

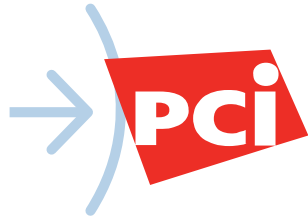


A blue-tinted overhead photograph of a meeting table. Several people are seated around the table, looking at documents and a laptop. The table is cluttered with papers, a laptop, a coffee cup, and other office supplies. The overall atmosphere is professional and collaborative.

Compliance and Security Impacts and Answers

PCI DSS 4.0, GDPR, U.S. State Civil Codes

Compliance Changes, Concerns, and Answers



In the wake of the pandemic, firms of all sizes have been hit with a new wave of changes and concerns. For many firms, remote and hybrid work is here to stay with some industries and regions experiencing a 10X increase from pre-pandemic levels. The advantages are lower employee and facility costs, but the disadvantages include expanded cybersecurity attack surfaces and increased breach risks.

Exacerbating work-from-home security risks, threat actors have increased the sophistication and frequency of most attacks and are now more often targeting firms across a variety of industries. To reduce these risks, governing bodies and regulators have turned up the dial on compliance mandates and requirements.

Payment Card Industry Security Standards for PCI-DSS 4.0 include significant new requirements for that increase the possibility of failures and fines. GDPR mishaps

are escalating given the difficulty of avoiding Availability Breaches wherein attackers have access to sensitive data. U.S. firms that do business with EU citizens must also comply. Lawsuits and brand damage stemming from the inability to meet stringent U.S. State Civil Codes, such as the California Consumer Privacy Act (CCPA), are becoming commonplace with the expansion of remote, hybrid, and satellite office work.

This eBook offers insights into these new challenges, as well as answers and best practice recommendations to avoid policy compliance misconfigurations and mistakes that can lead to tens of millions in costs for security breach remediation, lawsuits, fines, and brand damage.



Civil Codes

PCI-DSS 4.0 Challenges



On March 31, 2022, the Payment Card Industry Security Standards Council published version 4.0 of its PCI Data Security Standard (PCI-DSS). The updated standards provide significant new guidance on the scope and applicability for requirements for businesses, including:

- ✓ PCI-DSS 4.0 now applies to any systems that could impact account data security, so any compliance solution agents must run on all your systems and operating systems.
- ✓ Allows for multiple "on-demand" assessments upon request, so you could be audited at any time and must be fully prepared... quickly.
- ✓ A new track, called a Customized Approach, requires valid documentation to prove controls, such as comprehensive reports against those controls .



Applies to any systems that could impact account data security



Work from home increases breach risks by expanding attack surface



Allows for multiple "on-demand" assessments upon request

Consequences



The Consequences for PCI-DSS non-compliance can be severe

The average cost for audit failures has climbed to more than \$15 million in recent years, and specifically for PCI-DSS, fines of up to \$100K per month can be levied until issues are resolved. Exposure of Personally Identifiable Information (PII) can lead to multiple lawsuits with average costs per firm now exceeding \$4 million. Completing eDiscovery, to uncover all records for all individuals who may be affected, can also take many long months and cost millions. Finally, non-compliance can lead to security breaches and brand damage, and remediation costs to clean up the mess can exceed \$4 million. Obviously, avoidance is the best policy to mitigate damages and costs.



Fines of up to \$100,000 per month for non-compliance



Security breaches & brand reputation losses average \$4M+



Lawsuits averaging \$4M+ for violating PCI compliance guidelines



Qualys Answers



The Qualys Compliance Solution Set covers widest range of systems & OSs



Qualys Compliance ensures fast, accurate reporting for on-demand assessments



Qualys Compliance validates controls & remediates misconfigurations

How to avoid compliance failures...

The good news is that the Qualys Compliance Solution Set covers the widest range of operating systems, so you can meet the new guidelines, Qualys PC also ensures fast and accurate reporting so you can be ready quickly for on-demand assessments. Finally, you can ensure PCI-DSS compliance and mitigate risks as Qualys PC validates controls and remediates misconfigurations and

mistakes.

Qualys Compliance goes beyond vulnerability management to help enterprises simplify, expand, and automate the labor-intensive process of assessing security configurations, settings, and controls with a single cloud solution, multiple sensors, robust policy library, and seamless integration.

“To comply with **PCI DSS requirements**, we must show that there are no critical vulnerabilities in our core payment services. Qualys PCI helps us do that by monitoring payment services around the clock, enabling us to identify and **eliminate security issues** as soon as they arise.”



– Aleksejs Kudrjasovs, Head of Information Security



“ Qualys Policy Compliance simplifies the process of checking configuration settings on our servers, data bases and workstations, helping us make sure that all systems are properly configured.”

- Aleksejs Kudrjasovs, Head of Information Security

Industry	Financial Services
Business	Headquartered in Riga, Latvia, ABLV Bank offers private banking, investment, and financial planning services.
Scope	Regional across several locations and 850+ employees.
Business challenge	To protect critical systems and customer data while complying with regulations. ABLV must precisely target and mitigate the impact of vulnerabilities and potential threats to its infrastructure and ensure policy compliance.

Why ABLV Chose Qualys

- ✔ Helps keep critical systems and sensitive client data protected at all times.
- ✔ Supports compliance with regulations including GDPR and PCI DSS.
- ✔ Reduces workload for IT security team with automated vulnerability and configuration scanning.

GDPR Challenges



For European Union (EU) businesses that need to comply with the General Data Protection Regulation (GDPR), and U.S. firms that do business with EU citizens, there is now greater pressure to avoid an Availability Breach. This is essentially defined as a cyberattacker having unauthorized access to sensitive data, even if a full breach did not occur. Most organizations must:

- ✓ Report all security measures in place to address data breaches.
- ✓ Prove they can ensure full compliance with all GDPR requirements.
- ✓ Validate that proper GDPR controls are in place and implemented properly.

Auditors will scrutinize a firm's adherence to Availability Breach mandates to prevent access to personally identifiable information (PII) that can lead to data theft or other serious outcomes for EU citizens.



Applies to U.S. firms that do business with EU citizens and expose sensitive data



Must report Availability Breach for unauthorized access to sensitive data



To prevent data breaches, security controls must be implemented

Consequences



The Negative Impacts for GDPR Violations Can be Extreme

The impact of GDPR violations can be severe, including fines up to \$25M or 4% of turnover, or revenue. For example, British Airways paid \$26 million when several of their systems were compromised. The security breach affected 400,000 customers as cybercriminals obtained passenger names, addresses, log-in details, and credit card information. Litigation and legal discovery costs stemming from these types of breaches and data exposure can add up to more than \$4M, while also damaging an organization's reputation.



Fines of up to \$25M or 4% of revenue for non-compliance



\$4M+ in eDiscovery & litigation costs for violating guidelines



\$4M+ in brand damage and breach remediation costs



Qualys Answers



Comprehensive performance reports against GDPR requirements



Track and validate non-access to files and databases



GDPR library of controls, fast policy creation and remediation of issues

The Qualys Compliance Solution Set offers fast deployment and simplified management with seamless integration for GRC and other SIEM/ticketing systems. This ensures accelerated compliance audits and assessments for GDPR, as well as FedRAMP, PCI, SOX, HIPAA, FINRA, NYDFS, CCPA, and many other regulations.

Qualys Compliance allows you to track and validate non-access to files and databases to comply with GDPR's Availability Access requirements. Take advantage of a robust library of out-of-the-box GDPR controls to simplify and speed up policy creation and remediate any issues before they can cause violations or security breaches.

“ Qualys is a completely independent, automated platform. I can schedule regular scans on our internal and external networks. Not only is it very accurate, but it doesn't disrupt our network operations. We've never had any performance issues from running Qualys.”

- Fabio De Maron, Sr Manager Information Security



“ Whether it’s new vulnerability data, or enhancements to their software, the system is updated continuously by Qualys. I’m just as impressed by the technology as I am in how much easier it’s made our job of managing security.”

- Fabio De Maron, Sr Manager Information Security

Industry	Consulting / Services
Business	Arval, a BNP Paribas subsidiary, provides vehicle fleet financing and long-term contract hire.
Scope	Eight sales subsidiaries across Italy, with 750 employees and 110,000 managed vehicles, required security policy compliance solutions.
Business challenge	Migrate vulnerability analyst from manual processes to automated and seamless capabilities to reduce security breach risks and avoid regulatory failures.

Why ARVAL Chose Qualys

- ✓ Comprehensive reports that intelligently inform management, operations, and internal auditors.
- ✓ Qualys’ international reach, and the availability and competence of technical support teams.
- ✓ Ease of deployment, implementation, and automated management capabilities.



State Civil Code Challenges

For almost any business, but especially those operating in multiple U.S. States, Civil Codes have become far more onerous in recent years. Stiff requirements and penalties have been levied by the New York Department of Financial Services (NYDFS) and for California Consumer Privacy Act (CCPA) violations. In 48 of the 50 U.S. States, any business, large or small, must protect Personally Identifiable Information (PII) from exposure.

This requirement extends to remote and satellite offices and may cover remote workers if they have access to PII, such as customer or employee data. There are costly civil remedies available to individuals for violations that could negatively impact large firms and devastate small ones.



Applies to any business with PII in any of the 48 U.S. States with Codes



May be applicable for remote offices or workers if they have access to PII



Costly civil remedies available to individuals injured by any violations

Consequences



Violations Can Lead to Expensive Litigation

U.S. State Civil Code violations can be expensive. These can include fines levied by each State, as well as requirements to disclose security breaches or exposure of PII for more than a few hundred individuals. Most States allow Attorneys General to litigate and may also have a Private Cause of Action. If so, this allows private attorneys to file lawsuits on behalf of all parties who had PII exposed. These claims can easily cost millions in eDiscovery and court time, even if a firm wins. Moreover, brand damage and lost revenue resulting from the disclosure can also cost an organization millions.



Civil Codes



Can be fined by each State, must publicly disclose breaches



May be applicable for remote offices or workers if they have access to PII



Private Cause of Action lawsuits averaging \$4M+ in many States



Civil Codes

Qualys Answers



Qualys Compliance validates there are no critical vulnerabilities



Internal policy compliance reduces attack surfaces, helps prevent breaches



Robust library of compliance controls; monitoring & fast remediation

The Qualys Compliance Solutions Set helps you avoid the impact of U.S. State Civil Code violations. Qualys PC validates that there are no critical vulnerabilities that can lead to violations or security breaches. By complying with internal and external policies, attack surfaces are reduced to help prevent breaches. For businesses with limited recourses and time, a robust library of PCI controls are available, as well as complete monitoring and fast remediation of any issues.

Qualys Compliance enables you to have consolidated data gathered by Qualys sensors across all your network segments, as well as simplified management and robust reporting from a single-pane-of-glass dashboard.

“ We’ve found Qualys to be very simple, which we appreciate. Everything can be managed through the Web, whether from the office, my smartphone, or even my home PC. Wherever I am, I can log in and access and manage my reports and set up assessments. From the start of our evaluation, Qualys was the forerunner of the SaaS model.”



–COO, Blueport Commerce



“ At Blueport Commerce, we always seek the highest quality technology partners, selecting only the best companies in their respective areas of expertise. For vulnerability management, the search was not long: it always came down to Qualys.”

- Morgan Woodruff, Chief Operating Officer at Blueport Commerce

Industry	Technology
Business	Blueport Commerce provides trusted, managed e-commerce technology and services to retail chains and organizations with unique e-commerce needs including big ticket, customizable or difficult to ship products and complex business structures.
Scope	Services retail chains representing 2,000+ stores that represent \$8+ billion in sales.
Business challenge	Blueport Commerce must remain compliant with PCI DSS, and its customers need assurance that its systems operate to the highest security and compliance standards.

Why Blueport Chose Qualys

- ✓ Highly accurate and comprehensive reporting.
- ✓ Qualys provides control of the entire vulnerability management life cycle: asset discovery, vulnerability assessments, and tracking of security fixes.
- ✓ Qualys' SaaS delivery model reduces management overhead and provided the automation Blueport Commerce's IT team needed.

Recent Compliance Priorities for Businesses



✓ Validate that your policy compliance covers a wide range of systems and OSs

✓ Ensure you have fast, accurate reporting for on-demand assessments by auditors

✓ Deploy the ability to validate controls and remediate misconfigurations or mistakes



✓ Create the ability to track and validate non-access to files and databases

✓ Invest in solutions that provide comprehensive performance reports against GDPR requirements

✓ Leverage an extensive GDPR library of controls for fast policy creation and remediation for any issues



✓ Ensure your policy compliance solutions can validate that there are no critical vulnerabilities

✓ Establish internal policy compliance adherence to reduce attack surfaces and prevent security breaches

✓ Maintain a robust library of compliance controls, continuous monitoring, and fast remediation capabilities



Compliance Solutions Set

Qualys customers have avoided serious consequences by adding Qualys Policy Compliance to their security stacks, often alongside vulnerability management.

Qualys Compliance enables them to have consolidated data gathered by Qualys sensors across all their network segments, as well as simplified management and robust reporting from a single-pane-of-glass dashboard.

Qualys Compliance goes beyond vulnerability management to improve your ability to avoid security breaches and audit failures.

- ✓ **Quickly deploy and simplify management** with seamless integration for GRC, SIEM, and ticketing systems
- ✓ **Reduce Attack Surfaces** with improved compliance for internal policies and external mandates to avoid security breaches, brand damage, and audit failures
- ✓ **Accelerate compliance audits and assessments** for PCI DSS 4.0, SOX, HIPAA 2023, FINRA, GDPR, PCI, NYDFS, CCPA, and many other regulations
- ✓ **Simplified management and visibility** with single-pane-of-glass compliance tracking to security standards, regulations, and frameworks.
- ✓ **Active monitoring and remediation** for failed compliance controls to ensure audit readiness and improve reporting.



Compliance Apps



COMPLIANCE

Policy Compliance (PC)

File Integrity
Monitoring (FIM)

Security Assessment
Questionnaire (SAQ)

PCI-ASV (PCI)

FEATURES



Compliance data available via ad hoc search queries, customized dashboards, and reports



Out-of-band configuration assessment capabilities for inaccessible assets with Qualys FIM



Audit ready for 900 pre-configured policies, 20,000 compliance controls, 350 advanced technologies, and 100 regulatory frameworks



PCI-ASV scans all Internet-facing networks and systems with Six Sigma (99.9996%) accuracy



Alert noise reduction by up to 98%, monitoring critical files, directories, and registry paths for changes with Qualys FIM



(SAQ) creates campaign questionnaires with due dates, notifications, assigned reviewers, various answer formats, question criticality, answer scores, evidence requirements, and varying workflows

Asset Management Apps



Cybersecurity Asset
Management (CSAM)

External Attack Surface
Management (included)

Cyber Asset Attack Surface
Management (included)

Web Application Scanning
(WAS)

FEATURES

- ✓ Identify vulnerabilities in externally facing systems, and applications
- ✓ Support for automatic compliance implementation
- ✓ Inventory applications/software with expired and expiring instances (EOL/EOS management)
- ✓ Support for automatic compliance implementation
- ✓ Alive IPs, Shadow IT, forgotten applications and other applications no longer needed by the organization
- ✓ External attack surface data informed by Shodan data
- ✓ What/When/Who data (Discovery Path, DNS records, WhoIS registrars and hosting providers)
- ✓ Misconfigured ports, unintended databases/buckets, or storage devices
- ✓ Manage and build asset inventories required by security standards, including CISA, PCI DSS, FedRAMP, NIST, and SOC 2
- ✓ Tag and assign criticality scores to assets and asset groups according to industry, compliance, or operational need with TruRisk™

Remediation Apps




REMEDICATION

Patch Management (PM)

Custom Assessment and Remediation (CAR)

FEATURES

- ✓ Unified view across VM and IT infrastructure, supporting all IT patch workflows with RBAC for 'separation' where needed
- ✓ Automatically patch based on your TruRisk or Vulnerability Type (aka. Ransomware, CISA etc.)
- ✓ Zero Touch Patching – automatically patch the right assets at the right time based on risk
- ✓ Prioritize what to patch based on real risk reduction
- ✓ Out-of-the-box support for patching Windows OS, Linux and 3rd Party applications
- ✓ Configure rules and workflows so patches are deployed when they meet certain criteria, like severity level, CVSS score or product name
- ✓ Test script on test assets before executing it on production assets
- ✓ Export, edit, clone, download, and deprecate scripts with clear script status visibility throughout the processes
- ✓ Custom script and add information in the required fields, select required assets, and assign tags



Learn more about how Qualys is helping organizations like yours to stay ahead and maintain compliance with the latest security and regulatory challenges.

<https://www.qualys.com/solutions/compliance>

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based Security, Compliance, and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. Qualys, Qualys VMDR® and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

For more information, please visit [qualys.com](https://www.qualys.com)