PCI Security Standards Council

Cross Walking IT Compliance Standards with PCI DSS

Streamlining Compliance in a Multi-Standard Environment

PCI Security Standards Council

Satya Rane

COO, ControlCase

ControlCase

ControlCase Snapshot

CERTIFICATION AND CONTINUOUS COMPLIANCE SERVICES

Go beyond the auditor's checklist to: **Dramatically reduce the time, cost, and burden of maintaining IT compliance and becoming certified.**

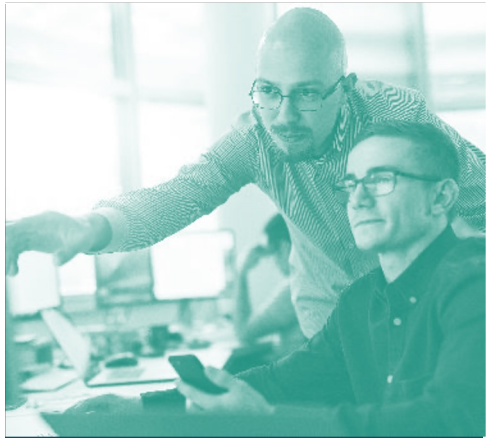
Demonstrate compliance more efficiently and cost effectively (cost certainty)

Offload much of the compliance burden to a **trusted compliance partner**

275+
SECURITY EXPERTS

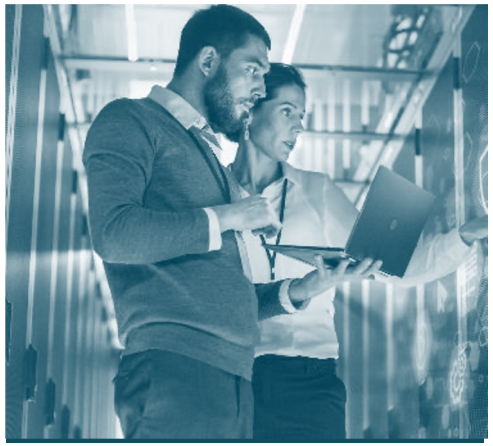
10,000+
IT SECURITY CERTIFICATIONS

1,000+
CLIENTS



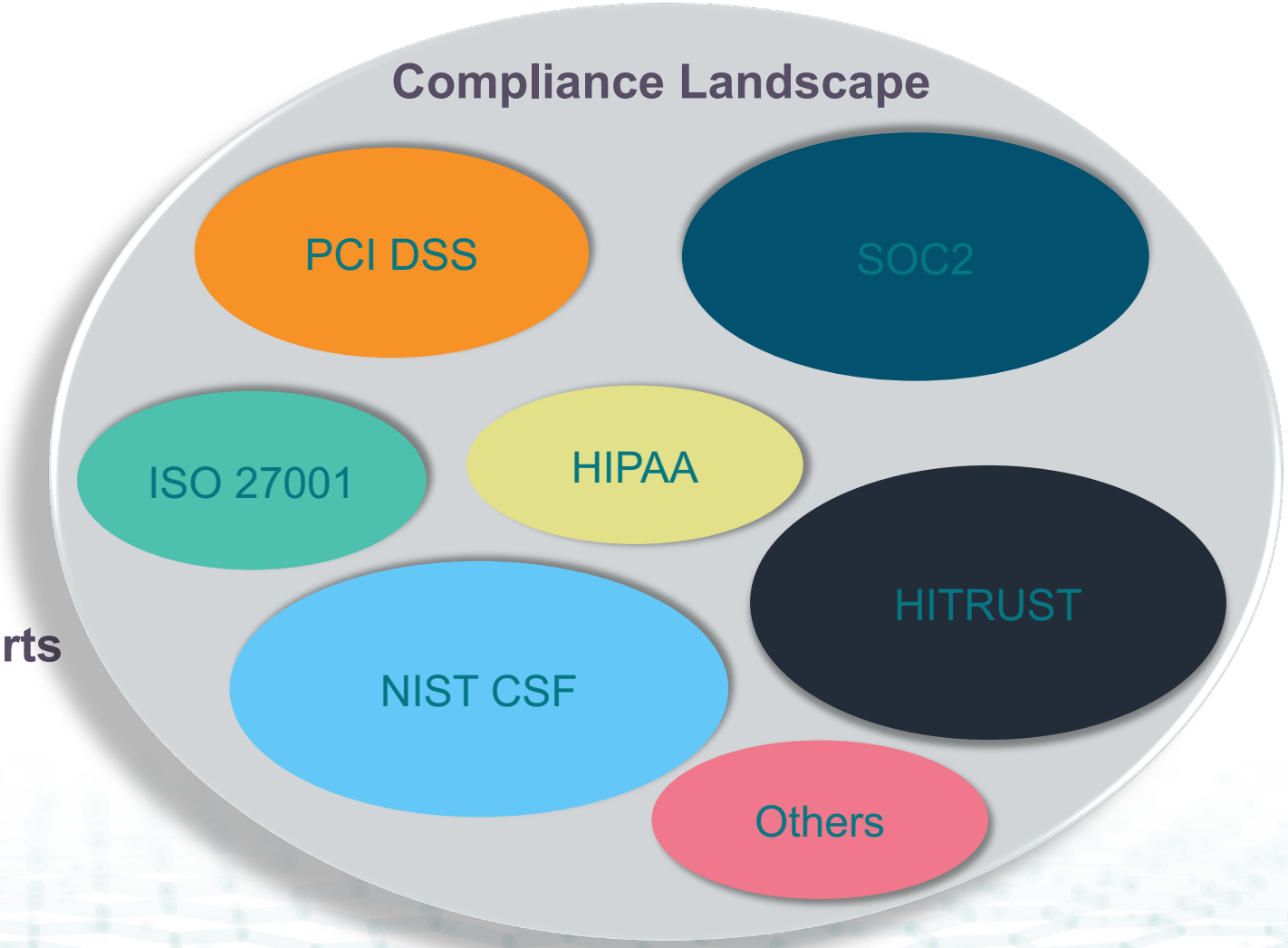
Free up your internal resources to **focus on other priorities**

Improve efficiencies by doing more with less resources and gain compliance peace of mind



The Compliance Landscape

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



PCI Security Standards Council

Why PCI DSS to Consider for Cross walking?

- 6 Goals and 12 Requirements
- Intended for Entities that :
  - Store, process, or transmit cardholder data (CHD) and/or
  - Sensitive authentication data (SAD) or
  - Could impact the security of the cardholder data and/or sensitive authentication data.
- Covers widely used system components
- Prescriptive and specific
- Defined and Customized approach

Goal 1: Build and Maintain a Secure Network and Systems

- Requirement 1: Install and Maintain Network Security Controls
- Requirement 2: Apply Secure Configurations to All System Components

Goal 2: Protect Account Data

- Requirement 3: Protect Stored Account Data
- Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Goal 3: Maintain a Vulnerability Management Program

- Requirement 5: Protect All Systems and Networks from Malicious Software
- Requirement 6: Develop and Maintain Secure Systems and Software

Goal 4: Implement Strong Access Control Measures

- Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know
- Requirement 8: Identify Users and Authenticate Access to System Components
- Requirement 9: Restrict Physical Access to Cardholder Data

Goal 5: Regularly Monitor and Test Networks

- Requirement 10: Log and Monitor All Access to System Components and Cardholder Data
- Requirement 11: Test Security of Systems and Networks Regularly

Goal 6: Maintain an Information Security Policy

- Requirement 12: Support Information Security with Organizational Policies and Programs

PCI Security Standards Council®

Common IT Compliance Standards

	PCI DSS	ISO 27001	SOC	HITRUST	GDPR	FedRAMP	CMMC
Why you need?	Protect Account Data	Establish ISMS	Evaluate, test, and report on the effectiveness of the service organization's internal controls	Safeguard PHI and other regulated data	Safeguard PII	US federal information	Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)
Standard Version	4.0.1	27001:2013 and 27001:2022	SSAE 18, AT-C	9.6	(EU) 2016/679	5	2
Approx Controls	300+	11 clauses, 93 controls	200+	500+	150+	1000+	110
Qualified Auditor	QSA	Certifying Body	CPA	CCSFP	Privacy Assessor	3PAO	3PAO
Non Compliance Consequence	Fines/Penalties by Card Brands	Regulatory Body/Customer obligations	Regulatory Body/Customer obligations	Regulatory Body/Customer obligations	Fines based on tiers up to $1.5 million for each violation	Regulatory Body/Customer obligations	Regulatory Body/Customer obligations

PCI Security Standards Council®

Cross Walking Methodology

Step 1
Identify common control objectives

Step 2
Map controls across standards

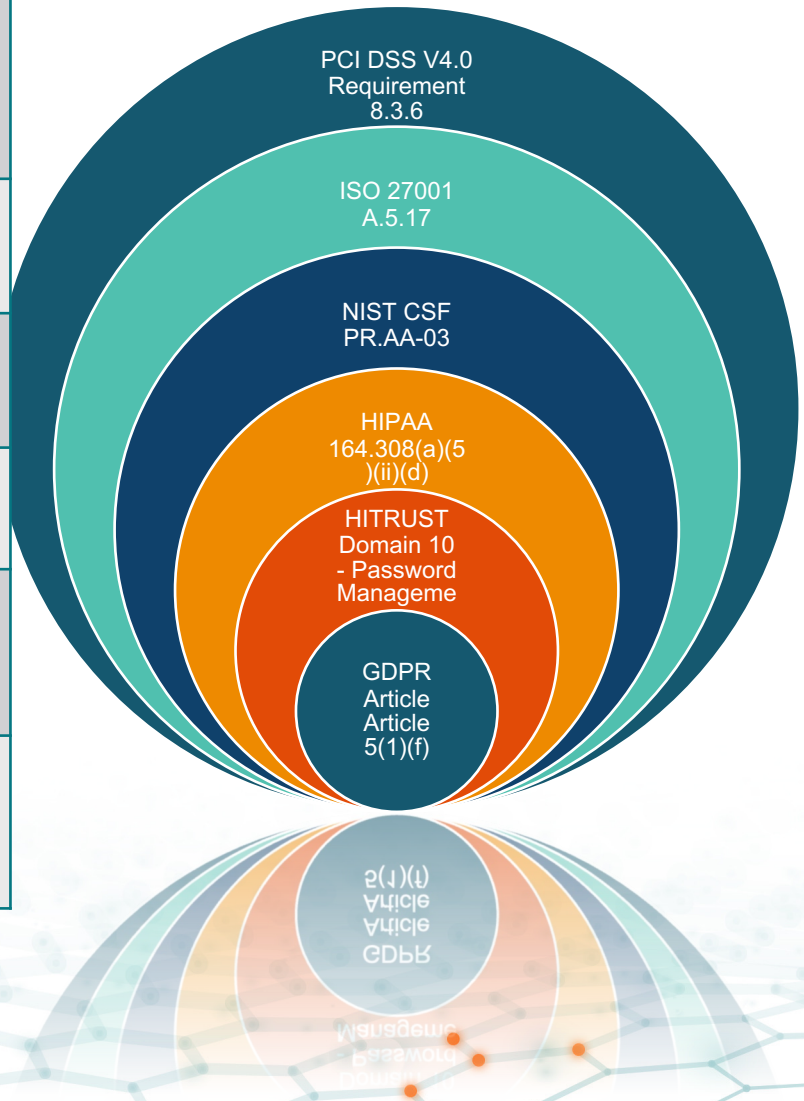
Step 3
Analyze gaps and overlaps

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

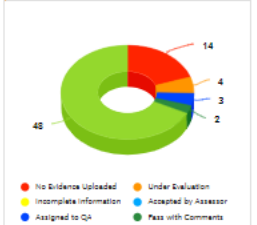
PCI Security Standards Council®

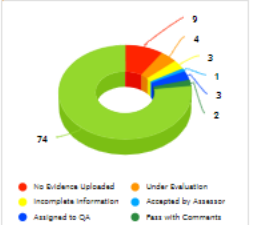
Practical Example – Password Management

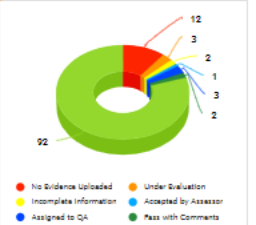
PCI DSS V4.0 **Requirement 8.3.6**	8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters • Contain both numeric and alphabetic characters.
ISO 27001 **A.5.17**	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.
NIST CSF **PR.AA-03**	Users, services, and hardware are authenticated Enforce policies for the minimum strength of passwords, PINs, and similar authenticators
HIPAA **164.308(a)(5)(ii)(d)**	Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.
HITRUST **10 - Password Management**	Allows users to select long passwords and passphrases
GDPR **Article 5(1)(f)**	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

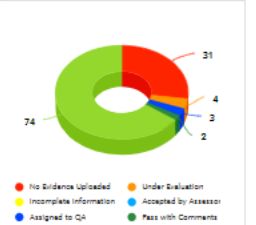


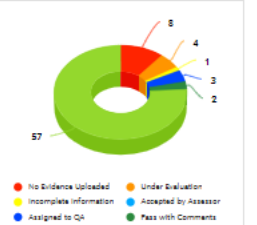
PCI Security Standards Council

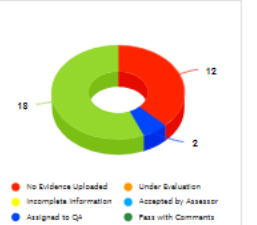
Add-on HIPAA


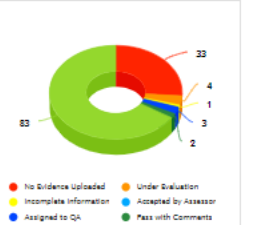
Add-on PCI DSS 3.2.1


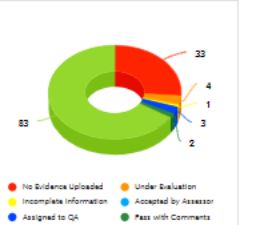
Add-on ISO 27001


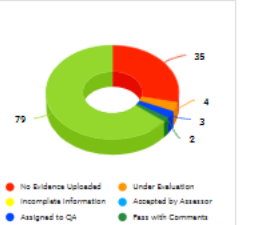
Add-on NIST 800-53 (MODER...


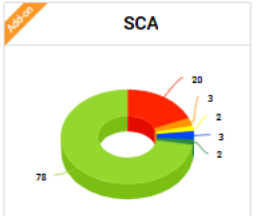
Add-on NIST 800-171


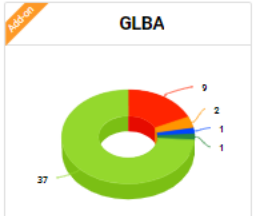
Add-on CCPA


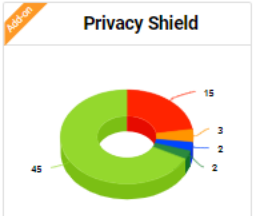
Add-on MARS-E V 2.0


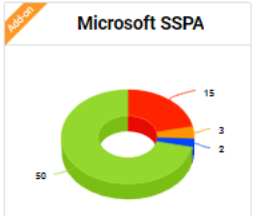
Add-on CMS ARS V 2.0


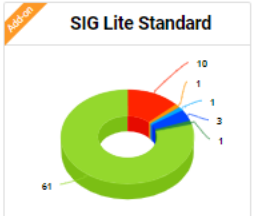
Add-on NIST 800-53


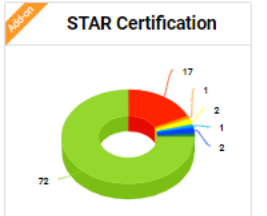
Add-on SCA


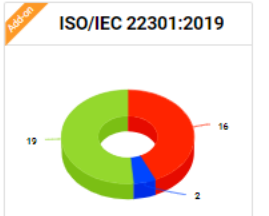
Add-on GLBA


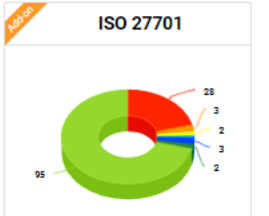
Add-on Privacy Shield


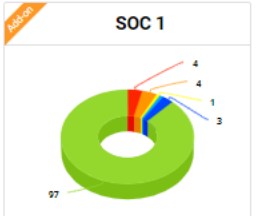
Add-on Microsoft SSPA


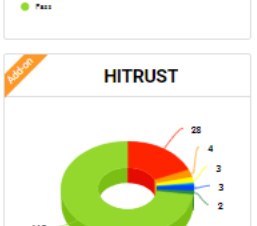
Add-on SIG Lite Standard


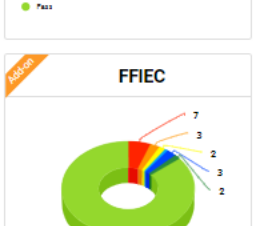
Add-on STAR Certification


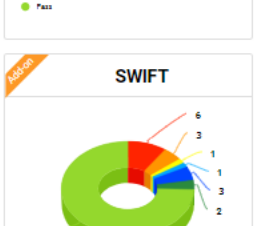
Add-on ISO/IEC 22301:2019


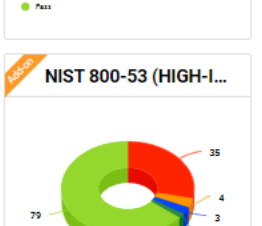
Add-on ISO 27701


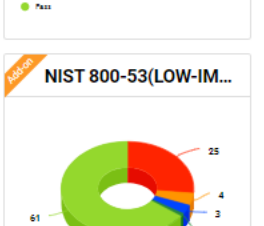
Add-on SOC 1


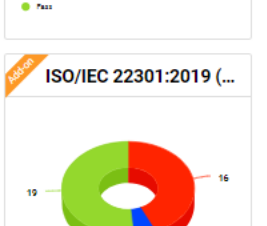
Add-on HITRUST


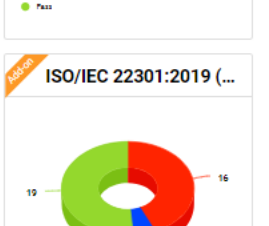
Add-on FFIEC


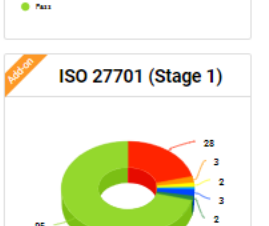
Add-on SWIFT


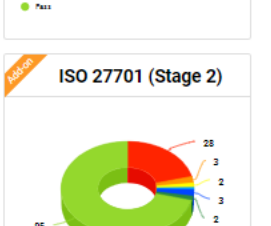
Add-on NIST 800-53 (HIGH-I...


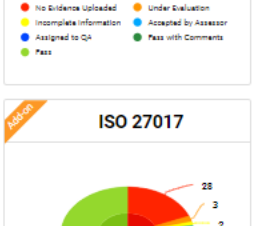
Add-on NIST 800-53(LOW-IM...


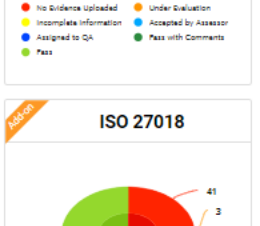
Add-on ISO/IEC 22301:2019 (...


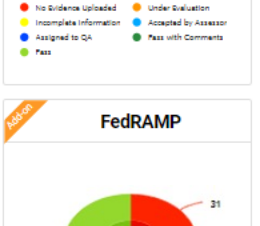
Add-on ISO/IEC 22301:2019 (...


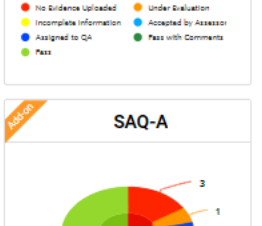
Add-on ISO 27701 (Stage 1)


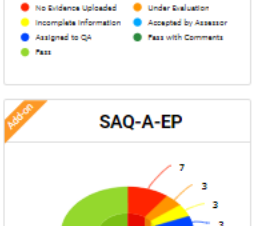
Add-on ISO 27701 (Stage 2)


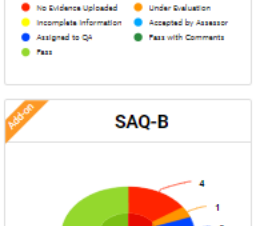
Add-on ISO 27017


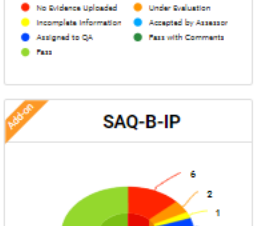
Add-on ISO 27018


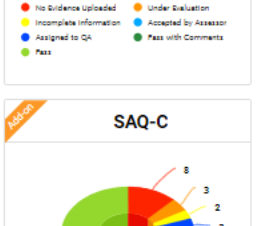
Add-on FedRAMP


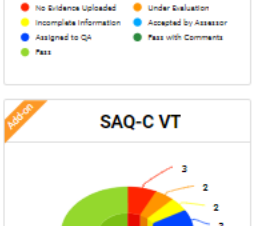
Add-on SAQ-A


Add-on SAQ-A-EP


Add-on SAQ-B


Add-on SAQ-B-IP


Add-on SAQ-C


Add-on SAQ-C VT


Add-on SAQ-D Merchant

Add-on SAQ-D Service Provider

Add-on SAQ-P2PE

Add-on CJIS 5.9

Add-on CMMC 2.0

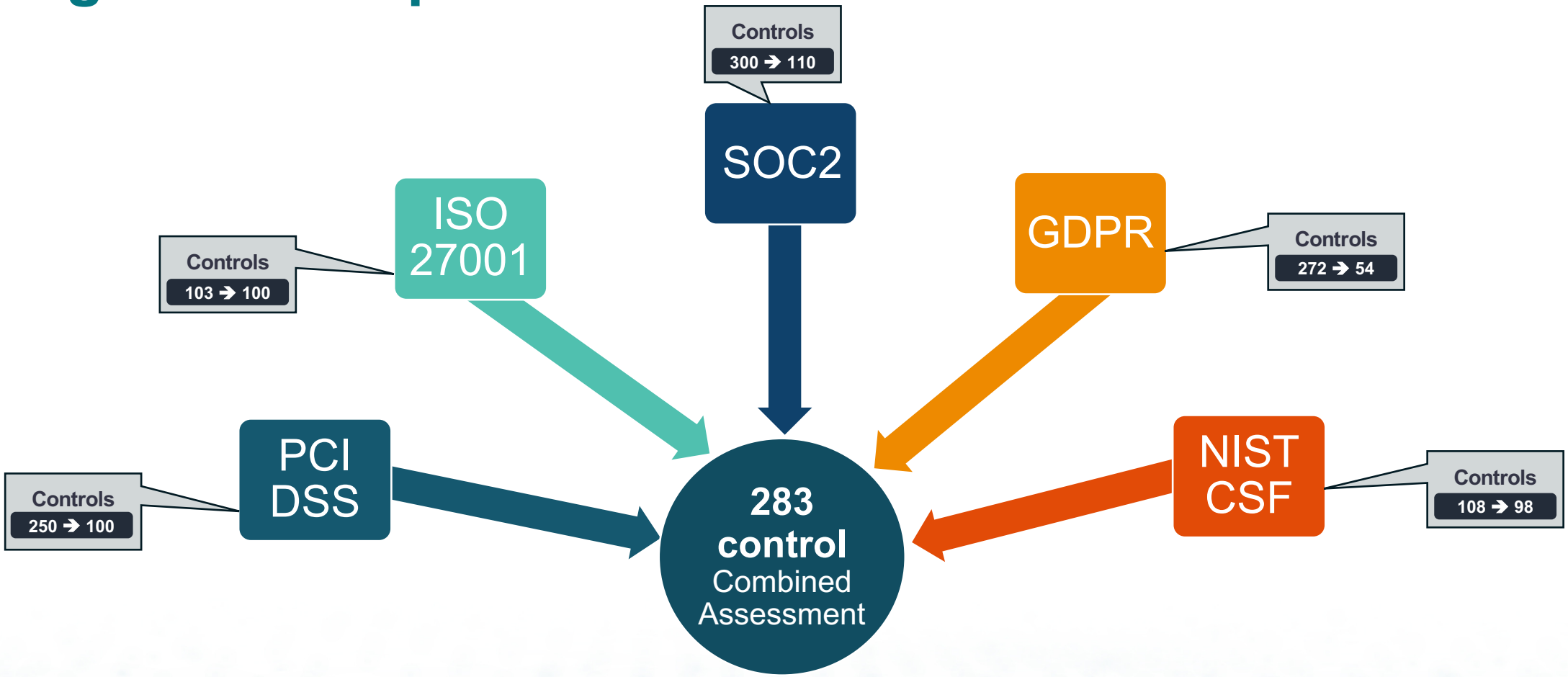
Add-on EBA Guidelines

Add-on MARS-E V 2.2

Add-on Cyber Essentials UK

Add-on SAQ A - V4.0

Integrated Compliance



- ✓ Makes you audit ready for well-known Industry Standards
- ✓ Sets up Information Management System
- ✓ Evaluation of your systems for internal control
- ✓ Coverage of Privacy aspects
- ✓ Defines the entire breadth of cybersecurity

PCI Security Standards Council

Benefits and Challenges

Benefits:

- Reduced compliance costs
- Streamlined audits
- Improved overall security posture
- Better resource allocation

Challenges:

- Initial time investment
- Keeping up with standard changes
- Addressing standard-specific nuances
- Convincing stakeholders

PCI Security Standards Council®

Best Practices

Use automated tools for mapping and tracking

Involve experts from different compliance domains

Regularly update your crosswalk as standards evolve

Focus on the intent behind requirements, not just the letter

Leverage existing frameworks and pre-built crosswalks

Document your methodology and decisions

Key Takeaways

PCI DSS can

- streamline your compliance efforts
- reduce costs
- and improve your overall security posture

The goal

- create a unified compliance framework
- that meets multiple standards efficiently

How to proceed

- start small, perhaps with just two standards
- gradually expand your crosswalking efforts


PCi
Security
Standards Council
®