Olivier Takam

PCI QSA, P2PE QSA, 3DS Assessor, Secure SLC Assessor, Secure Software Standard Assessor

Vice President

ControlCase

ControlCase

PCI Security Standards Council

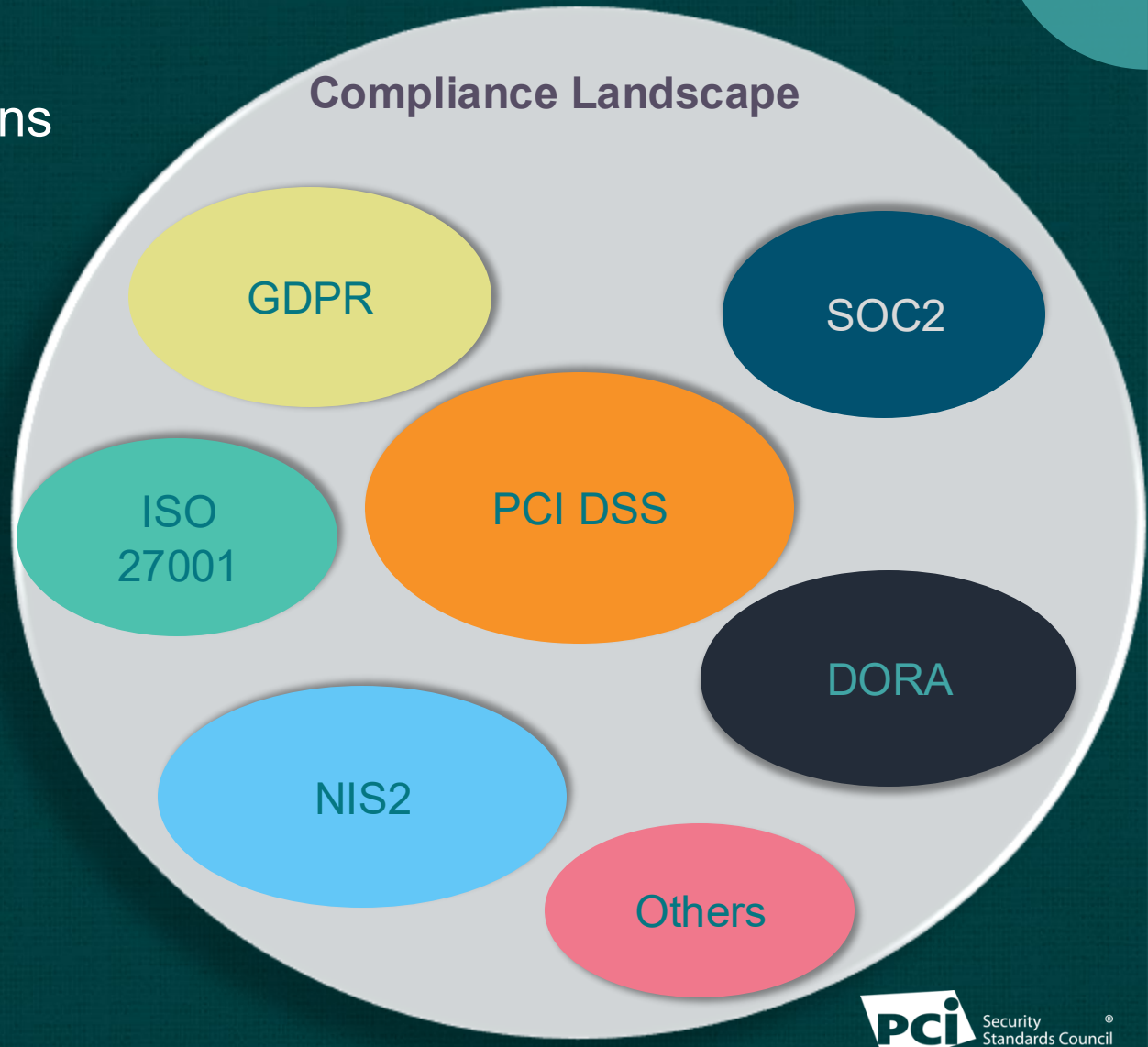
Bridging the Gap Between PCI DSS and EU Regulations

A strategic approach to aligning PCI DSS with GDPR, NIS2, and DORA to streamline compliance and enable holistic security governance

PCI Security Standards Council

The Compliance Landscape

- Increasing number of standards & regulations
- Overlapping requirements
- Resource-intensive compliance efforts



PCI Security Standards Council

PCI DSS, GDPR, NIS2 and DORA Objectives

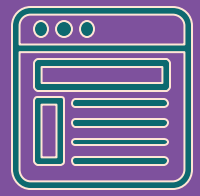
- **Payment Card Industry Data Security Standard (PCI DSS)**: Safeguards payment card data by establishing baseline security controls and reducing the risk of cardholder data breaches and fraud.
- **General Data Protection Regulation (GDPR)**: Protects European Union citizens' personal data, ensuring privacy and giving individuals control over their personal information.
- **Network and Information Security (NIS) 2 Directive**: Seeks to significantly raise cybersecurity standards and improve incident response capabilities and information sharing among essential and important entities across the European Union.
- **Digital Operational Resilience Act (DORA)**: Ensures that the financial sector can withstand, respond to, and recover from ICT-related disruptions and threats.

Comparative Overview: PCI DSS Vs. GDPR Vs. NIS2 Vs. DORA

Regulation/ Standard	Number of controls	Applicability	Primary Focus Areas	Key Entities Covered
PCI DSS 4.0.1	12 core requirements	Merchants, Service Providers	Payment account data	Entities storing, transmitting or processing payment account data or could impact the security of the account data
GDPR	13 core security related articles	Organizations processing EU & UK citizen personal data	Personal data privacy rights, security	Data controllers & processors
NIS2	6 core security related articles	EU essential & important entities	Cybersecurity risk mgmt., incident reporting & information sharing	Operators in critical sectors
DORA	41 core security related articles	EU financial entities & ICT providers	Digital risk & operational resilience	Banks, insurers, ICT service providers

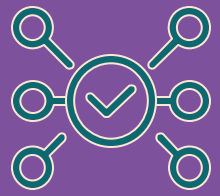
PCI Security Standards Council

Unified Compliance Methodology



Step 1
Identify common control objectives

Step 2
Map controls across standards & Regulations to objectives



Step 3
Analyze gaps and overlaps

Step 4
Develop, Implement and monitor, a unified control framework

PCI Security Standards Council

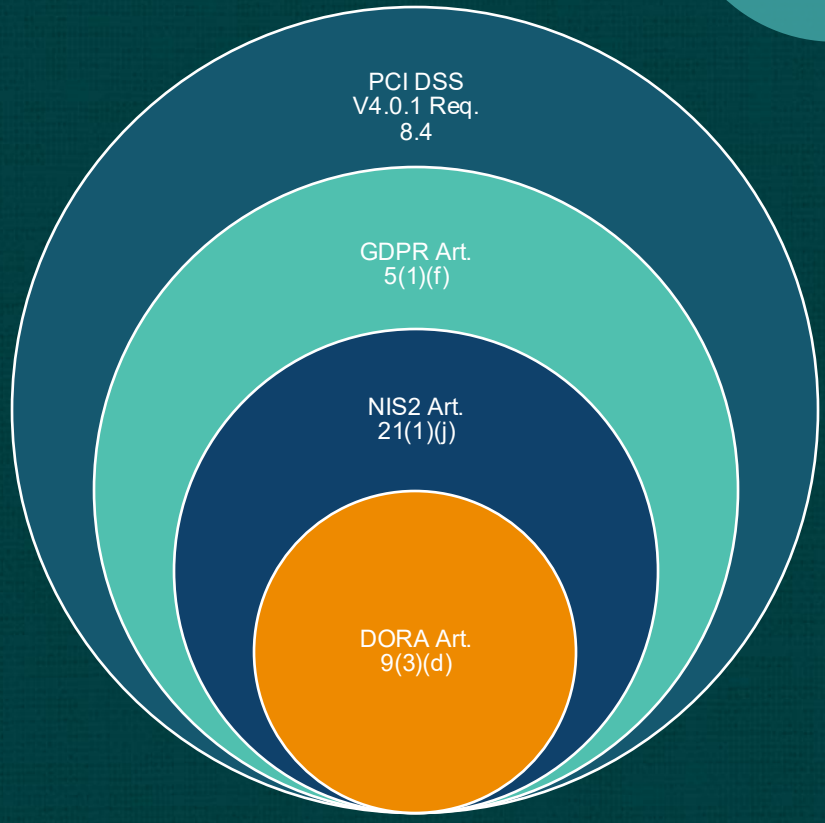
Common Controls Areas

Common Control objectives	PCI DSS	GDPR	NIS2	DORA
Access Control & Authentication	Req. 7, Req. 8	Art. 5, 32	Art. 21	Art. 9
Encryption & Data Protection	Req. 3, Req. 4	Art. 5, 25, 32	Art. 21	Art. 9, 15
Logging & Monitoring	Req. 10	Art. 30, 33, 34	Art. 23	Art. 10
Risk Management	Req. 12.3	Art. 24, 25	Art. 21	Art. 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16
Incident Response & Notification	Req. 12.10	Art. 33, 34	Art. 23	Art. 11, 17, 18, 19, 20, 21, 22, 23,
Third-Party Risk Management	Req. 12.8	Art. 28, 32	Art. 21	Art. 28, 29, 30
System Hardening & Patch Mgmt.	Req. 2, 6	Art. 5, 32	Art. 21	Art. 9
Awareness & Training	Req. 12.6	Art. 39	Art. 20	Art. 5, 13, 16
Business Continuity/Resilience	Req. 12.10.1	Art. 32	Art. 21, 23	Art. 11, 12, 13, 16
Governance & Accountability	Req. 12	Art. 5, 24, 25, 30, 35	Art. 18, 20, 21	Art. 5, 15

PCI Security Standards Council®

Practical Example – Use of MFA

PCI DSS V4.0.1 **Requirement 8.4**	Multi-factor authentication (MFA) is implemented to secure access into the CDE.
GDPR **Article 5(1)(f)**	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).
NIS2 **Article 21(1)(j)**	The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.
DORA **Article 9(3)(d)**	Implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes;



PCI Security Standards Council

Unified Compliance Scenario

ABC Bank

PCI Security Standards Council

Scenario: ABC Bank Unified Compliance

Requirements

- PCI DSS V4.0.1 covering the Bank payment processing environment
- GDPR Compliance Assessment – the Bank processes EU citizen data
- NIS2 Readiness assessment – the Bank is classed as “Essential” entity under NIS2
- DORA Readiness assessment – DORA is applicable to financial institutions

Scenario: ABC Bank Unified Compliance – Approach

Pre-Scoping Phase:

- Common scope definition
- Identify common control objectives
- Controls mapping
- Control gaps and overlaps analysis
- Develop & Implement common control framework

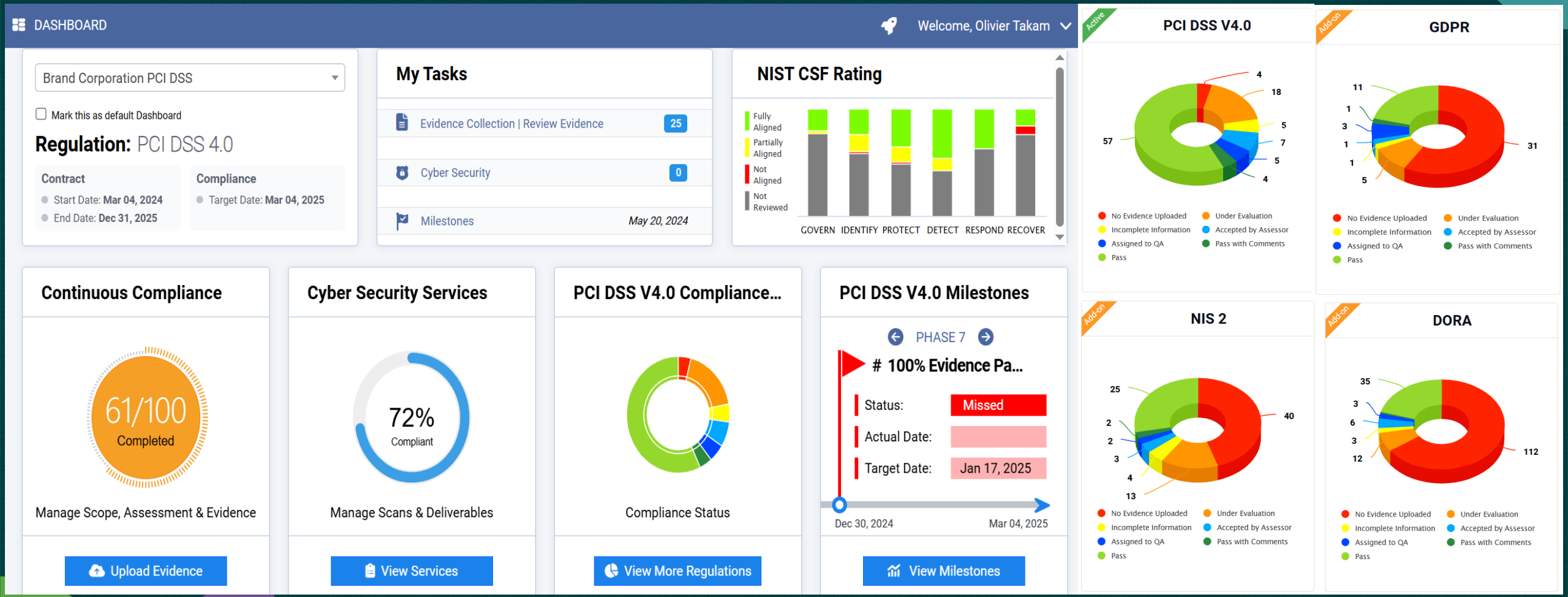
Scoping Phase:

- Scope validation
- Identification of common system components, policies, procedures and processes, and teams
- Common sample set selection for the assessment
- Assessment plan

Assessment Phase:

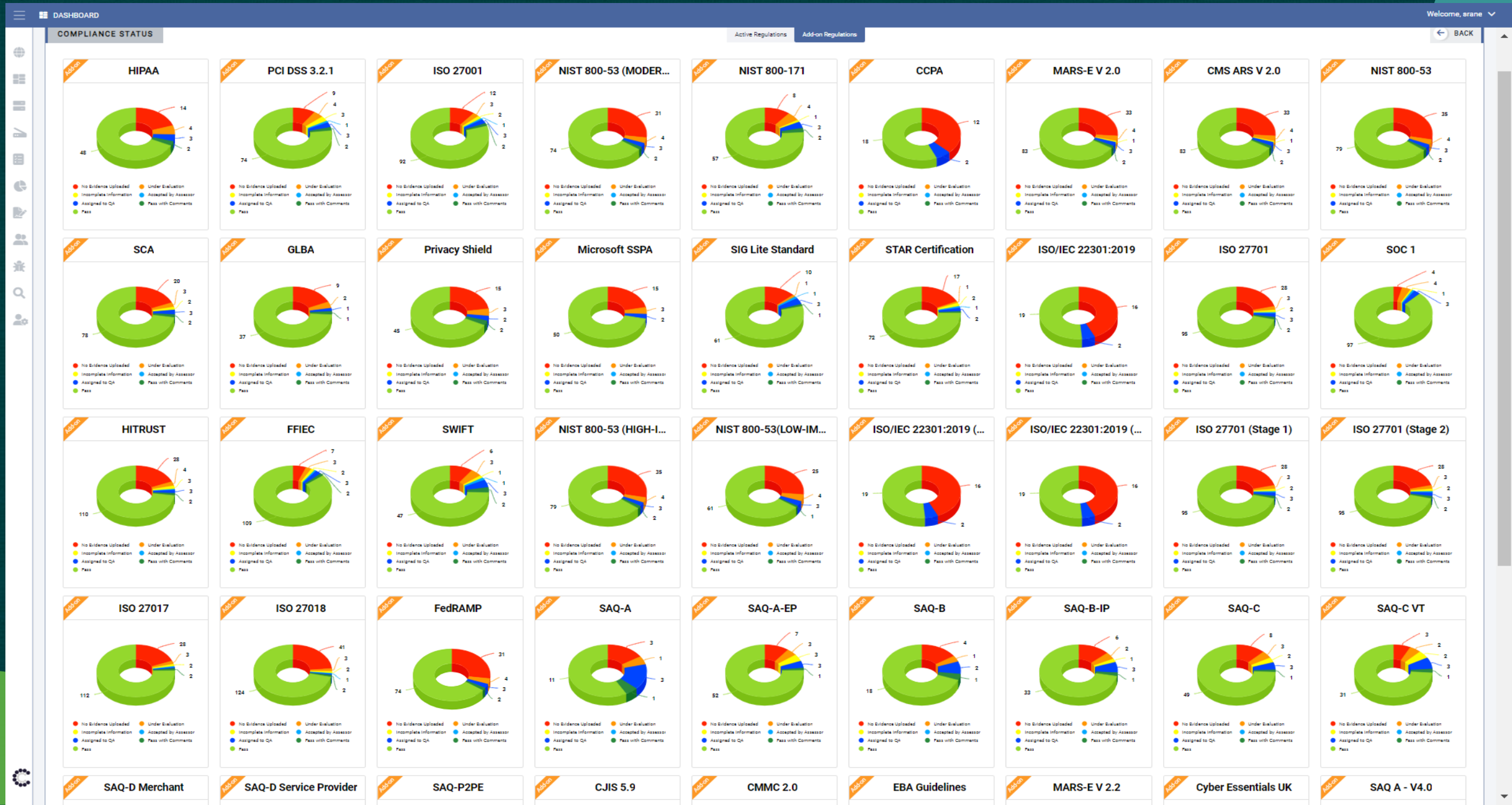
- Common controls validation with common teams (i.e. PCI DSS assessment in tandem with GDPR, NIS2 and DORA) as per the common control framework
- Delta controls validation (i.e. validation of controls specific to each regulations)

ControlCase One Audit Approach



PCI Security Standards Council

Unified Compliance Approach



Benefits and Challenges

Benefits:

- Reduced compliance costs & effort
- Streamlined audits
- Reduced audit fatigue
- Improved overall security posture
- Better resource allocation

Challenges:

- Initial time investment
- Keeping up with standard & regulations changes
- Addressing standard/regulation-specific nuances
- Convincing stakeholders

Best Practices & Key Takeways

Use automated tools for mapping and tracking

Involve experts from different compliance domains

Regularly update your framework as standards & Regulations evolve

Focus on the intent behind requirements, not just the letter

Leverage existing and pre-built frameworks

Document your methodology and decisions