PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING

2025 EUROPE COMMUNITY MEETING

Implementing Common Controls, Automation, and Monitoring Tools for PCI & GRC Success

PCI Security Standards Council

Mahmoud Sultan

Sr. Director, Technical Compliance
Toast, Inc

Mai Tran

Manager of Product Solutions
Auditboard

PCI Security Standards Council

Introduction

Modernise compliance to enhance assessment readiness, streamline compliance operations, and improve overall risk visibility within a changing regulatory environment.

- Common challenges faced within FinTech
- Updated Audit and Assessment practices
- GRC Innovation and Engineering
- Value provided to organisations

PCI Security Standards Council

Challenges Facing FinTech Today

Challenges faced at Toast

- Manual and heavily time consuming audits tasks (Evidence collection, etc)
- Inefficiencies in managing overlapping and repetitive controls activities and audits.
- Labor intensive and inconsistent reporting and dashboarding
- Challenges in managing a control compliance lifecycle (self attestations, policy reviews, issues management, etc)

Challenges faced by Auditboard customers

- Manual environment with information in disparate, decentralised systems or applications, requiring additional reconciliation effort from resources.
- Repeated effort from all three lines of defence in separate audits for overlapping controls and evidence collection.
- Lack of agility when the need to adhere to new frameworks, regulations or standards arise.
- High audit or consulting costs due to hiring of external consultants for gap analysis or extended auditing work.

Regulatory Compliance & Agility

What are the top challenges to comply with DORA?

In Nov 2024, we conducted a survey of over 272 professionals in risk management, IT, and InfoSec. The survey identified key challenges in regulatory compliance.

What are the top challenges to comply with DORA?

	Executive /C-Suite	*Senior Leadership*	*Management*
Implementing disaster recovery/business continuity planning and testing	47%	36%	38%
Continuous resilience testing/monitoring	47%	49%	34%
Establishing a comprehensive incident reporting system	45%	44%	31%
Ensuring monitoring of resilience in third-party relationships	43%	33%	16%
Procuring resources (financial, human, technological)	41%	44%	69%
Maintaining ongoing compliance	40%	36%	56%
Understanding the requirements	31%	17%	25%
Stakeholder accountability and engagement	29%	29%	22%
Complexity of integrating multiple regulatory requirements	29%	56%	53%
High implementation costs	27%	40%	59%

PCI Security Standards Council

Updated GRC Practices

Framework Management & Common Controls

- Align your applicable frameworks, regulations and standards to a common control set.
- Audit once, comply with many frameworks.
- Reduce repeated testing procedures across different audits.

Integrations & Automated Evidence Collection

- Integrate with source systems, such as AWS, Azure, SAP and more.
- Pull in data from these systems for GRC functions, e.g. KRI monitoring.
- Collect audit evidence automatically from your systems.

Continuous Monitoring & Analysis

- Build out automated testing workflows or analytics over your system data.
- Link these automated tests to your control or audit documentation.
- Schedule automated tests, monitor for exceptions and set notifications for results.

GRC Innovation & Engineering

Toast: Plan for maturing GRC function

Crawl → Walk → Run

- Establish a common controls framework
- Evidence collection efficiencies and automation
- Expanded and consistent controls monitoring
- Proactive readiness for future programs

Vision: Enable the business by making compliance feel more embedded and less of a burden

Auditboard: New features to automate GRC

- Automated report generation for audits, risks and third-parties
- Suggested controls mapping and Framework update workflow to ensure compliance maintenance
- AI-identified risks and recommended actions for audit findings
- AI governance workflow to aid with EU AI Act

PCI Security Standards Council

Business Value From GRC Automation

Value found at Toast

- **Significant reduction in manual effort, saving hundreds of team hours** per audit cycle previously spent on evidence collection and administrative follow-up.
- **Streamlined compliance across multiple frameworks** (e.g., SOX, PCI DSS) using a common control set, which is on track to reduce redundant testing by 20-40%.
- **Provided real-time visibility into control health**, enabling proactive issue management and more confident, data-driven reporting to the audit committee.
- **Accelerated external audit cycles** by providing auditors with direct, read-only access to pre-approved evidence within the platform, fostering a more collaborative process.

Feedback from Auditboard customers

- Regulation compliance: align existing controls to frameworks the organisation plans to adhere to and easily conduct a gap analysis in platform.
- Reduce manual workload: Integrations and evidence collection for tasks such as compliance issues, automated evidence collection, chase-up, etc, and reduce manual workload.
- Audit once, comply with many: evidence and control tests map over to all frameworks, reducing repeat work across the same processes. Allow external auditors access into the platform to gather evidence to approved controls.

PCI Security Standards Council

Contact

Mahmoud Sultan
Sr. Director, Technical Compliance - Toast
mahmoud.sultan@toasttab.com

Mai Tran
Manager of Product Solutions - Auditboard
mtran@auditboard.com

PCI Security Standards Council

PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING