



Qualys Policy Audit

常に準備を整え、コンプライアンスを遵守しましょう。

監査の自動化、リスクインサイト、ビジネスアライメント によるコンプライアンスの革新

今日の進化する脅威の状況では、サイバーセキュリティ ポリシーのコンプライアンスは、規制上のチェック項目としての役割を超えています。

先進的な企業は、**Qualys Policy Audit (PA)** が包括的なリスク管理に不可欠であり、競争優位性の推進力となることを認識しています。データプライバシーを確保し、ブランドの評判を守ることで、コンプライアンスは戦略的な必須事項となっています。

コンプライアンスをビジネスの推進力として活用するには、企業は従来の手作業によるツールから脱却する必要があります。最新のソリューションは、コンプライアンスリスクを定量化し、労働集約的な監査プロセスを自動化し、監査への準備を確実に整える必要があります。Qualys Enterprise TruRisk プラットフォームの中核コンポーネントである**Qualys PA**は、コンプライアンスを競争優位性へと転換するために必要な自動化、インサイト、そして効率性を提供します。

規制基準は、ポイントインタイム監査から継続的な成果ベースのコンプライアンスへと移行しています。この進化により、現代のセキュリティと規制の期待に応えるために、自動化の強化とリスクの優先順位付けへの新たな重点化が求められています。

コンプライアンスの維持は、ITチームとセキュリティチームにとって大きなコスト負担となります。ある推計によると、監査準備には規制要件ごとに年

間**10,000時間**以上かかり、企業のIT予算の約**40%**を占めると言われています。

証拠収集とコントロールマッピングを自動化することで、組織は手作業を最大**90%**削減し、監査準備コストを大幅に削減し、監査への継続的な対応力を維持できます。煩雑な作業に費やす時間が減ること
で、ITチームはセキュリティとコンプライアンス全体を強化する、より価値の高い取り組みの推進に注力できるようになります。

進化するコンプライアンス要件に対応するには、企業は従来のチェックボックス方式を超えたソリューションを必要としています。**Qualys PA**がコンプライアンスを変革する方法をご紹介します。

エンドツーエンドの監査自動化

証拠収集を自動化し、発見事項をコンプライアンス要件に整合させ、ギャップ分析を実行することで、コンプライアンスプロセスを革新します。**100**を超える幅広い要件と**450**を超えるテクノロジーをサポートする**Qualys PA**は、コンプライアンスの運用効率を最初から最後まで向上させます。

TruRisk™による監査とコンプライアンス指摘事項の優先順位付け

チェックリストの枠を超え、リスク情報に基づいたコンプライアンスを実現しましょう。**Qualys PA**は、セキュリティと監査への真のインパクトに基づいてコンプライアンス指摘事項の優先順位付けを行

い、最も重要なリスクを優先的に判断できるよう支援します。これらはすべて、Enterprise TruRisk™の視点から行われます。

監査レポートを簡単に作成

自信を持って監査に備えましょう。Qualys PAは、1つのデータ収集を複数のコンプライアンスレポートに自動的に変換するため、手作業の負担が軽減され、あらゆる監査人の精査に対応できるドキュメントが確実に作成されます。

Audit Fixによるコンプライアンス問題の迅速な解決

Audit Fix機能アドオンによる自動修復により、コ

ンプライアンス違反への対応にかかる時間と労力を削減します。手動介入を排除することで、迅速にギャップを埋め、全体的なリスクを軽減し、組織のセキュリティ体制を強化し、常に監査に対応できる状態を維持できます。

監査業務を効率化

セキュリティチームとIT部門間のギャップを埋めます。ITSM統合ワークフローにより、適切な情報が適切な関係者に適切なタイミングで確実に届き、コラボレーションの向上、対応時間の短縮、監査体制の強化を実現します。

規制への期待が高まり、デジタル環境が複雑化するにつれ、コンプライアンスは単なるチェックリストの枠にとどまらず、ビジネスに不可欠な信頼、レジリエンス、市場アジリティを戦略的に実現する手段となる必要があります。Qualys Policy Auditは、組織がコンプライアンスの複雑さを軽減し、コストを最小限に抑え、コンプライアンスを大規模に運用できるよう支援します。

継続的かつ成果重視のコンプライアンスへの移行に伴い、コンプライアンス維持にはこれまで以上に多くの時間、労力、そして投資が必要となります。コンプライアンスプロセスを自動化することで、企業はコンプライアンスコストを1件あたり最大30%削減し、手作業による労力を90%削減し、イノベーションや戦略的イニシアチブのためのリソースを確保できます。

調査によると、エンドツーエンドのコンプライアンス自動化により、監査時間が平均 75% 短縮され、監査関連のエラーが 95% 削減され、監査と環境全体で一貫性と信頼性の高いコンプライアンス結果が保証されます。

Qualys Policy Auditのような自動化機能を活用することで、企業はリスクの優先順位付け、業務の効率化、そして常に監査への準備態勢を維持できます。Qualys Policy Auditは、コンプライアンスを戦略的推進要因として捉え直すことで、規制要件を測定可能な管理策へと転換し、監査業務の負担を軽減し、テクノロジースタック全体にアカウンタビリティを組み込むことを可能にします。

その結果、コンプライアンス コストが削減され、世界および地域のポリシー変更への対応が迅速化され、リスクポスチャーとビジネス パフォーマンスの整合性が強化されます。

主要指標：

<div>90%</div> <div>手作業による コンプライアンス作業を短縮</div>	<div>30%</div> <div>義務ごとの コンプライアンスコストを削減</div>
<div>75%</div> <div>監査準備時間を削減</div>	<div>95%</div> <div>監査関連の不備を削減</div>

Qualys Policy Auditを試してみる準備はできましたか？

今すぐ試す

Qualys Policy Auditは、レポート生成において以下の義務をサポートしています。義務は地域またはセクター別に分類されており、簡単に参照できます。

Australia

- The Australian Signals Directorate
- The Essential 8 Strategies (ASD 8)
- Australian Signals Directorate Information Security Manual (ISM)
- Australian Signals Directorate - Essential Eight Maturity Model
- APRA Prudential Practice Guide (PPG):
CPG 234 - Management of Security Risk in Information and Information Technology

Brazil

- Brazilian General Data Protection Law (LGPD)

Canada

- Personal Information Protection and Electronic Documents Act
- Annex 3A (Security Control Catalogue) to IT Security Risk Management: A Lifecycle Approach (ITSG- 33)

European Union

- The Network and Information Systems (NIS 2 Directive) (EU) 2022/2555
- The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554
- General Data Protection Regulation (GDPR)
- European Union Agency for Network and Information Security

France

- ANSSI 40 Essential Measures for a Healthy Network

North America

- NERC Critical Infrastructure Protection (CIP)

Qatar

- Qatar 2022 Cybersecurity Framework National Information Assurance Policy

Saudi Arabia

- Saudi Aramco SACS-002 Third Party Cybersecurity Standard
- Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework (CSF)
- Essential Cybersecurity Controls

Singapore

- Technology Risk Management (TRM) Guidelines
- Monetary Authority of Singapore (MAS)
- Notice 834: Cyber Hygiene Practices

South Africa

- Protection of Personal Information Act (POPI Act)

Spain

- Royal Decree 311/2022 - Annex II (MEDIUM)
- Royal Decree 311/2022 - Annex II (HIGH)
- Royal Decree 311/2022 - Annex II (BASIC)
- Royal Decree 311/2022

United Arab Emirates (UAE)

- NESA UAE Information Assurance Standards (IAS)

United Kingdom

- NCSC Basic Cyber Security Controls (BCSC)
- US Gramm Leach Bliley Act (GLBA)
- US Food & Drug Administration (FDA)

United States

- Criminal Justice Information Services (CJIS) Security Policy
- Control Objectives for Information and Related Technologies (COBIT)
- CERT Resilience Management Model
- California Consumer Privacy Act of 2018 (SB-1121)
- 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

- NIST 800-53 (Special Publication)
- New York State Department of Financial Services 23 NYCRR 500
- Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- Microsoft Cloud Security Benchmark
- IRS Publication 1075
- Health Insurance Portability and Accountability (HIPAA) Security Rule 45 CFR Parts 160/164, Subparts A/C:1996
- Federal Risk and Authorization Management Program (FedRAMP M) - Moderate Security Baseline
- Federal Risk and Authorization Management Program (FedRAMP H) - High Security Baseline
- Federal Financial Institutions Examination Council (FFIEC)
- Federal Acquisition Regulation (FAR)
- Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7008-7012
- Cybersecurity Maturity Model Certification (MM) Level 5
- Cybersecurity Maturity Model Certification (MM) Level 4
- Cybersecurity Maturity Model Certification (MM) Level 3
- Cybersecurity Maturity Model Certification (MM) Level 2
- Cybersecurity Maturity Model Certification (MM) Level 1
- Cybersecurity Maturity Model Certification (CMMC)
- US Cybersecurity Maturity Model Certification (MM) 2.0 Level 2
- US Cybersecurity Maturity Model Certification (MM) 2.0 Level 1
- The NIST Cybersecurity Framework (CSF)
- Sarbanes-Oxley Act: IT Security
- NIST Special Publication 800-171
- NIST Cyber Security Framework (CSF)
- NIST AI 100-1 - Artificial Intelligence Risk Management Framework, January 2023
- CSA 405(d) - Technical Volume 2: Cybersecurity

Practices for Medium and Large Healthcare Organizations

- CSA 405(d) - Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations

Global

- SWIFT Customer Security Controls Framework - Customer Security Programme v2024
- SWIFT Customer Security Controls Framework - Customer Security Programme v2023
- SWIFT Customer Security Controls Framework - Customer Security Programme v2021
- SWIFT Customer Security Controls Framework - Customer Security Programme v2019
- Secure Controls Framework (SCF)
- Payment Card Industry Data Security Standard (PCI-DSS) v4.0
- Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1
- ISO/IEC 27001:2022
- ISO/IEC 27001:2013
- Critical Systems Cybersecurity Controls
- Cloud Controls Matrix (CCM)
- CIS Controls Version 8.1
- CIS Controls Version 8
- CIS Controls

India

- Reserve Bank of India (RBI) - Baseline Cyber Security and Resilience Requirements (Annex 1)
- IRDAI Guidelines On Information and Cyber Security for Insurers

Malaysia

- Risk Management in Technology (RMiT)

New Zealand

- New Zealand Information Security Manual (NZISM)

Qualys Policy Audit は、Windows、Unix、Mac、データベース、ネットワークデバイスなどの主要なプラットフォームを含む450以上のテクノロジーをサポートしています。また、標準的なCISベンチマークの対象外となる、幅広い特殊技術やエキゾチックなテクノロジーもカバーしており、多様なIT環境における包括的なセキュリティとコンプライアンスを確保します。

Qualys Policy Auditでサポートされているテクノロジーの一部：

Applications

- VMware Horizon
- Microsoft .NET Framework
- Microsoft Exchange Server
- Skype for Business Server
- SharePoint Server
- Ivanti Connect Secure
- IBM Datapower Gateway
- A10 Advanced Core OS
- AudioCodes Session Border Controller
- Aruba EdgeConnect OS
- Citrix NetScaler
- Riverbed SteelHead RiOS
- CentOS Stream
- VMware Photon OS
- Bottlerocket OS
- IBM VIOS
- IBM i 7.x
- Azure Stack HCI
- Windows 2025 Server

Container Security

- Docker CE/EE
- Kubernetes
- Cisco SD-WAN
- Cisco UCS Manager
- Riverbed SteelHead Interceptor
- Gigamon GigaVUE-OS
- INFOBLOX NIOS

Databases

- Apache Cassandra
- Apache Hadoop
- IBM DB2 z/OS
- Redis
- SAP Adaptive Server Enterprise

Mainframes

- IBM z/OS Security Server RACF
- HP Safeguard

Network Devices

- Extreme Networks VOSS
- Cisco FTD
- Nokia SROS
- Brocade Fabric
- CBL-Mariner Linux
- Google Container -Optimized OS
- Red Hat Enterprise Linux CoreOS
- Checkpoint MDS
- Virtuozzo Linux
- Kali GNU/Linux
- Microsoft Azure Linux
- Alibaba Cloud Linux
- CloudLinux OS

Security Applications

- Windows 2019 Server Certification Authority

Operating Systems

Printers

- Xerox VersaLink
- HP Printers
- Samsung Printers

Storage

- Data Domain OS
- NetApp Data ONTAP

Virtualization

- Citrix
- XenApp/XenDesktop
- Citrix Hypervisor
- Red Hat OpenShift Container Platform

Web Services

- IBM WebSphere
- MQ Nginx
- VMware vFabric Web Server
- Oracle HTTP Server

Qualysについて

Qualys, Inc. (NASDAQ: QLYS) は、破壊的イノベーションをもたらすクラウドベースのセキュリティ、コンプライアンス、ITソリューションを提供する先駆的かつ業界をリードする企業であり、全世界で10,000社以上のサブスクリプション顧客を有しています。その中には、Forbes Global 100およびFortune 100の企業の大多数が含まれます。Qualysは、組織がセキュリティおよびコンプライアンス対策を単一のプラットフォーム上で効率化・自動化し、俊敏性の向上、ビジネス成果の最大化、そして大幅なコスト削減を実現する支援を行っています。Qualys、Qualys VMDR®、およびQualysのロゴは、Qualys, Inc.の登録商標です。その他すべての製品名および名称は、それぞれの企業の商標である可能性があります。詳細については、qualys.comをご覧ください。