# Defining Your Organization's Compliance and Certification Strategy

## P2P1-W08: Defining Your Organization's Compliance and Certification Strategy

**David Graves, Security Architect, Hewlett Packard Enterprise**

**Defining Your Organization's Compliance and Certification Strategy**

Compliance with security standards and legislation is challenging. Thirty security professionals gathered in an informative peer-to-peer session at RSA Conference 2019 to discuss how to navigate through compliance requirements and to share methods for dealing with multiple standards.

**Diverse sectors and requirements**

Our group was diverse, representing Banking, Cloud Computing, Cyber Security, Energy, Health Services, Insurance, IT Security, Manufacturing, Military/Defense, Technology Services, and Transit.

A majority of the participants stated that their organization deals with more than one standard. The most frequently used standards in this group were GDPR, HIPAA, and PCI-DSS. A quick tally of standards used included DISA Cloud, other DISA STIGs, FedRAMP, and FIPS 140.

**Frameworks of Standards**

Some participants shared that they use frameworks of standards as a means of organizing their compliance with multiple standards. The most frequently used framework for our group was the ISO 27001 standard, but also used were Common Criteria, the CSA's Common Controls Matrix, and NIST 800-53. Since many of the standards overlap with other standards, compliance with one standard's controls may mean that you are covering related controls in another standard.

One implementation approach is to start by identifying the security controls required in multiple standards needed by your organization, to get the greatest results for your efforts. After gaining compliance with the overlapping controls, you could prioritize the controls that are outliers, to fill gaps in your compliance strategy, striving for process improvement with maturity over time.

**Privacy Trends**

We agreed that new privacy regulations are driving increased attention to data security. Notable are the UK's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). One participant recommended Jason Cronk's book "Privacy by Design" as teaching good data governance, wrapped in security.

**Where to Get Standards**

Most standards are freely available on the Internet. It was also noted that mappings of security controls (indicating the correspondence of security controls from one standard to another) are available. These mappings can be acquired via keyword search for the standards and frameworks of interest to you using your favorite search engine.

NIST 800-53 is a framework of security controls available as a document or a spreadsheet-readable file. The ISO 27001 framework is available at a nominal cost, but the mappings to other standards are available free of charge by various organizations.

The Cloud Security Alliance publishes the very impressive Cloud Controls Matrix, a framework of security controls including mappings to FedRAMP, HIPAA, the ISO 27001 family, NIST 800-53, PCI DSS, and other standards.