COMPASS
IT Compliance

Qualys.

Managing Compliance in Rapidly Changing Regulatory Environment

JERRY HUGHES, CISA, QSA, CRISC, MCPM
MANAGING PARTNER/SR EXECUTIVE IT AUDITOR
NOVEMBER 15TH, 2018

Secure. Comply. Save.

Agenda

COMPASS IT Compliance

- Introduction
- Objectives
- Threats
- Requirements
- Tools
- Summary
- Questions

Secure. Comply. Save.

Introduction

COMPASS IT Compliance

- Organizations face complex compliance challenges in today's business environment. These organizations are audited/assessed to various laws such as HIPAA, state privacy laws, GDPR, standards like PCI-DSS, and frameworks like ISO, NIST, and COBIT, to name a few.

Objective

COMPASS IT Compliance

- I will take you through the changing Threat, Legal, and Compliance landscape and how utilizing tools like the Qualys Cloud Platform to perform internal and external vulnerability assessments, and SSL Labs to test a browser's SSL implementation and a server's configuration, can help you meet these changing requirements.
- You will get valuable, actionable takeaways that they can be implemented in your organization to help you meet these requirements and mitigate their overall risk in the process.

Threats

COMPASS IT Compliance

- Many security organizations track these threats and trends like Krebs on Security, US-Cert, and SANS.org
- According to antivirus company Kaspersky Lab, “The number of new malicious files processed by Kaspersky Lab’s in-lab detection technologies reached 360,000 a day in 2017.” That’s 250 new malware threats every minute.
- There are many more cybersecurity threats and network vulnerabilities in existence that malicious actors can exploit to steal your company’s data or cause harm.
- Getting ahead of these threats is critical

Secure. Comply. Save.

Threats/Trends

COMPASS IT Compliance

1. Malware – Ransomware, Trojans, and Worms…
2. Unpatched Security Vulnerabilities - While there are countless new threats being developed daily, many of them rely on old security vulnerabilities to work
3. Social Engineering - Phishing, Pretexting, Baiting/Quid Pro Quo…
4. Your IoT – Internet of things includes smart devices such as Wi-Fi capable appliances, robots, etc. that many business don't even realize are on their network
5. Employees – The biggest security vulnerability in any organization is its own employees

Secure. Comply. Save.

Requirements

COMPASS IT Compliance

- Laws
- Regulations
- Frameworks
- Guidelines
- Best Practices

FFIEC

COMPASS IT Compliance

The Federal Financial Institutions Examination Council is a formal U.S. government interagency body composed of five banking regulators that is "empowered to prescribe uniform principles, standards, and report forms to promote uniformity in the supervision of financial institutions“

- Information Security Examination Handbook - II.C.4 Control Implementation
- Management should implement controls that align security with the nature of the institution’s operations and strategic direction. Based on the institution’s risk assessment, the controls should include, but may not be limited to, patch management, asset and configuration management, vulnerability scanning and penetration testing, end-point security, resilience controls, logging and monitoring, and secure software development (including third-party software development).

Secure. Comply. Save.

HIPAA -

COMPASS IT Compliance

Health Insurance Portability and Accountability Act of 1996

STANDARDS	CONTROL CATEGORY	CONTROL OBJECTIVES
Security Management Process	Security	164.308(a)(1)(ii)(A) Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the covered entity.

GDPR

COMPASS IT Compliance

The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area.

- The regulation applies if an organization collects or processes data from EU residents, or the data subject (person) is based in the EU. Under certain circumstances, the regulation also applies to organizations based outside the EU if they collect or process personal data of individuals located inside the EU.
- The regulation does not apply to the processing of data by a person for a "purely personal or household activity and thus with no connection to a professional or commercial activity."

Secure. Comply. Save.

GDPR

COMPASS IT Compliance

- **Responsibility and accountability**
- To be able to demonstrate compliance with the GDPR, the data controller must implement measures which meet the principles of data protection by design and by default. This includes ongoing Vulnerability Management.
- Data protection by design and by default (Article 25) require data protection measures to be designed into the development of business processes for products and services.
- It is the responsibility and the liability of the data controller to implement effective measures and be able to demonstrate the compliance of processing activities even if the processing is carried out by a data processor on behalf of the controller.

PCI DSS 3.2.1

COMPASS IT Compliance

- **Web Application Scanning**
- **6.6** For *public-facing* web applications, ensure that *either* one of the following methods is in place as follows: • Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows: - At least annually. - After any changes.

PCI DSS 3.2.1

COMPASS IT Compliance

- Section 11 – Internal & External Vulnerability Assessments
- **11.2.x** Run internal and external network vulnerability scans at least quarterly (performed by an Approved Scanning Vendor (ASV)) and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- **11.3.1** Perform ***external*** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).
- **11.3.2** Perform **internal** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

Secure. Comply. Save.

SANS Top 20

COMPASS IT Compliance

Center for Internet Security (CIS) and other organizations, developed the 20 Critical Security Controls (CSC) for Effective Cyber Defense

CSC 1: Inventory of Authorized and Unauthorized Devices
CSC 2: Inventory of Authorized and Unauthorized Software
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 5: Controlled Use of Administrative Privileges
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7: Email and Web Browser Protections
CSC 8: Malware Defenses
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 10: Data Recovery Capability
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12: Boundary Defense
CSC 13: Data Protection
CSC 14: Controlled Access Based on the Need to Know
CSC 15: Wireless Access Control
CSC 16: Account Monitoring and Control
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18: Application Software Security
CSC 19: Incident Response and Management
CSC 20: Penetration Tests and Red Team Exercises

Tools

COMPASS IT Compliance

- External Vulnerability Assessments: We leverage Qualys' portal (QualysGuard) for scanning external IPs. Essentially this is a cloud product. We define the assets that we want tested, but we actually don't have insight on what scanner is actually being used.
- Internal Vulnerability Assessments: we have a few options now. All varieties have the same capabilities (personal/vm are cheaper than the traditional U1 box)
- * Internal Hardware scanner. This is a U1 hardware device that can be installed on your stack that connects to Qualys online.
- * Internal personal edition: this is a lightweight hardware device roughly 5 in. x 5 in. in size.
- * VM - a Qualys virtual machine that can be installed on virtual box/ hypervisor/VMWare

Secure. Comply. Save.

Tools (cont.)

COMPASS IT Compliance

- This scanner (both internal/external) is used for discovery of vulnerabilities in both regular vulnerability assessments and also penetration testing. These scanners create the blueprint for our analyst to start their testing on.
- Qualys also has the capability to run web application scanning and we leverage this along with other types of products to perform this task.
- Qualys leverages selenium scripting technology to easily login into web applications and allow the scanner to spider each page for threats.

Qualys – SSL Labs

COMPASS IT Compliance

- This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet.
- **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Secure. Comply. Save.

Qualys. SSL Labs

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > www.[redacted]

SSL Report: www.[redacted]

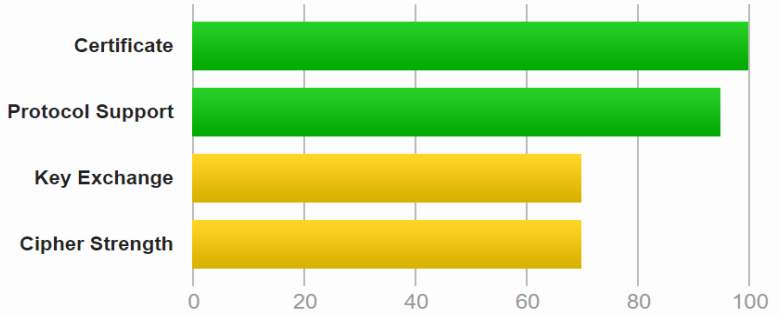
Assessed on: Wed, 31 Oct 2018 02:31:00 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B



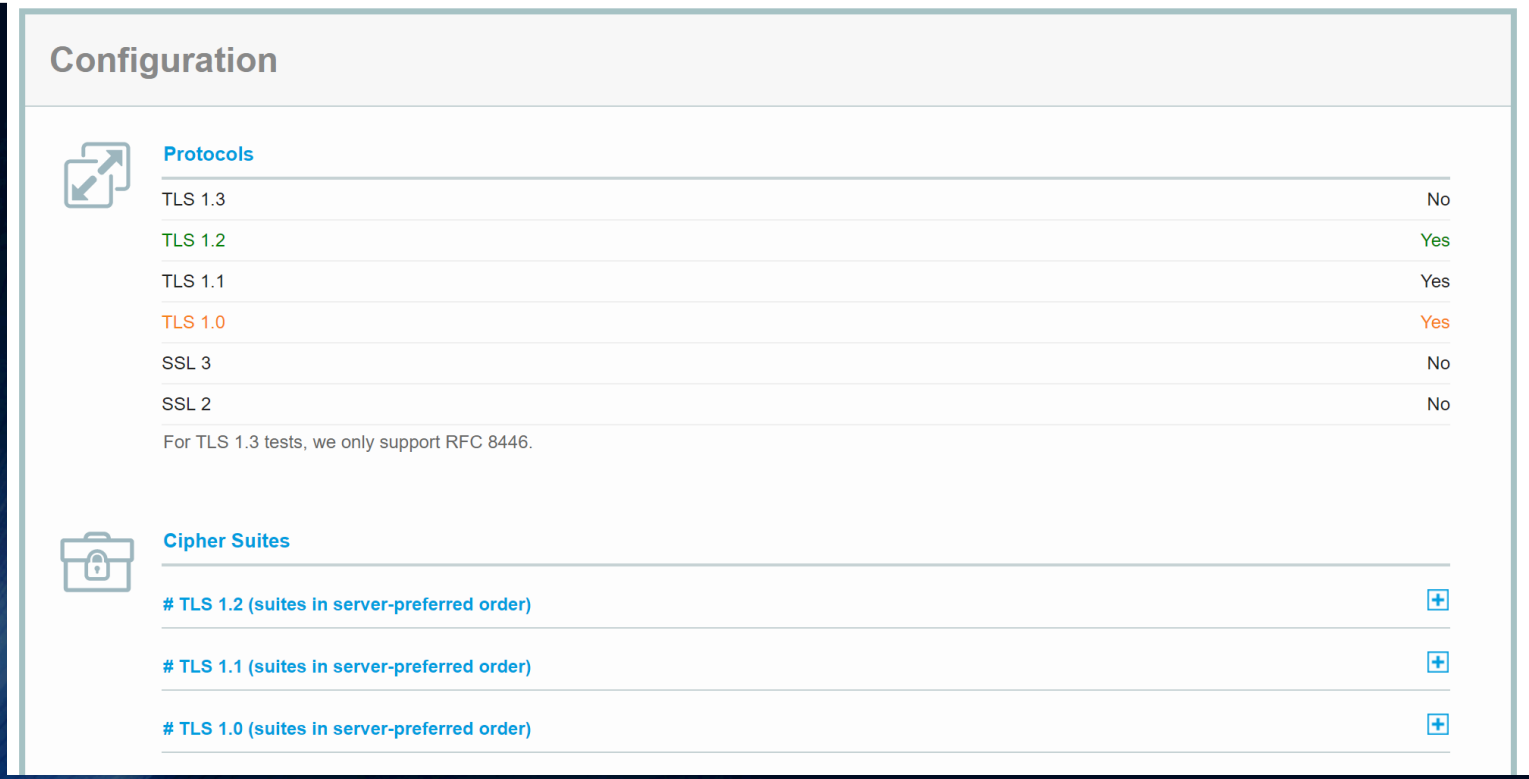
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

This server does not support Authenticated encryption (AEAD) cipher suites. Grade capped to B. MORE INFO »

Qualys – SSL Labs (cont.)

COMPASS IT Compliance



Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we only support RFC 8446.

Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS 1.1 (suites in server-preferred order)

TLS 1.0 (suites in server-preferred order)

Secure. Comply. Save.

Summary

COMPASS IT Compliance

- There is an everchanging threat landscape
- Businesses are not static
- Threats are exploited & in response laws come out to protect consumers
- Staff Education
- Run quarterly internal and external vulnerability assessments
- Perform Annual External Penetration Tests (and after critical changes)
- Perform Semi-Annual Internal Penetration Tests (and after critical changes)
- Ongoing Vulnerability Management
- Don’t just be compliant - be secure

Secure. Comply. Save.

Thank You

COMPASS IT Compliance