2024 Asia-Pacific Community Meeting

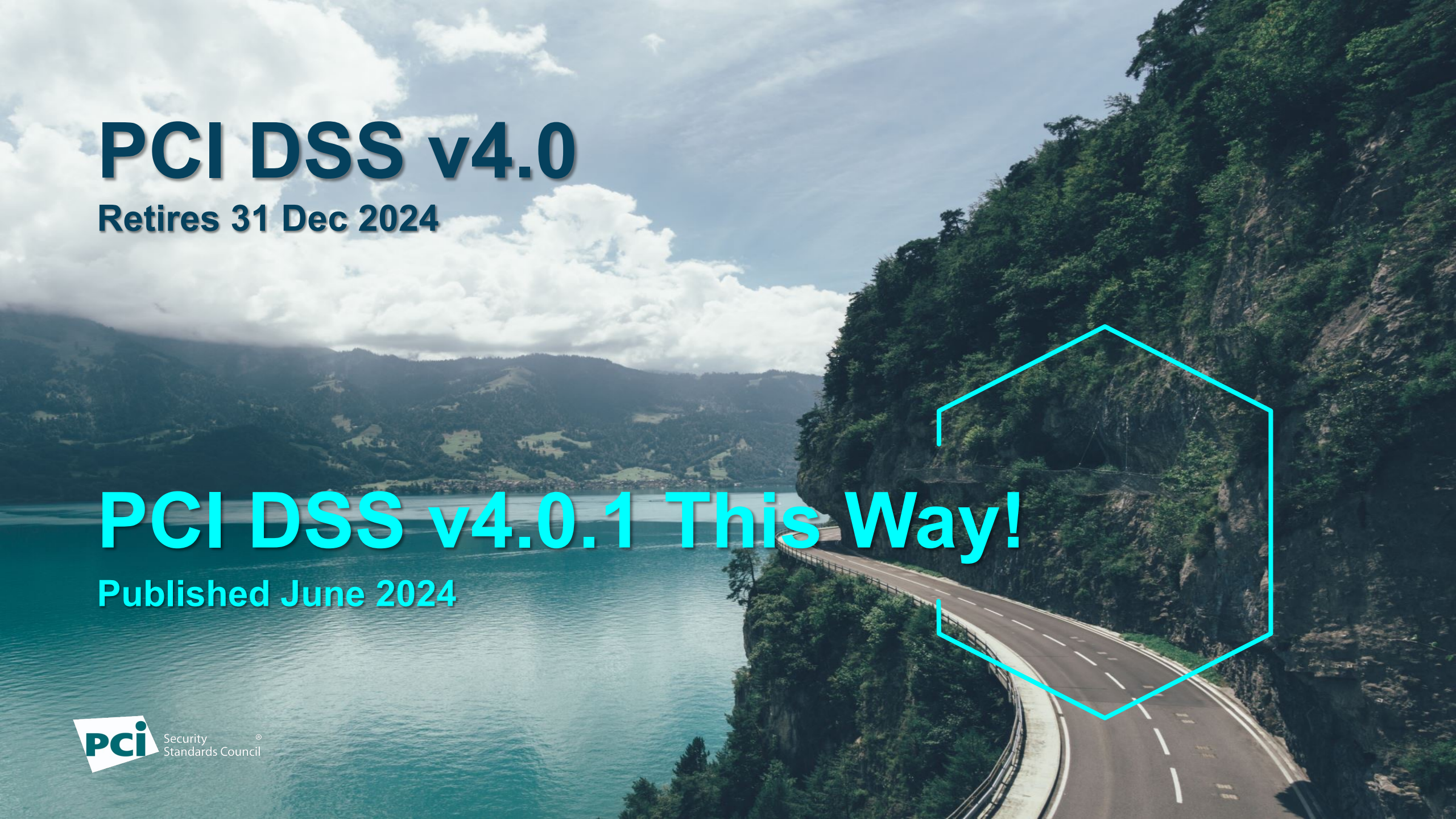
Your Journey Through Key New PCI DSS v4.x Requirements

PCI Security Standards Council®

PCI Security Standards Council

Kandyce Young

Manager, Data Security Standards
PCI Security Standards Council


PCI DSS v4.0
Retires 31 Dec 2024
PCI DSS v4.0.1 This Way!
Published June 2024
PCI Security Standards Council

PCI Security Standards Council®

Network Security Controls

PCI Security Standards Council®

Protect Stored Account Data

- Prohibition of copy/relocation of PAN unless there's a legitimate need
- Encrypted PAN is only decrypted when there's a legitimate need

PCI Security Standards Council®

Protection of Data in Transit

Certificates used to safeguard PAN are confirmed as valid and not expired or revoked.

PCI Security Standards Council®

Anti-Phishing Protection

Processes and automated mechanisms to detect and protect personnel against phishing attacks

Security Awareness training includes information about phishing and related attacks

PCI Security Standards Council®

Payment Page Security Controls

Script inventory must include **business or technical** justification

Alerts on changes to **security-impacting** HTTP headers and the **script** contents of payment pages

PCI Security Standards Council

Scripts!

PCI Security Standards Council®

Scripts!

PCI Security Standards Council®

PCI Security Standards Council®

Automated Audit Log Reviews

PCI Security Standards Council®

Automated Audit Log Reviews

PCI Security Standards Council®

Internal Vulnerability Scans

- Must be *Authenticated* Internal Scans

PCI Security Standards Council®

Internal Vulnerability Scans

- Must be *Authenticated* Internal Scans

PCI Security Standards Council®

Internal Vulnerability Scans

- Must be *Authenticated* Internal Scans

PCI Security Standards Council®

More Flexibility

- Cryptographic Agility
- Targeted Risk Analyses

PCI Security Standards Council®

More Flexibility

- Cryptographic Agility
- Targeted Risk Analyses (TRAs)

PCI Security Standards Council®

Third-Party Service Providers (TPSPs)

- TPSPs must support their customer requests for information to meet requirements

PCI Security Standards Council®

Third-Party Service Providers (TPSPs)

- TPSPs must support their customer requests for information to meet requirements

PCI Security Standards Council®

Multi-Factor Authentication

- *Phishing-resistant authentication factors* may be used for non-console access into the CDE

PCI Security Standards Council®

Multi-Factor Authentication

- *Phishing-resistant authentication factors* may be used for non-console access into the CDE

PCI Security Standards Council®


PCI DSS v4.0.1 This Way!
PCI
Security
Standards Council


PCi
Security
Standards Council
®