Hewlett Packard Enterprise

Business white paper

Addressing compliance with HPE Security

Table of contents

3 **Introduction**

3 **Complexity is the enemy of security**

4 **Regulatory complexity**
6 Automation
6 HPE Security — Data Security
8 HPE Security — Data Security for PCI compliance
8 GDPR
9 HPE Security ArcSight Logger Compliance Insight Package
10 HPE Security Fortify
11 Summary

12 **About HPE Security**

12 **About HPE Security Products Global Services**

Compliance is a critical component of an effective security program.

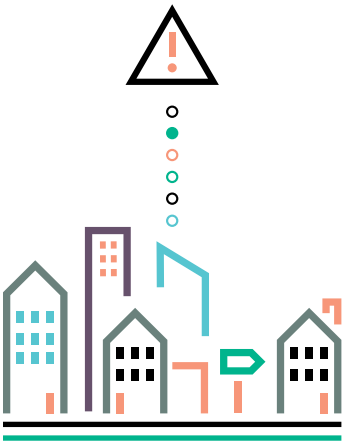
Introduction

Few people would deny that enterprises and governments are facing the most aggressive and complex threat environment in history. The adversaries have become **cleverer, more structured, and more determined** as they seek their prize of information capital and intellectual property. There is a growing sense that the number of cyber threats is proliferating more rapidly than companies can protect against. With technological and regulatory complexity creating a snowball effect, the lack of resources that are specifically skilled in compliance and the continual pressure to do more with less is a common complaint for leaders in the industry today.

Compliance is a critical component of an effective security program. Tight integration between compliance and security competencies will make each stronger than they would be by themselves. Generally, **the most serious risks to any compliance program** are similar to those of overall cyber-risk, such as loss, theft, manipulation, or unauthorized dissemination of important data. This data is often covered by regulatory mandate as well as legal liability expectations, so the costs of non-compliance in terms of fines, sanctions, and other remedies can easily run into millions of dollars annually. According to the **2016 Information Governance Compliance Survey**, half of the companies surveyed are already losing money to non-compliance and most are challenged (93% reported compliance challenges), and the overall compliance risks they face are becoming more severe, regulations are more complex, and the stakes for non-compliance are rising. Most companies already have people devoted to compliance and information governance; however, serious questions remain as to the efficiency of those programs.

Organizations that properly blend security and compliance programs are able to more effectively reduce their attack surface and combat security breaches, as well as meet rigorous compliance rules and regulations at the same time. This is the ideal scenario but isn't always straightforward. Compliance failures can be catastrophic especially concerning regulated industries such as healthcare, government, and banking. When properly implemented, a rigorous compliance and information governance program can reduce an organization's regulatory, legal, and operational risk. However, the road to compliance is never easy and is often very individualized for every organization.

Complexity is the enemy of security. Ninety-three percent of organizations struggle with compliance challenges.



Complexity is the enemy of security

Cost-cutting has been a major buzzword for even the most successful of businesses in recent years. Resources are scarce, but expenses continue to grow, and executives everywhere look to reduce cost wherever possible. Given the vast reduction of resources, the average IT professional is being asked to do more than ever before. IT organizations spend much of their time supporting customers, managing systems, facilitating change requests, administering patches, running scans, writing scripts, managing endless paper work, and much more. For many delivery organizations, compliance is an afterthought until a failed audit, a security breach, or a massive fine. The biggest challenges associated with IT governance, risk, and compliance today are twofold: there are not enough skilled compliance resources, and those resources must keep up with the rapid pace at which the technological and regulatory landscape changes. Organizations want to know how to solve this multifaceted problem. While the problem may be complicated, the solution is simple: where there is a lack of skilled resources to address growing complexity, automated solutions are critical to success.

The idea economy that includes technologies such as cloud, mobile applications, bring your own device (BYOD), virtualization, and social platforms create further complexity in the equation. It is more difficult than ever before for chief information security officers (CISOs) to proactively manage an information security and risk strategy because they are constantly reacting to new threats brought into the organization by these technologies.

PwC's annual **Risk in Review survey** says business executives and risk managers worldwide are struggling with increasing risk across the board. Nearly 60% of executives said they see increased risks related to technological change and information technology, as well as increasing regulatory complexity. Fifty percent of respondents said they also see increased risk related to rapidly changing customer needs due to complexity. The most serious risks to any information governance program are fairly similar to those of overall cyber-risk, such as loss, theft, manipulation, or unauthorized dissemination of data. This data is often covered by regulatory mandate as well as legal liability expectations. The costs of non-compliance in terms of fines, sanctions, and other remedies can easily run into millions of dollars each year. According to the **2016 Information Governance Compliance Survey**, most companies surveyed are already losing money to non-compliance, and the compliance risks they face are becoming more precarious, regulations are becoming more complex, and the stakes for non-compliance are rising. Most companies already have people devoted to compliance and information governance, but serious questions remain as to the efficiency of those programs.

Compliance is complex. Forty-nine percent of organizations reported receiving fines or sanctions in the last few years.

Regulatory complexity

As times have changed, so too have the rules by which organizations, businesses, agencies, and entire industries are expected to conform to. New regulations continue to emerge from obscurity on a daily basis, and compliance staff are often the ones facing the consequences. One of the biggest challenges faced by organizations looking to audit changes is the need to adhere to multiple compliance standards. According to the **2016 Information Governance Compliance Survey**, 49% of organizations reported receiving fines or sanctions in the last few years due to regulatory non-compliance. Many organizations are responsible for adhering to the demands of the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI DSS), the Federal Information Security Management Act (FISMA), the Federal Risk and Authorization Management Program (FedRAMP), IRS Publication 1075, the General Data Protection Regulation (GDPR), National Institute of Standards and Technology (NIST standards), and a multitude of other audit standards, all at once.

Overall, regulatory compliance boils down to proactively accessing, managing, and understanding information (that is, data). Whether it is healthcare information, credit card data, personally identifiable information (PII), tax information, or some other form of sensitive information that needs to be controlled with the proper insight, Hewlett Packard Enterprise has a solution to help.

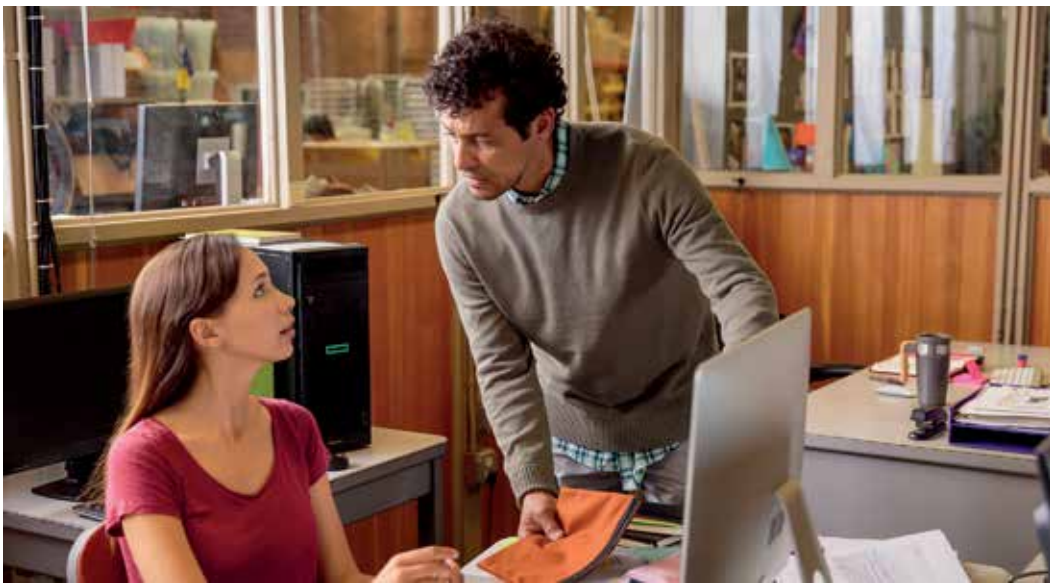


Table 1. HPE product mapping for applicable regulatory frameworks involved in common data privacy regulation compliance

Regulatory framework	Jurisdiction/Scope	Applicable products	Compliance benefits
PCI DSS 3.2	Global—Any entity credit cards	HPE ESKM, HPE SecureData, HPE SecureData Payments, HPE SecureMail, HPE SecureData Web, HPE SecureData Mobile	HPE SecureData: PCI scope reduction (up to compliance cost reduction [up to 95%] protection while in use, in motion, at rest)
GLBA	U.S.—Insurance industry	HPE SecureMail (for data shared to, for example, independent agents), HPE SecureData	Meets best practice data protection to avoid enforce controls for data at rest and audit
U.S. state privacy laws: California S.B. 1386 section 217	U.S.—All businesses' personal data	HPE SecureMail, HPE SecureData, HPE ESKM	Meets best practice data protection to avoid enforce controls for data at rest and audit
UK, ICO, Data Privacy	UK—All businesses' personal data	HPE SecureMail, HPE ESKM, HPE SecureData Enterprise	Meets best practice data protection to avoid enforce controls for data at rest and audit
GDPR	Global—EU and anyone handling EU data	HPE SecureMail, HPE ESKM, HPE SecureData Enterprise	Meets recommended pseudonymization and requirements; enforce controls for data at compliance
PIPEDA	Canada—Any business' personal data	HPE ESKM, HPE SecureData, HPE SecureData Payments, HPE SecureMail, HPE SecureData Web, HPE SecureData Mobile	Meets best practices for data protection in regulated data; enforce controls for data at compliance
HIPAA/HITECH	U.S. healthcare entities' sensitive data	HPE ESKM, HPE SecureData, HPE SecureData Payments, HPE SecureMail, HPE SecureData Web, HPE SecureData Mobile	Meets data privacy rule requirements for enforce controls for data at rest and audit

This is not an exhaustive list—a compendium of international data privacy laws and security requirements by country is available here: **edrm.net/resources/data-privacy-protection/bakerhostetler-data-privacy-laws**

More extensive information on additional U.S. laws is available here: **us.practicallaw.com/6-502-0467**

Automation (and reporting) will lower complexity.

There is a point of diminishing returns when it comes to headcount and compliance, and that point gets closer to zero the more automation is integrated into the system.

Automation

Hiring more people into the compliance function was only seen by **47% of survey respondents** as being effective. The reality is that, in many operations, there is a point of diminishing returns with regard to compliance headcount, and that point gets closer to zero the more automation is integrated into the system.

The easiest way to reduce pressure on existing IT staff is with automation solutions. Due to lack of governance and compliance skilled resources, companies are desperate for tools to alleviate the staffing burden, as well as assist in building and maintaining their information governance and compliance programs.

The following is a sampling of some of the solutions where HPE solutions can assist with the daunting task of automating security and compliance initiatives.

HPE Security — Data Security

HPE Security — Data Security is a leader in data-centric security safeguarding data throughout its entire lifecycle—at rest, in motion, or in use—across the cloud, on-premises, and in Big Data and mobile environments, with continuous protection. HPE Security — Data Security with HPE SecureData with Hyper Format-Preserving Encryption (FPE), is a next-generation high-performance FPE for virtually unlimited data types. Strengths of HPE Security — Data Security include:

- HPE SecureData with Hyper FPE enables GDPR compliance for encryption and pseudonymization while remaining transparent to critical business processes that require a consistent data format for companies hosting sensitive PII in structured form, whether in production apps and databases, Big Data analytics and warehouse environments, or public and hybrid cloud applications.
- It helps protecting PII across its full lifecycle, whether at rest, in motion, or in use, across nearly all data breach vectors, to provide complete end-to-end coverage to structured data falling within GDPR scope.
- HPE Enterprise Secure Key Manager (ESKM) along with application partners provide standardized interoperability for data-at-rest encryption using high-assurance key management for companies with undifferentiated bulk and unstructured PII across heterogeneous HPE or multivendor storage.
- For customers focused on data breach vectors such as loss or misuse of physical tape or disk media, and looking to make accelerated progress towards GDPR compliance, plugging in key management to existing encryption-ready systems by using a turnkey appliance is an easy first step to ensure broad-based data-at-rest coverage and minimize risk at a global data center infrastructure level.

Table 2. Purchase triggers and pain points

Pain point	Purchase trigger
What is my readiness status?	• Deadline of May 2018 that is fast approaching • Need for initial internal awareness in 2016 to get resources on board for GDPR implementation • Urgent need for group-wide risk assessment to identify how prepared the company is under existing national and EU regulation, including its technology facilities
Where is the information that will fall under these regulations?	• Firstly need to accept that information in any format is to be addressed—Hard copy, audio, visual, and alpha-numeric • Need to assess connectivity to all sources of data in all jurisdiction, which may contain EU PII • Issue of ability to unify records to provide a 360° view of a private customer • Issue of PII arising even in B2B corporate, for example, employees' data as well as that required for due diligence from agents, distributors, and so on • Challenge of impacting no-EU subsidiaries that nonetheless deal in/access EU PII
How can I cost-effectively respond to legal matters requiring information under my management?	• Do I have the legal policies and procedures in place to meet GDPR requirements? • Have I trained my staff? • What technology am I using to isolate information required by in-house counsel, compliance, risk? • Do I rely on internal or external counsel for breach reporting or handling?
How do I best ensure sensitive data is protected, stored, and backed up securely?	• How effective is my total records management? • How easily can I identify breach both externally by cyber hacking as well as employee misdemeanor or mistake? • What existing cyber defense do I already have in place? • What encryption and anonymization do I have as policy, procedure, data access, security mapping, and technology implementation? • How strong is my existing backup to ensure PII is safeguarded? • How effective is my retention policy enforcement for the defensible deletion of data?
How do I identify information for disposition, in accordance with "the right to be forgotten"?	• Need legal advice as to how PII is defined • Need a policy enforcement tool to enable policy to be enforced • Need multidata format access, correlation, and accrual of PII across possible multiple silos and jurisdictions to be able to assure complete deletion
Can I report a breach within the timeline required by the regulation?	• Seventy-two hours is a tough target to reach—meaning that a comprehensive and defensive policy and system need to be in place • Need for alerting mechanism for security breach to be provided in the form of technology-assisted monitoring • Need for well-trained compliance staff who are able to use technology and effect the reporting required to national data protection regulators
How do I reduce my overall risk profile?	• Depend on a sound and rigorous risk assessment of policy, procedure, and technology • May require technology investment to achieve risk reduction • Need to have both proactive defense as well as post-event handling to protect reputation and avoid enforcement both in terms of fines and business-limiting criminal enforcement

HPE Security — Data Security for PCI compliance

Customers must mitigate against risk of data breach and address PCI compliance. HPE SecureData addresses both challenges and additionally is differentiated by standards-based technology, stateless tokenization, stateless key management, and the ability to significantly reduce attack surface, as well as PCI audit scope (which then translates to major compliance cost savings). When an enterprise collects credit card data, at swipe or in browser, it is subject to PCI audits and must meet the minimum criteria for protecting that sensitive data. PCI DSS is a set of requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. Compliance with these standards earns consumer trust and helps to protect against data breaches. This is real ROI for customers.

Benefits for existing customers

- Secures sensitive Payment Account Number (PAN) data via tokenization
- Enables enterprises and merchants to completely remove stored credit card data from their environments
- Helps pass PCI audits and significantly reduce compliance audit scope and costs
- Enables business processes and analytics to be run on de-identified data

Benefits for new prospects

- Protects credit card (PAN) data from breach
- Protects brand and reputation
- Enables both tokenized and de-identified data to meet business needs

GDPR

The GDPR is a new privacy law enacted by the European Union (EU) that gives citizens control over how and where their personal data is used. The legislation impacts controllers'—organizations that determine the purposes and means of the processing of personal data and processors—organizations that process personal data on behalf of a controller. Processors must also impose the same data protection obligations on their subprocessors (subcontractors). GDPR is applicable worldwide—wherever EU citizen personal data exists. Enforcement of the GDPR begins on 25 May 2018 and the regulation provides for substantial financial penalties for non-compliance. For example, the GDPR has a two-tier fining system for non-compliance. The lower tier sets fines up to a maximum of the greater of 10 million Euros or 2% of the company's global revenue. The higher tier sets fines at a maximum of the greater of 20 million Euros or 4% of the company's global revenue. GDPR also mandates the addition of a data protection officer (DPO) to any business that has at least 250 EU-based employees or processes personal data of at least 5000 EU citizens.

Many organizations are examining encryption and pseudonymization technologies; however, they quickly discover the complexities and management overheads with traditional approaches. FPE allows a highly granular approach to encryption, which facilitates field-level protection. It also preserves business functionality, meaning that normal data processing activities are maintained even though the data is encrypted. HPE FPE fulfills both encryption and pseudonymization functions, which makes it a particularly useful technology in the context of providing some assistance with GDPR compliance.

Hewlett Packard Enterprise provides comprehensive solutions to assist customers with some of the technical aspects of GDPR including the following:

- Identify personal data and apply records management controls
- Encrypt and de-identify personal data such that it remains protected even if a data breach takes place. The personal data remains encrypted from the point of capture, in transit, and in use. Personal data can still be used for analytics

- Identify attempts to breach information security controls rapidly enabling operations teams to focus their attention on containing breaches
- Enhance the security quality of application code significantly (on the web, mobile, and PCs or servers) by identifying vulnerable code and automatically providing detailed guidance on code remediation

Information governance solutions help organizations meet some of the GDPR requirements for identifying, applying policy to, and protecting targeted information throughout its lifecycle, including personal data.

HPE ControlPoint (unstructured data) and HPE Structured Data Manager (SDM) (structured data) enable information classification, and powered by rich HPE analytics, these technologies bridge formerly distinct data silos, deliver granular insight into information, and surface only the most critical and sensitive data. It is personal data armed with deep insight into customer data; organizations can streamline and drive cost-efficiencies into the process of protecting, leveraging, and taking action on this information. The HPE Digital Safe Suite offers leading compliance archiving, supervision, and surveillance solutions that have been proven and are relied upon by many of the largest global organizations to help protect them from the significant financial and legal risk.

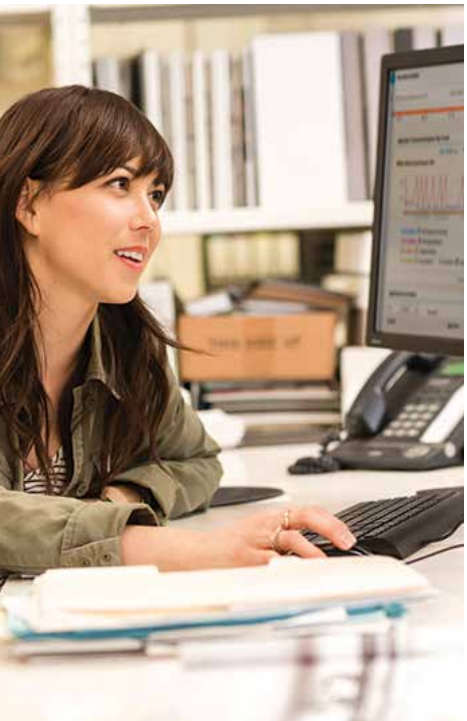
This is an ideal opportunity for organizations to review their entire security posture, with a view of understanding the processes and controls that need to be implemented to protect the privacy of EU citizens. HPE Security — Data Security with HPE SecureData with Hyper FPE specifically meets encryption and pseudonymization criteria. HPE Security ArcSight provides an excellent way to detect the early stages of attacks having filtered out false positives automatically using Big Data analytics. HPE Security Fortify identifies weaknesses in source code automatically and protects running applications from attack to enable breaches to be prevented.

HPE Security ArcSight Logger Compliance Insight Package

HPE Security ArcSight Logger Compliance Insight Package (CIP) for IT governance is ideal for organizations that implement a governance program, either independently or as the foundation of an IT regulatory compliance initiative. Combined with the HPE Security ArcSight Enterprise Security Manager (ESM) or HPE Security ArcSight Data Platform products, the CIP for IT governance provides companies and government organizations the ability to identify and assess the effectiveness of internal controls. A host of ready-to-use technical and business-level checks, in an easily customizable package with dashboards, are presented in accordance with the ISO/IEC 27002:2005 and NIST SP 800-53 standards. These checks help automate review and demonstrate whether controls are effectively implemented, monitored, and maintained.

The HPE Security ArcSight CIP for IT governance creates a centralized view of critical assets with regard to event logs. It allows organizations to automatically and easily leverage the powerful collection capability of dedicated security solutions to meet compliance requirements. This eases the cost and complexity to identify critical issues and therefore helps organizations avoid risk as well as achieve compliance efforts. HPE Security ArcSight helps make governance and compliance programs more efficient, effective, and auditable. The CIP for IT governance is tuned to help organizations perform the following automatically:

- Review event and log data on an ongoing basis
- Store logs online and in long-term archives
- Meet forensically sound practices
- Prepare and demonstrate compliance for auditors



Focused tracking of administrative activity, for example, provides separation of duties control, for a common audit request—review of administrative activity related to access controls for regulated systems. The CIP for IT governance reveals administrative users and their activity via unique functionality that easily fulfills requirements for logging and monitoring.

HPE Security Fortify

Application security is a critical element for the enterprise wishing to be PCI compliant. Application attacks compromise the logic flow and data handling from within the application, affording access to sensitive data and more. Identifying and removing vulnerabilities during development and testing, and protecting vulnerabilities that may remain in production, are the most effective ways to reduce these risks.

Compliance requirements can drive change in the information security field, but it's important for firms to deploy a diverse toolset that will cover more than just compliance. The HPE Security Fortify suite does both by checking several compliance initiative requirements, such as PCI DSS, while bringing relevant and current countermeasures to information security professionals.

The HPE Security Fortify application security suite has a long-standing history in application defense. The portfolio expands beyond static code analysis into a fully integrated suite of products that help meet several compliance initiatives and standards including PCI DSS, FISMA, HIPAA, North American Electric Reliability Corporation (NERC)/Federal Energy Regulatory Commission (FERC), and ISO 27000.

- **HPE Security Fortify Static Code Analyzer (SCA)** is a static application security testing (SAST) used by development groups and security professionals to analyze the source code of an application for security vulnerabilities. It reviews code and helps developers identify and resolve issues with less effort and in less time.
- **HPE Security Fortify DevInspect,** integrated within the development environment, provides immediate and continuous feedback to the developer on security vulnerabilities within their existing workflow. DevInspect improves the security of software by helping developers identify and remove application security vulnerabilities as code is written.
- **HPE Security Fortify WebInspect** is a web application security assessment solution designed to scan web applications and web services thoroughly for security vulnerabilities. It is an essentially automated penetration testing.
- **HPE Security Fortify Application Defender** is a run-time application self-protection solution (RASP). It deploys into Java and .NET applications by sitting in the byte code interpreters that run them. This allows for a quick deployment without changing source code and without a recompile. It can monitor and protect custom code or commercial off-the-shelf applications.
- **HPE Security Fortify on Demand** is an application security testing and program management solution that delivers static and dynamic testing technologies of HPE Security Fortify with expert review and superior customer support. It enables customers to easily create, supplement, and expand a software security assurance program.

Table 3. Mapping of HPE Security Fortify solutions to regulatory standards

Mapping categories

Mapping	Versions supported	Description
Common Weakness Enumeration (CWE)	N/A	It provides a unified, measurable set of software weaknesses that is enabling more-effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.
FISMA	N/A	The 200 document is part of the official series of publications, issued by the NIST, relating to standards and guidelines adopted and promulgated under the provisions of the FISMA. Specifically, Federal Information Processing Standard (FIPS) Publication 200 specifies the minimum security requirements for federal information and information systems.
NIST SP 800-53 Rev. 4	N/A	It provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats.
Open Web Application Security Project (OWASP) Mobile Top 10	2014	This provides a powerful awareness document for mobile application security. The OWASP Mobile Top 10 represents a broad consensus about what the most critical mobile application security flaws are.
OWASP Top 10	2004, 2007, 2010, 2013	It provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.
PCI	1.1, 1.2, 2.0, 3.0, 3.1, 3.2	HPE Security Fortify tests for 31 application-security-related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is in place or not in place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.
SANS Top 25	2009, 2010, 2011	This provides an enumeration of the most widespread critical errors, categorized by CWE identifiers that lead to serious vulnerabilities in software. These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.
STIG	3.1, 3.4, 3.5, 3.6, 3.7, 3.9, 3.10, 4.1	Each requirement or recommendation identified by the DISA STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code (APP ID: CAT SEV). DISA STIG defines three severities with respect to vulnerabilities where their: • Exploitation leads to direct and immediate loss of confidentiality, availability, or integrity (CAT I) • Exploitation potentially results in loss of confidentiality, availability, or integrity (CAT II) • Existence degrades protections against loss of confidentiality, availability, or integrity (CAT III)
Web Application Security Consortium (WASC)	24 + 2, 2.00	The WASC was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a website. Version 2.00 of their Threat Classification outlines the attacks and weaknesses that can commonly lead to a website being compromised.

Summary

Compliance needs to be a priority in conjunction with security. Internal controls and sound business processes must be in place. In addition to regularly scrutinizing internal controls and assessing potential risks, leaders and decision makers should also consider the following:

- **Educate staff:** Whether through regular meetings, email updates, or more formal communications, keep everyone in the know about regulatory and compliance changes; provide regulatory compliance training, and make sure employees also have access to resources such as industry publications and webinars on relevant topics.
- **Invest in expertise:** This includes hiring compliance experts and internal auditors. Specialized consultants with deep expertise in regulatory matters can also help organizations to manage compliance initiatives more effectively.
- **Learn from others:** Keep an eye on competitors. Adopt their best practices and avoid repeating their blunders.

Non-compliance can damage an organization's reputation as much as its bottom line. Organizations should identify and manage risks, stay current with new legislation, hire compliance experts, and leverage the right solutions.

Organizations today are struggling to find the right balance between a growing compliance burden and an increasing demand for more strategic or operational security coverage. Remember that compliance requires proactive management and understanding of information and security demands a dynamic, intelligent, and preemptive approach. Use compliance as a foundation for security and as a baseline for security. Once companies have achieved compliance, they will then have the tools necessary to build a solid security foundation.

About HPE Security

Hewlett Packard Enterprise is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from **HPE Security ArcSight**, **HPE Security Fortify**, and **HPE Security — Data Security**, the HPE Security Intelligence Platform uniquely delivers the advanced correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.

About HPE Security Products Global Services

HPE Security Products Global Services take a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results, and demonstrate ROI. Our proven, use-case driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized people.

Learn more at
hpe.com/security

Sign up for updates

Hewlett Packard Enterprise

4AA6-8876ENW, December 2016