Elevating PCI DSS v4.0 Compliance

CONVERGE
TECHNOLOGY SOLUTIONS
CYBERSECURITY

Speakers

HOST

Tony Petcou
Sr. Director
Cybersecurity

PRESENTING QSAs

Anton Abaya
Practice Manager
GRC & Cloud Security

Josh Berry
Practice Lead
Advanced Testing & GRC

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

Agenda

MEET CONVERGE CYBERSECURITY

THE PCI v4.0 RUNWAY

NEW REQUIREMENTS DEEP DIVE

QSA Q&A | WRAP UP

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

Converge Overview

Advanced Analytics

- AI/ML
- Business Analytics
- Data Visualization
- Data Platforming & Integration
- Financial & Operational Mgmt.
- Robotic Process Automation

Application Modernization

- Application Development & Migrations
- DevOps
- Containers Services & Kubernetes
- Automation & Orchestration
- Observability & Intelligent Ops
- Integration & Middleware

Cloud Platforms

- Cloud Foundations & Landing Zones
- Cloud Migrations
- IBM Power on Cloud
- VMware on Cloud
- Infrastructure as Code & Automation
- Cloud Governance & Operations
- FinOps & Cost Optimization

Cybersecurity

- Advanced Testing
- Governance, Risk & Compliance
- Incident Response
- Architecture & Integration
- Strategic Staffing
- Managed Security

Digital Infrastructure

- Datacenter & Compute
- Intelligent Networking
- Customer Experience
- Multi-site Deployment
- Configuration Centers
- Infrastructure Security

Digital Workplace

- Voice & Unified Communications
- Workplace Productivity Solutions
- Endpoint Management Solutions
- Virtual Desktop Solution
- End User Compute

GIDS

- Planning/Acquisition
- Configuration
- Deployment
- Support
- Management
- Retirement/Disposal

Advise

- Architecture Planning & Insights
- Roadmap Design & Prioritization
- Software Asset Management
- Strategic Transformation Workshops & Assessments

Implement

- Agile Methodology & DevSecOps
- Build & Design
- Integration & Support
- Program & Project Management
- Talent Services

Manage

- Service Desk & Managed ITSM
- Managed Applications (AMS)
- Security Operations Center (SOC)
- Infrastructure Operations Center (IOC)

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

Why Converge Cybersecurity

Advanced Testing

- Application Testing
- Emerging Threats
- Penetration Testing
- Penetration Testing as a Service

Governance, Risk & Compliance

- Cloud Security Compliance
- Regulations & Compliance
- Virtual CISO

Incident Response

- Readiness
- Response

Architecture & Integration

- Cloud Security
- Data & User
- Network
- Threat & Vulnerabilities

Strategic Staffing

- Daily Operations
- Advanced Technology & Controls
- Executive Strategy

Managed Security

- Cloud
- Data Protection
- Detection & Response
- Threat Management

TECHNOLOGY SOLUTIONS

ADVISE → IMPLEMENT → MANAGE

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

Why Converge for PCI Compliance

15+ Yrs.
QSA* Cert.

1,000s Hrs.
Consultation

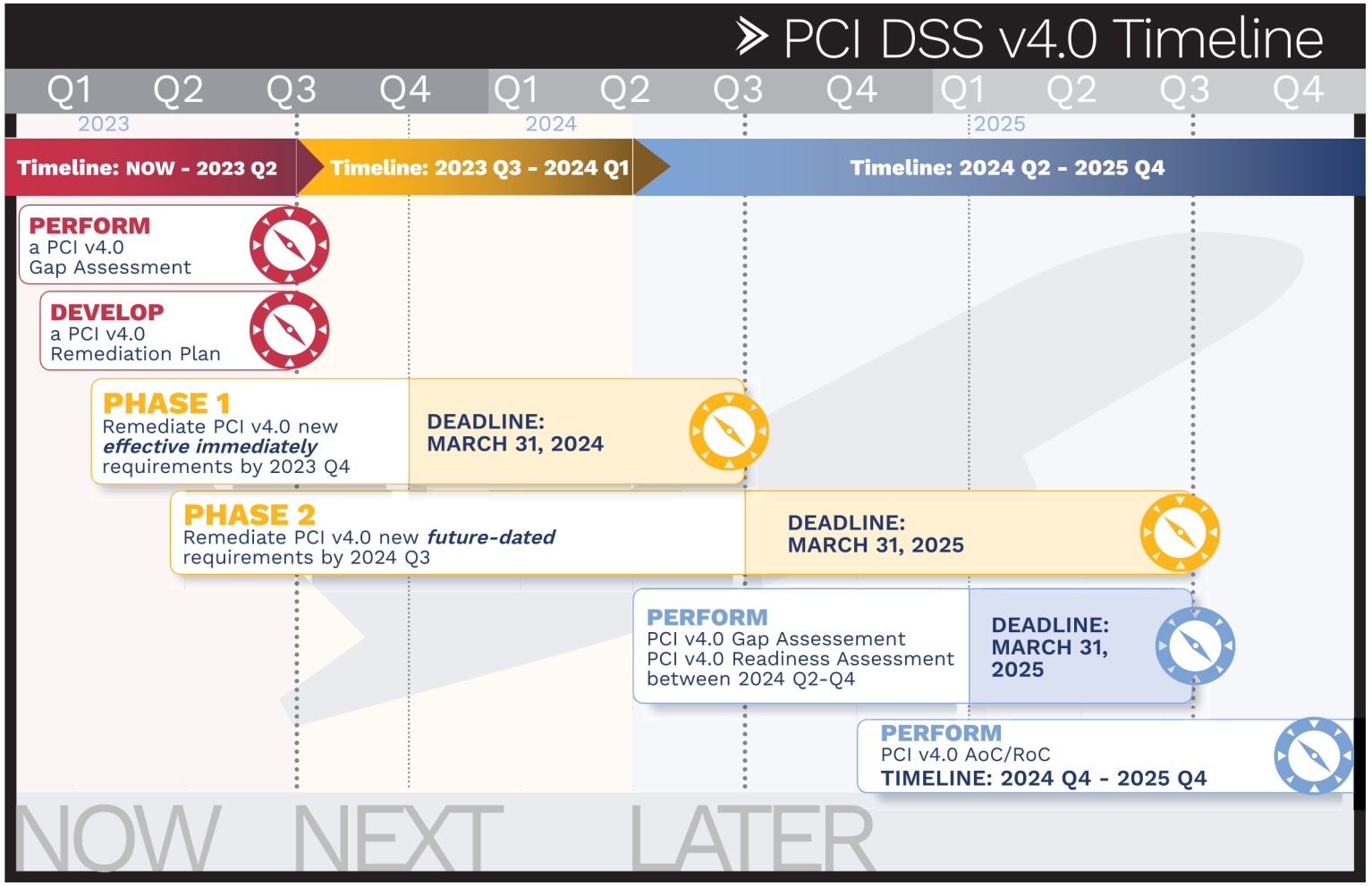
130+ Clients
14+ Verticals

81 NPS
YTD 2023

- Scope & Baseline Assessments
- PCI Penetration Testing
- Gap Assessments
- Risk Assessments
- Compliance Attestations
- QSA Certified

* Via Accudata Systems, A Converge Company

PCI v4.0 Timeline

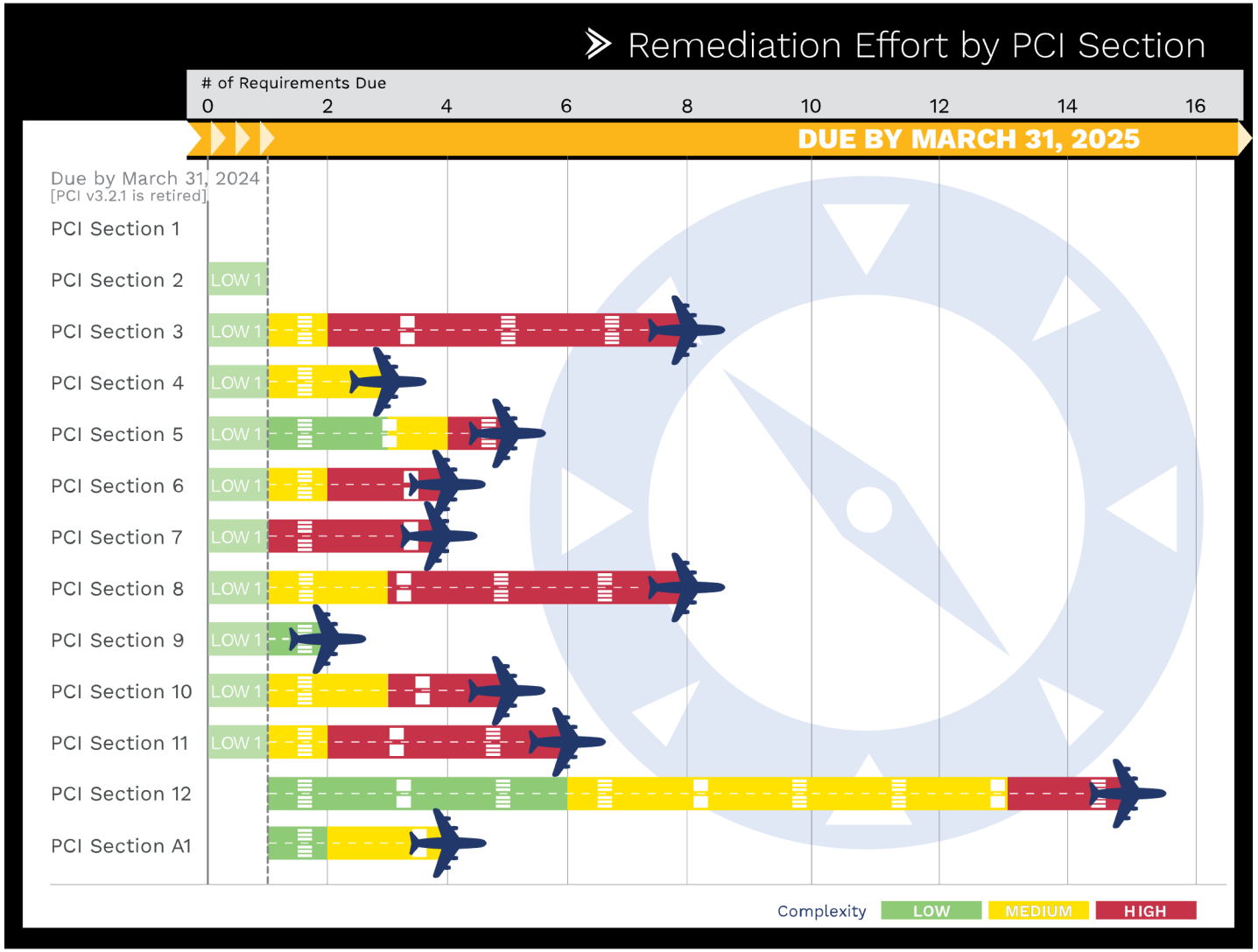


13 ***new*** requirements effective immediately or no later than **March 31, 2024**

50 ***new*** future-dated requirements that must be in place by **March 31, 2025**

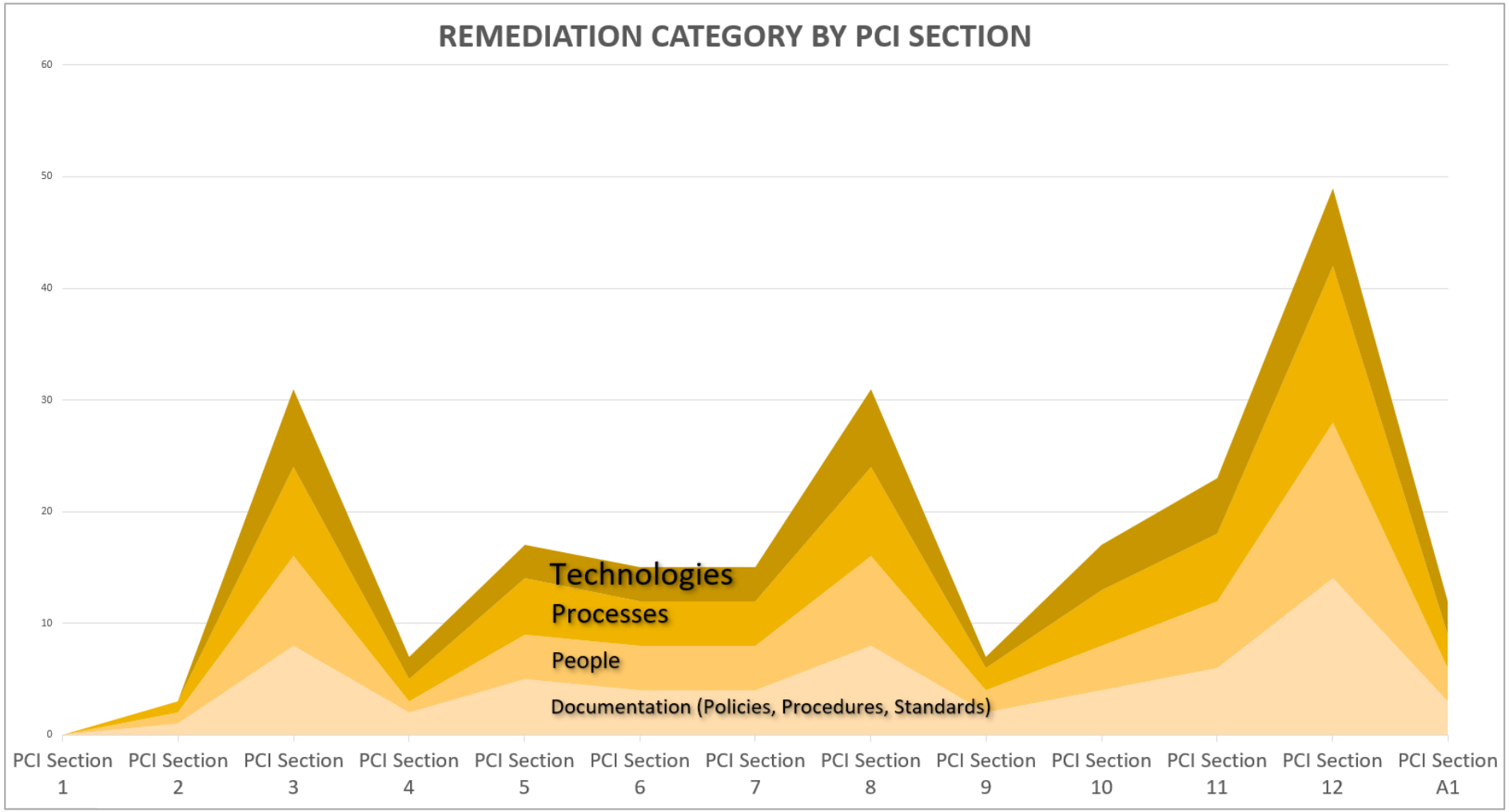
CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

PCI v4.0 Remediation Effort



CONVERGE
TECHNOLOGY SOLUTIONS
CYBERSECURITY

People, Processes & Technology



CONVERGE
TECHNOLOGY SOLUTIONS
CYBERSECURITY

SAQ A for v4.0

eCommerce sites using iFrames & full redirects are significantly impacted by changes to PCI DSS v4.0.

Attackers are targeting ecommerce sites with iFrames & full redirects using a variety of tactics.

CONVERGE
TECHNOLOGY SOLUTIONS
CYBERSECURITY

SAQ A for v4.0

11.3.2 Approved Scanning Vendor (ASV) Scan

MANDATORY | DUE: MARCH 31, 2024 | ACT NOW

3.2.1 Sensitive Authentication Data

COMMON FOR $$$ PURCHASES

6.3.1 | 6.3.2 Security Vulnerabilities

IFRAMES & REDIRECTS DO NOT PROTECT

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

SAQ A for v4.0

12.10.1 Incident Response Approach

EXPANDED IR PLAN **CARD BRAND NOTIFICATION**

TAKEAWAY

eCommerce web servers using iFrames and full redirects for payment ***must*** be protected.

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

eCommerce Attacks

6.4.3

MAR 31 2025

Payment page scripts **loaded & executed in consumer browsers** must be managed with methods confirming script **authorization** and ensuring **integrity.**

Each script, including third- and fourth-party sources, must be **inventoried** with **documented justification.**

11.6.1

MAR 31 2025

HTTP headers and **payment page contents** received in **consumer browsers** must be monitored for **unauthorized modifications** using a change- and tamper-detection mechanism to alert personnel.

This should be done at least **once every 7 days**, or periodically when **indicated by a risk assessment**.

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

Shadow Cardholder Data Environments

12.5.2

MAR 31 2024

Each entity must establish a process to document and **confirm PCI DSS scope** at least **once every 12 months** and with **significant change** to the in-scope environment, including:

- Uncontrolled sprawl of cloud CDEs
- AI and data analytics tools
- Outsourcing ecommerce development
- APIs for web apps and mobile devices
- Mergers and acquisitions

This is **separate** from scoping efforts done during an annual QSA assessment.

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

Authenticated Vulnerability Scans

11.3.1.2

MAR 31 2025

Internal vulnerability scans must be performed through **authenticated scanning.**

Any system that can’t be scanned in this manner must be fully documented.

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

Access Management

8.3.6

MAR 31 2025

Minimum password length must be **12 characters** long, or 8 if the system has limitations.

8.6.1

MAR 31 2025

Interactive login by systems or application accounts must be **prevented** or limited to the time needed for exceptional circumstances that are justified, documented, and approved by management. Individual use must be confirmed before access is granted, and every action must be attributed to the individual.

TAKEAWAY

Use strong user password filters and deploy privileged account management.

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

Defining Periodicity

12.3.1

MAR 31
2025

Requirements with flexible frequency must be supported by a documented, targeted risk analysis to support the timeframe applied. Timeframe definitions are stricter and referenced 22 times in PCI DSS v4.0.

Timeframes	Descriptions and Examples
Daily	Every day of the year (not only business days)
Weekly	At least once every 7 days
Monthly	At least once every 30-31 days, or on the nth day of the month
Every 3 Mos. | Quarterly	At least once every 90-92 days, or on the nth day of each third month
Every 6 Months	At least once every 180-184 days, or on the nth day of the sixth month
Every 12 Mos. | Annually	At least once every 365 days (366 for leap years) on the same date every year
Periodically	Frequency at entity's discretion, documented and supported by risk analysis to demonstrate that the frequency is appropriate for the activity to be effective and meet requirements
Immediately	Without delay | In real time or near real time
Promptly	As soon as reasonably possible

CONVERGE
TECHNOLOGY SOLUTIONS
CYBERSECURITY

Service Providers, Beware of Attacks

11.4.7

MAR 31 2025

Multi-tenant providers must support customer **penetration testing.**

11.5.1.1

MAR 31 2025

Intrusion detection and/or prevention techniques to detect, alert, prevent, and address **covert malware communication** channels must be in place in critical areas, such as **command-and-control servers** (C&C).

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

Service Providers, Beware of Attacks

APPENDIX

A1.1.1

A1.1.4

MAR 31 2025

Logical separation or isolation must **restrict access** between provider and customer environments (provider < -- > tenant). Access to environments requires **explicit authorization**.

Penetration testing must be done every six months to **confirm effectiveness** of the logical separation controls.

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

Phishing for Trouble

5.4

MAR 31 2025

Processes and automation must be implemented to protect personnel from **phishing attacks**.

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

Key Takeaways for Optimal Success

- PCI v4.0 Gap Assessment (ASAP)
- Reduce, Redirect, Isolate
- Cloud Security Assessment
- Data Discovery, Privacy & Protection Assessments
- Control/Limit Cloud Access

- Security, Compliance & Governance Tools
- Secure Authentication Directories | MFA & Vault All Secrets
- Cloud Control Plane Logging & Monitoring
- Prepare for Service Provider Compromise

CONVERGE TECHNOLOGY SOLUTIONS CYBERSECURITY

Thank You!

Connect With Us

Anton Abaya
Practice Manager, GRC & Cloud Security
anton.abaya@convergetp.com

Josh Berry
Practice Lead, Advanced Testing & GRC
josh.berry@convergetp.com

Tony Petcou
Sr. Director, Cybersecurity
tony.petcou@convergetp.com

convergetp.com

CONVERGE
TECHNOLOGY SOLUTIONS
CYBERSECURITY