- Advisor, board member, investor
- Board roles: InfraGard Atlanta, ISACA Atlanta
- Certs: CISSP, CISA, PCI QSA, HITRUST, ISO 27001 LA, CDPSE, PCIP

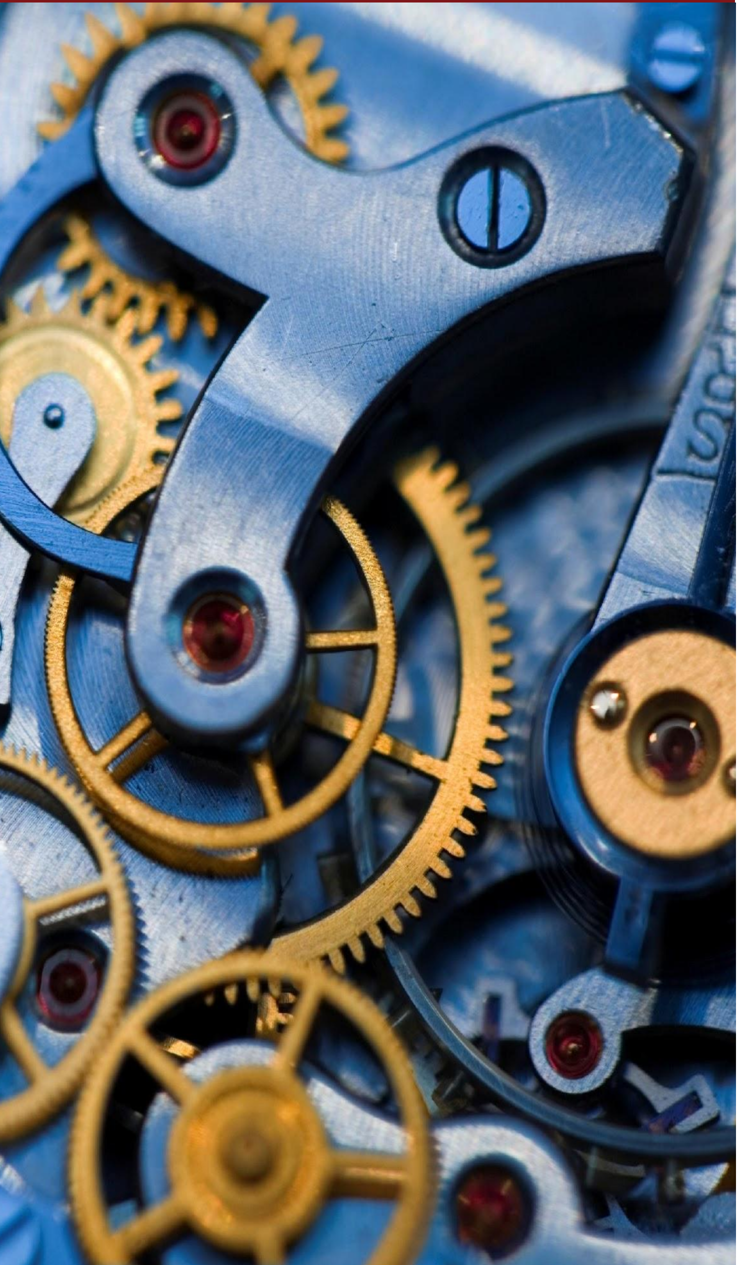


Compliance Has An Image Problem

Compliance Feels Like Bureaucracy

- **Checkbox Culture**: Controls implemented only to "pass the audit"
- **Slows Dev Velocity**: Manual policies, ticket bottlenecks
- **Low Signal, High Noise**: Vague language, security theater
- **Misaligned:** Don’t support day-to-day technical operations
- **Outdated Templates:** "Policies" that no one reads or enforces

"It’s for the auditors, not the engineers."



Evolution of Compliance Frameworks

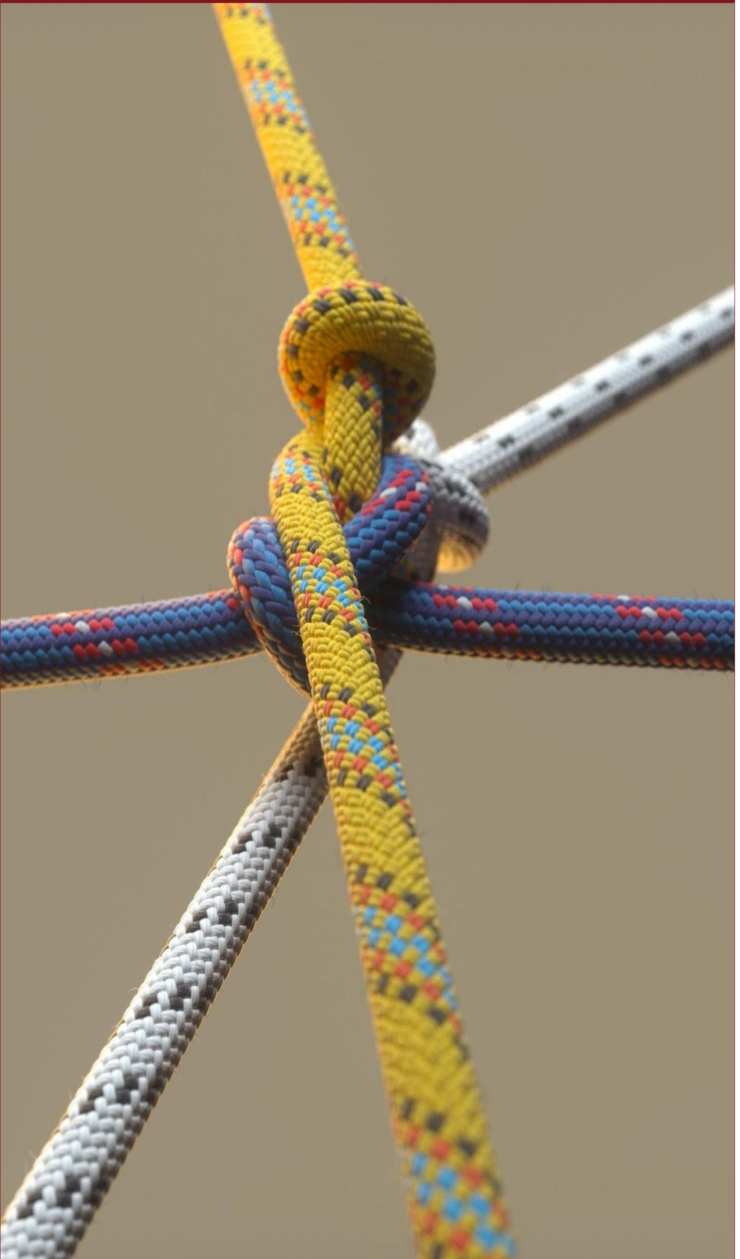
- **From Checklists to Security:** Frameworks are evolving from regulatory checklists to security-centric guidelines.
- **Impact of Breaches:** Major breaches exposed the need for stronger security frameworks.
- **Scope Imbalance:** Broad frameworks (NIST CSF) are seen as weak; specific ones (PCI DSS) are too rigid.
- **Balancing Act:** Modern frameworks blend specific controls with adaptive security strategies.
- **Future Focus:** AI-driven threats demand frameworks that are both comprehensive and agile.

Understanding the Compliance “Why”

What Compliance Really Delivers

- **Drives Revenue:** Assurance opens access to sell into new markets
- **Credibility:** Validates security investments meet industry standards
- **Operational Rigor:** Forces repeatable, measurable security practices
- **Enterprise Trust:** Creates intangible asset that improves business valuation

"Security + Compliance = Trust"



Compliance Drives Security Rigor

Make Security Repeatable, Auditable, and Measurable

- **Repeatability:** Build controls once, enforce them everywhere via automation
- **Auditability**: Clear, documented control coverage — no more "tribal knowledge"
- **Measurability:** Track security posture over time and quantify improvement

"If you can’t measure it, you don’t control it."

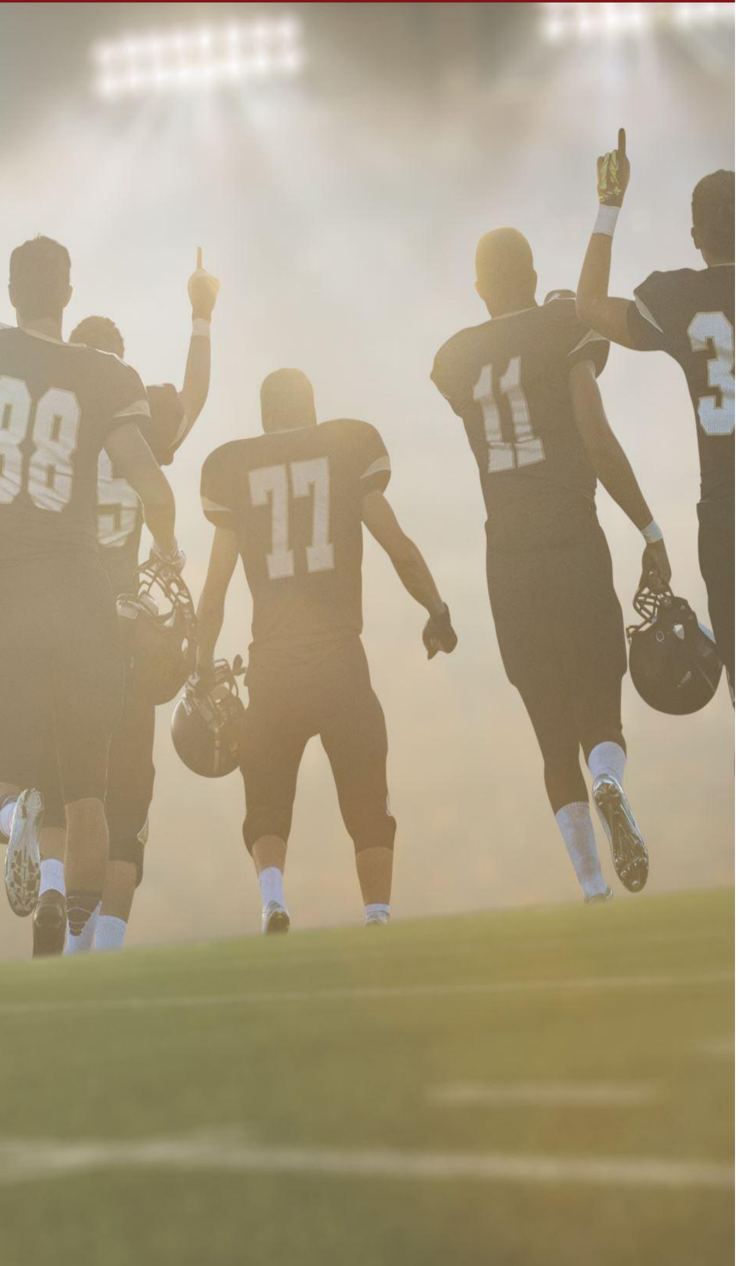
MSECB

Compliance Unlocks Resources

Compliance as a Catalyst for Security

- **Strategic Funding & Benchmarking:** Align security investments with mandates and provide benchmarks to justify budgets and resources.
- **Resource Planning Through Compliance:** Links compliance controls to specific staffing and tool requirements.
- **Compliance-Driven Tooling:** Links NDR, SIEM, ASM tools to compliance controls and security outcomes
- **Executive Visibility**: Compliance KPIs track security progress and emphasize the need for ongoing investment and risk mitigation.

MSECB



How Compliance Transforms Audits into Security Wins

Security-Driven Audit Approach

- **Reframing Compliance Audits:** Shift from a checklist mindset to a proactive security assessment.
- **Control Validation:** Test controls against industry standards
- **Vulnerability Focus:** Identify exploitable gaps, not just compliance issues.
- **Threat Mapping:** Align controls with emerging threats.
- **Actionable Insights:** Turn audit findings into targeted security measures (e.g., patching, MFA, continuous monitoring).

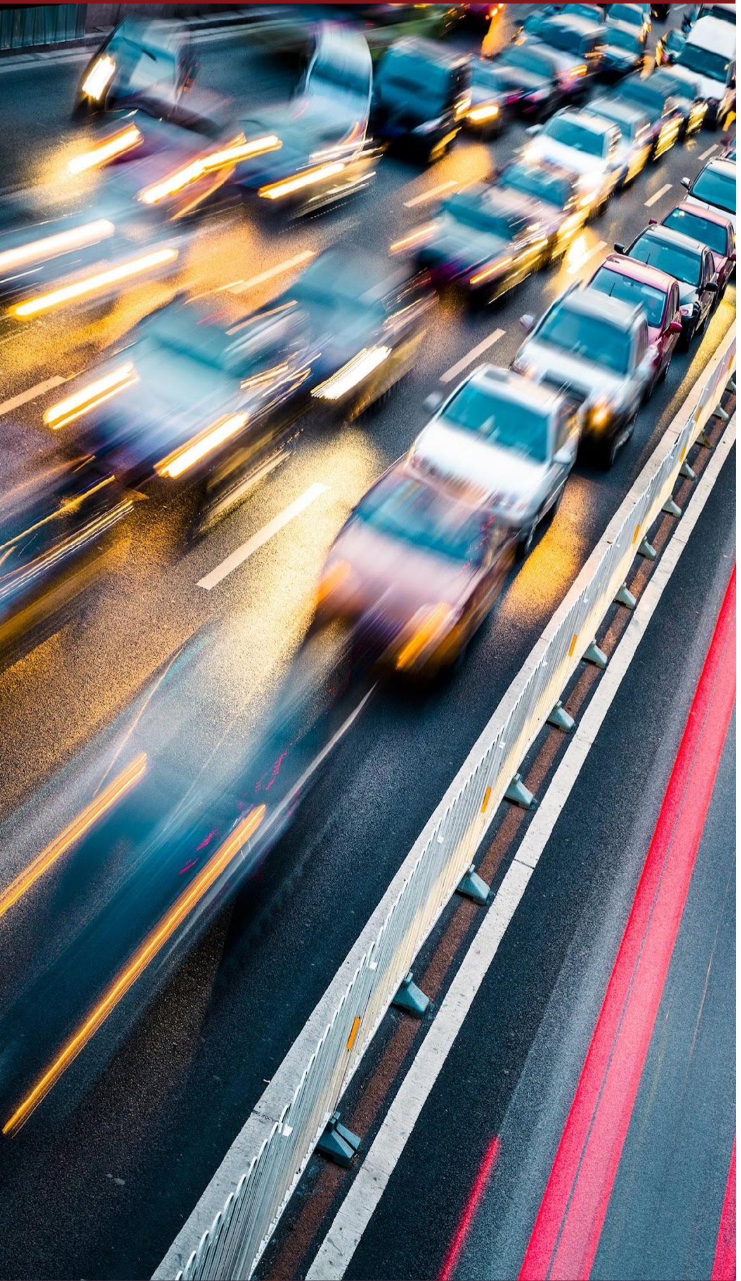
MSECB

Compliance as a Continuous Process

The Path to Security Resilience

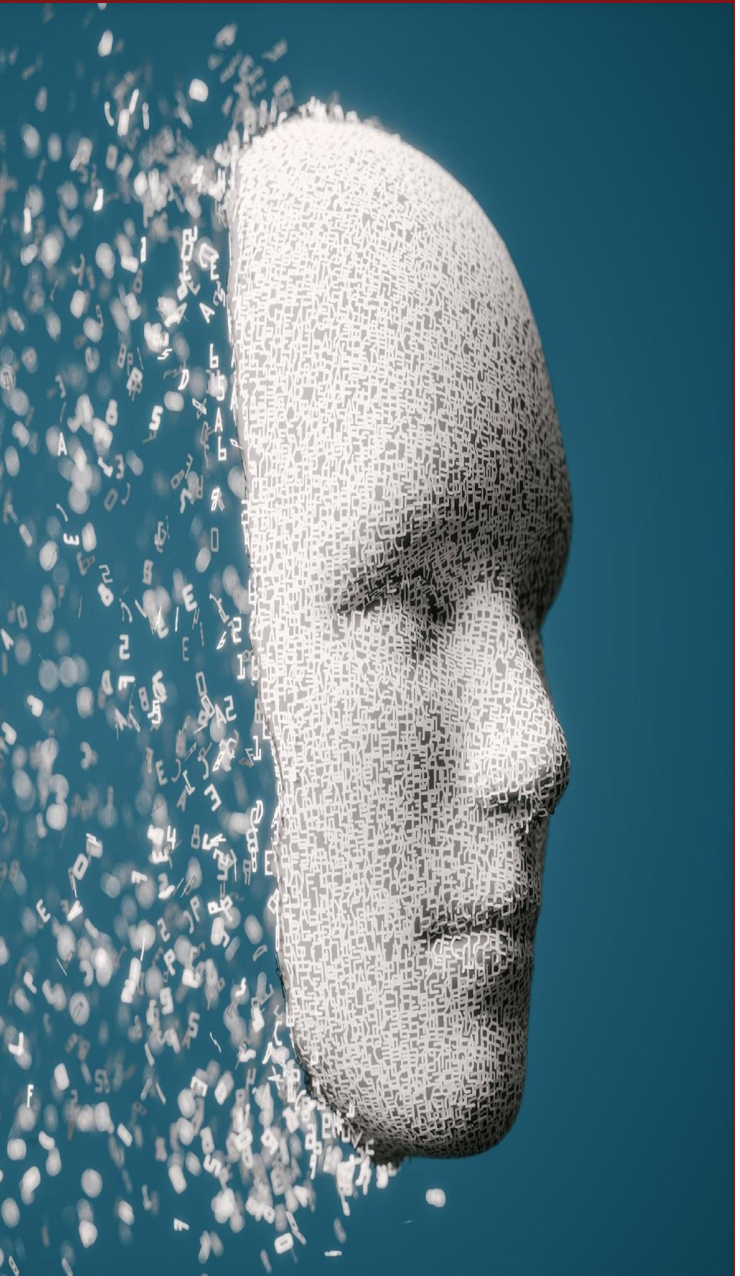
- **Lifecycle Stages:**
    - **Assessment:** Identify control gaps, vulnerabilities, and risk areas through audits and assessments.
    - **Monitoring:** Implement tools (e.g., SIEM, NDR) for control effectiveness and threat activity visibility
    - **Improvement:** Continuously refine controls based on evolving risks and audit findings
- **Continuous Monitoring:** Real-time tracking, integration of security tools, and automated alerts.
- **Validation Loop**:
    - Audit findings drive targeted security improvements.
    - Continuous feedback cycle ensures controls remain effective against evolving threats and regulatory changes.

MSECB



Compliance as a Security Accelerator – SOC 2 & ISO 27001

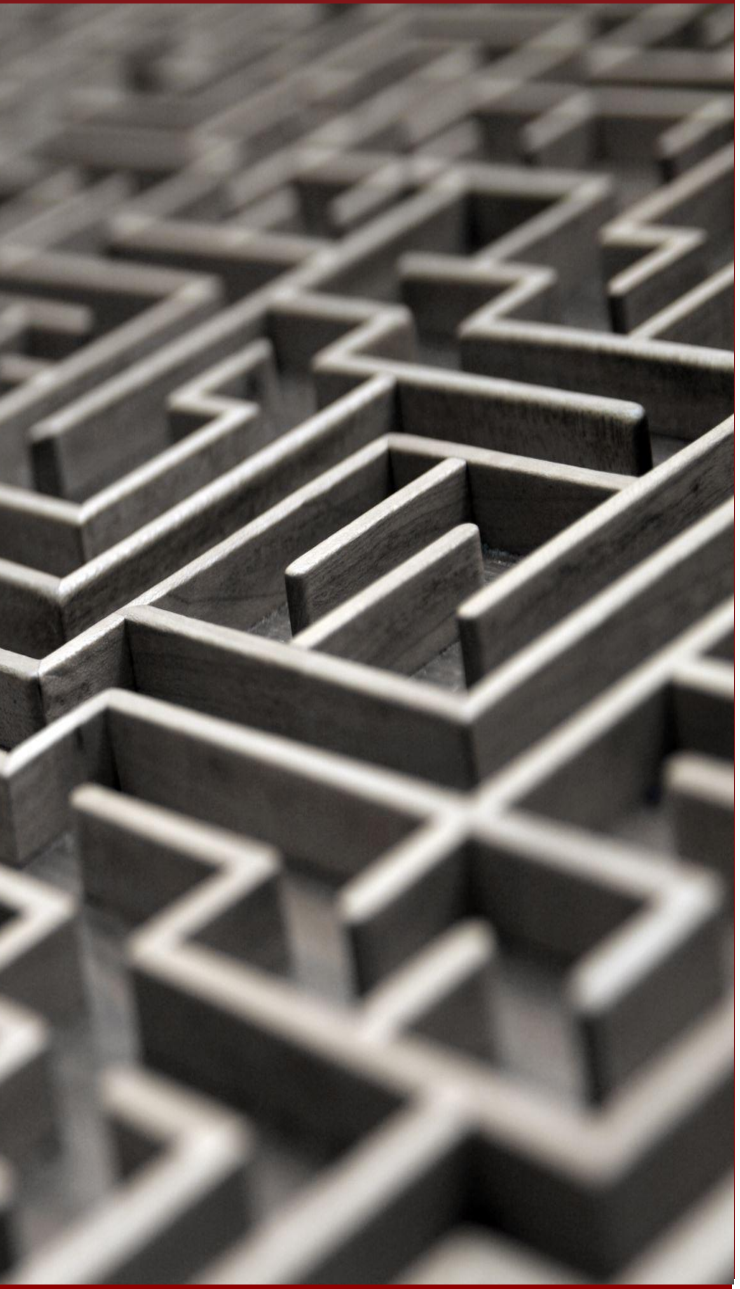
- **Risk Assessments:** Identify business-critical risks beyond standard security scans.
- **Third-Party Controls:** Map vendor controls to internal standards, preventing gaps.
- **Data Classification:** ISO 27001 enforces data retention policies to reduce insider threats**.**
- **Audit Trails:** SOC 2 mandates detailed logs, aiding forensic analysis.
- **Incident Response:** ISO 27001 requires incident response plans tied to business continuity.
- **Management Review:** Regular executive reviews ensure alignment of security controls with evolving risks.



Agentic AI’s Role and the Future of Compliance

- **Anomaly Detection:** AI identifies deviations from baseline behavior in real-time.
- **Predictive Risk Analysis:** Forecast potential compliance violations based on threat patterns.
- **AI Integration:** AI tools for continuous monitoring, threat detection, and compliance tracking.
- **Optimization:** Automated control testing, risk scoring, and incident response.
- **Agentic AI:** Autonomous systems that detect and initiate risk mitigations without human intervention

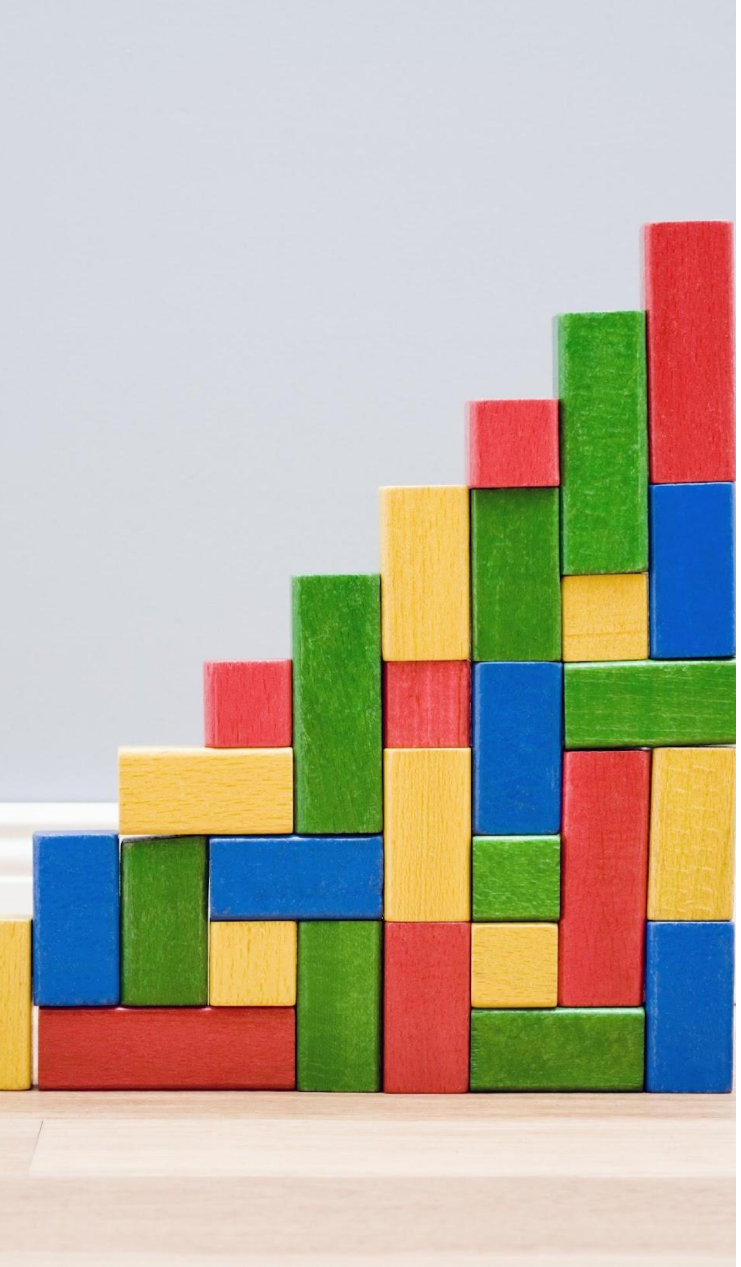
MSECB



Agentic AI’s Audit Challenges

- **Non-determinism:** Unpredictable behavior; hard to replicate outcomes.
- **Opaque Decision-Making:** LLMs lack explainability, undermining auditability.
- **Autonomy:** Unauthorized security actions can trigger cascading failures.
- **Data Provenance:** Verifying data accuracy and origin is difficult.
- **Model Poisoning:** Adversarial inputs can manipulate AI behavior.
- **Drift & Versioning:** AI models change over time, compromising audit consistency.

MSECB



Leveraging Compliance to Strengthen Security in Agentic AI

- **Risk Assessments:** AI risk checks uncover threats like model poisoning and data manipulation.
- **Data Integrity:** Ensures data accuracy – essential for AI decision-making.
- **Access Management:** Enforces role-based access to prevent unauthorized activity and AI model tampering.
- **Monitoring:** Detects AI anomalies and behavioral drift in real time.
- **Incident Response**: Predefined plans for AI breaches enable rapid response.
- **Transparency:** Audits document AI actions, aiding in investigations.

MSECB

Key Takeaways and Action Items

- **Address the Compliance Image Problem**: Shift from a checkbox mentality to a strategic asset.
- **Educate on Compliance Value:** Boosts revenue, credibility, and operational discipline.
- **Security Rigor:** Highlight repeatable, auditable, and measurable security practices.
- **Resource Alignment:** Support budgets, staffing, and tools through compliance benchmarks.
- **Audits as Security Wins:** Transforms audits into proactive risk assessments.
- **Continuous Monitoring:** Real-time tracking and validation loop for ongoing security.
- **SOC 2 & ISO 27001:** Leverage third-party controls, data classification, audit trails, and management review to strengthen security posture.
- **AI Security Through Compliance:** Ensures the need for transparency, data integrity, access control, real-time monitoring, and incident response.

Q&A

Trevor Horwitz	trevorhorwitz
Rishi Bhatia	rishinbhatia

Free resources on SOC 2 and ISO 27001 courtesy of TrustNet

(Scan or use the link)

SOC 2 Accelerator + Guide

TrustNetInc.com/guides/SOC2-2-Compliance/

ISO 27001 Compliance Guide + Checklist

TrustNetInc.com/ISO-27001

Thank you for your attention!

Stay updated!

+1 (450) 328-1227

info@msecb.com

www.msecb.com

in f