ConductorOne

Understanding IT Compliance Audits: What to Expect, How to Prepare, and Best Practices

What is an IT compliance audit?

An IT compliance audit is a systematic and independent evaluation of an organization's IT infrastructure, policies, and procedures to ensure they align with relevant regulations, industry standards, and internal policies.

The main objectives of an IT audit for compliance are:

- → **Verify compliance:** Ensure the organization's IT practices adhere to specific laws, regulations, and standards like GDPR, HIPAA, PCI DSS, SOC 2, or ISO 27001.
- → **Identify vulnerabilities and risks:** Uncover any weaknesses or potential threats in the IT infrastructure that could lead to security breaches, data loss, or noncompliance.
- → **Recommend improvements:** Provide actionable recommendations to strengthen the organization's IT security posture and enhance compliance efforts.
- → **Demonstrate due diligence:** Show stakeholders, regulators, and customers that the organization is committed to protecting sensitive data and maintaining a secure IT environment.

Why do companies need to perform IT compliance audits?

IT compliance audits are not merely a checkbox exercise but a strategic investment in protecting your organization's future. They help you mitigate risks, avoid financial losses, and maintain a strong security posture while building trust with stakeholders and staying ahead of evolving regulatory requirements.

Here's why performing IT compliance audits is essential for businesses today:

Mitigate legal and financial risks

- → **Avoid hefty fines and penalties:** Noncompliance with regulations like SOX, GDPR, HIPAA, or PCI DSS can lead to severe financial penalties, potentially crippling your business. Audits ensure you're adhering to the rules, avoiding costly fines.
- → **Protect against legal action:** Data breaches and security lapses can lead to lawsuits and reputational damage. Audits identify vulnerabilities and help you prevent breaches, protecting you from legal repercussions.

Strengthen your security posture

- → **Uncover vulnerabilities:** Audits reveal weaknesses in your IT systems, processes, and policies that could be exploited by hackers.
- → **Improve incident response:** By assessing your incident response plans and capabilities, audits ensure you're prepared to handle security incidents swiftly and effectively, minimizing damage.

Enhance business processes and continuity

- → **Reduce downtime and disruptions:** IT outages and security breaches can disrupt operations and impact productivity. Audits identify potential risks that could lead to downtime, enabling you to take preventative measures.
- → **Safeguard critical data:** Data is the lifeblood of many organizations. Audits ensure your data is protected with robust backup and recovery mechanisms, preventing costly losses.

Build stakeholder trust

- → **Demonstrate due diligence:** Regular audits show clients, partners, and investors that you're serious about security compliance. This builds trust and confidence in your organization.
- → **Maintain a positive reputation:** Compliance failures can damage your brand and make it harder to attract customers and talent. Audits help you maintain a positive reputation as a trustworthy organization.

IT compliance regulatory frameworks you should know about

HIPAA (Health Insurance Portability and Accountability Act)

→ **Focus:** Protects the privacy and security of sensitive patient health information (PHI) in the United States.

→ **Key requirements:**

- Privacy rule: Establishes standards for the use and disclosure of PHI.
- Security rule: Sets national standards for protecting the confidentiality, integrity, and availability of electronic PHI (ePHI).
- Breach notification rule: Requires covered entities to notify individuals and the government in the event of a breach of unsecured PHI.

→ **Who it applies to:** Healthcare providers, health plans, healthcare clearinghouses, and business associates handling PHI.

PCI-DSS (Payment Card Industry Data Security Standard)

→ **Focus:** Protects cardholder data during and after payment transactions.

→ **Key requirements:**

- **Build and maintain a secure network:** Install and maintain firewalls and do not use vendor-supplied defaults for system passwords and other security parameters.
- **Protect cardholder data:** Protect stored cardholder data and encrypt transmission of cardholder data across open, public networks.
- **Maintain a vulnerability management program:** Use and regularly update antivirus software or programs.
- **Implement strong access control measures:** Restrict access to cardholder data by business need to know. Assign a unique ID to each person with computer access. Restrict physical access to cardholder data.
- **Regularly monitor and test networks:** Track and monitor all access to network resources and cardholder data. Regularly test security systems and processes.
- **Maintain an information security policy:** Maintain a policy that addresses information security for all personnel.

→ **Who it applies to:** Any organization that accepts, processes, stores, or transmits credit card information.

SOC 2 (System and Organization Controls 2)

→ **Focus:** Assesses the effectiveness of an organization's controls related to security, availability, processing integrity, confidentiality, and privacy.

→ **Key requirements:**

- Based on the AICPA Trust Services Criteria.
- Two types of reports:
  - **Type I:** Describes the service organization's system and the suitability of the design of controls at a specific point in time.
  - **Type II:** Covers a specified period (usually 6-12 months) and assesses both the design and operating effectiveness of the controls.

→ **Who it applies to:** Service organizations that store, process, or transmit customer data (e.g., cloud service providers, SaaS companies, data centers).

ISO (International Organization for Standardization)

→ **Focus:** Develops and publishes international standards across various industries, including IT.

→ **Key standards:**

- **ISO/IEC 27001:** Focuses on information security management systems (ISMS) and provides a framework for managing and protecting sensitive information.
- **ISO/IEC 27002:** Provides a code of practice for information security controls.
- **ISO 9001:** Focuses on quality management systems.

→ **Who it applies to:** Any organization seeking to implement best practices and demonstrate a commitment to quality and information security.

GDPR (General Data Protection Regulation)

→ **Focus:** Protects the personal data and privacy of individuals within the European Union (EU) and the European Economic Area (EEA).

→ **Key requirements:**

- **Lawful, fair, and transparent processing:** Personal data must be processed lawfully, fairly, and in a transparent manner.
- **Purpose limitation:** Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.
- **Data minimization:** Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** Personal data must be accurate and, where necessary, kept up to date.
- **Storage limitation:** Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Integrity and confidentiality:** Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

→ **Who it applies to:** Any organization that collects or processes the personal data of individuals in the EU and EEA, regardless of where the organization is located.

SOX (Sarbanes-Oxley Act)

→ **Focus:** Ensuring the accuracy and reliability of financial reporting for publicly traded companies, with implications for IT controls and processes that impact financial data.

→ **Key requirements:**

- Establishment of internal controls over financial reporting
- Independent audits of internal controls
- CEO and CFO certification of financial statements
- Increased criminal penalties for fraudulent financial activity

→ **Who it applies to:** Publicly traded companies in the United States

→ **Related Read:** SOX Audit: Who Needs It, When, and How to Prepare

NIST (National Institute of Standards and Technology)

→ **Focus:** Providing a framework for managing and improving cybersecurity risk for organizations of all sizes and sectors

→ **Key requirements:** (Specifically referring to the NIST Cybersecurity Framework (CSF))

- **Identify:** Develop an understanding of cybersecurity risks
- **Protect:** Implement safeguards to ensure the delivery of critical services
- **Detect:** Develop and implement activities to identify cybersecurity events
- **Respond:** Develop and implement activities to take action regarding a detected cybersecurity incident
- **Recover:** Develop and implement activities to maintain plans for resilience and restore capabilities or services impaired due to a cybersecurity incident.

→ **Who it applies to:** While voluntary, the NIST CSF is widely adopted across various industries and sectors, both public and private. For example, the US Department of Defense's CMMC requirements are partially based on the NIST CSF.

CCPA (California Consumer Privacy Act)

→ **Focus:** Protects the personal information and privacy rights of California residents by granting them control over how businesses collect, use, and share their data.

→ **Key Requirements:**

- **Right to know:** Consumers have the right to know what personal information businesses collect about them, how it's used, and with whom it's shared.
- **Right to delete:** Consumers can request that businesses delete their personal information (with some exceptions).
- **Right to opt-out of sale:** Consumers can prevent businesses from selling their personal information to third parties.
- **Right to non-discrimination:** Businesses cannot discriminate against consumers for exercising their CCPA rights.

→ **Who it applies to**: For-profit businesses that do business in California and meet at least one of the following criteria:

- Have annual gross revenues over $25 million.
- Buy, sell, or share the personal information of 50,000 or more consumers, households, or devices.
- Derive 50% or more of their annual revenue from selling consumers' personal information.

Compliance audit process: How are audits conducted?

1. Research and readiness

→ Auditors confirm the audit's scope and prepare checklists and schedules.

→ If they've audited you before, they review prior reports and documentation to understand changes.

2. Documentation and evidence review

→ Auditors review relevant policies and procedures, often using a checklist of evidence requests.

→ This step may continue throughout the audit or occur in rounds.

3. Conducting interviews

→ Auditors conduct interviews to understand processes and controls, asking questions about documentation and workflows.

→ Organizations should prepare interviewees and ensure the right people are present.

4. Process assessment and employee shadowing

→ Auditors assess the effectiveness of controls based on documentation, interviews, and testing.

→ Testing involves reviewing documents and observing processes in action (shadowing).

→ Organizations should document any deviations from policy and take corrective action if necessary.

5. Compilation of compliance report

→ Auditors prepare the final audit report, including findings and recommendations.

→ Senior team members review the report, and the business can provide feedback.

→ The final report may require sign-off from a certified individual or firm.

Things to keep in mind:

→ Open communication and collaboration between the organization and auditors are crucial throughout the process.

→ Organizations should be prepared to provide evidence and answer questions about their IT systems and processes.

→ Audit findings are an opportunity for improvement, not a failure.

→ The final report should accurately reflect the organization's compliance posture and efforts.

Compliance audit checklist: Best practices to follow

To successfully pass an IT compliance audit and maintain a strong security posture, organizations should implement and adhere to the following best practices:

Pre-audit

Understand the requirements

Thoroughly familiarize yourself with the specific compliance framework(s) applicable to your organization. This includes understanding the controls, objectives, and evidence required for demonstrating compliance.

Conduct a self-assessment (internal audit)

Perform an internal audit or risk assessment to identify any potential gaps or weaknesses in your IT controls and processes. This proactive approach allows you to address any issues before the external audit.

Organize documentation

Ensure that all relevant policies, procedures, and records are up-to-date, well-organized, and readily available for the auditors. This includes system configurations, access logs, incident reports, and other evidence of compliance.

Train employees

Educate employees on their roles and responsibilities in maintaining compliance. Promote a culture of security awareness training and ensure everyone understands the importance of following established policies and procedures.

Designate accountability

Assign a single point of contact or a dedicated compliance audit team to manage the audit process. Empower process owners to understand and fulfill their compliance responsibilities.

Leverage purpose-built technology

Consider using a comprehensive compliance management platform to streamline audit processes, facilitate collaboration, and centralize documentation. Utilize tools to enhance communication and evidence management.

Engage external auditors

If you lack internal resources or expertise, consider hiring a qualified third-party auditor to help you prepare for and manage the audit process.

During the audit

Facilitate access and communication

→ Provide auditors with the necessary access to systems, documentation, and personnel.

→ Maintain open and transparent communication with the auditors throughout the process.

→ Be responsive to their requests for information and evidence.

Demonstrate preparedness and cooperation

→ Show that you've taken the audit seriously and are prepared to address any findings.

→ Be organized and have all requested documentation readily available.

→ Assign knowledgeable personnel to assist the auditors and answer their questions.

Address findings proactively

→ If noncompliance or control gaps are identified, acknowledge them and demonstrate a commitment to remediation.

→ Develop a corrective action plan and provide evidence of its implementation to the auditors.

Post-audit

Implement corrective actions

→ Follow through on the corrective action plan and address any identified weaknesses promptly.

→ Assign responsibility and set deadlines for remediation efforts.

→ Document the actions taken and their effectiveness.

Continuous improvement

→ Treat the audit as a learning opportunity and use the findings to strengthen your overall security and compliance posture.

→ Regularly review and update policies, procedures, and controls to ensure they remain effective and aligned with evolving threats and regulatory requirements.

Maintain compliance

→ Conduct periodic self-assessments and follow-up audits to ensure ongoing compliance. To do this, you have to designate internal auditors who will take care of this.

→ Stay informed about regulatory changes and adjust your practices accordingly.

How ConductorOne enables IT compliance

ConductorOne can significantly aid IT compliance efforts by automating and streamlining various aspects of access management and security, which are critical components of most compliance frameworks.

Centralized access management

- **Unified access views:** ConductorOne provides a centralized platform to visualize and manage access across various applications, systems, and infrastructure, making it easier to identify potential risks and ensure least privilege access.
- **Automated access requests and approvals:** Streamline access request and approval workflows, ensuring that only authorized personnel have access to sensitive data and resources. This helps enforce segregation of duties and prevent unauthorized access, which are key requirements in many compliance frameworks.

Continuous Monitoring and Remediation

- **Real-time visibility:** Gain real-time visibility into user access and activity, enabling you to detect and respond to any suspicious behavior or potential security breaches quickly.
- **Automated remediation:** Implement automated remediation workflows to address access violations or noncompliant configurations automatically, ensuring that your IT environment remains secure and compliant.

Compliance Reporting

- **Generate audit-ready reports:** Automate user access reviews and generate comprehensive reports on user access, permissions, and activities, streamlining the evidence collection process for audits and demonstrating compliance with various frameworks.
- **Customizable reporting:** Customize reports to focus on specific compliance requirements or areas of concern, providing auditors with the information they need in a clear and concise format.

Least privilege access

- **Enforce least privilege:** Implement and enforce least privilege access policies to minimize the risk of unauthorized access and data breaches.
- **Right-sizing access:** Regularly review and adjust user access privileges to ensure they align with their current roles and responsibilities, reducing the attack surface.

Integration with existing infrastructure

→ ConductorOne integrates with your existing identity providers, cloud infrastructure, and other security tools, providing a comprehensive view of access across your IT environment.

→ Easily scale ConductorOne as your organization grows and your IT infrastructure evolves.

Overall, ConductorOne can help you:

→ Streamline access management and security processes.

→ Enhance visibility and user access reviews.

→ Automate compliance tasks and reporting.

→ Reduce the risk of unauthorized access and data breaches.

→ Demonstrate compliance with various regulatory frameworks.

Streamline IT compliance audits with ConductorOne

IT compliance audits are essential, but they don't have to be overwhelming.
By following the best practices outlined in this guide and leveraging the power of ConductorOne, you can proactively manage risk, simplify access controls, and ensure a successful audit outcome.

Don't let compliance be a burden. Embrace automation, streamline processes, and confidently demonstrate your organization's commitment to security.

Frequently asked questions about IT compliance audits

What's the difference between internal audit vs. external audit for IT compliance?

Internal Audit

An internal IT compliance audit is like a self-checkup performed by your own organization. It's conducted by employees within your company, often from the internal audit department. The main goal is to look inward and identify any weaknesses or vulnerabilities in your IT systems, policies, and procedures. This proactive approach allows you to address potential issues before they escalate into major problems, ensuring that your IT operations are efficient, secure, and aligned with industry best practices and internal policies.

Key things to keep in mind:

→ Conducted by internal employees

→ Focuses on identifying and addressing internal weaknesses

→ Proactive approach to risk management

→ Ensures alignment with internal policies and industry best practices

→ Improves internal processes and operational efficiency

External Audit

An external IT compliance audit, on the other hand, is like having an independent expert come in for a second opinion. It's performed by a third-party firm, completely separate from your organization.

Their primary objective is to provide assurance to external stakeholders — such as investors, regulators, or clients — that your IT systems and processes are secure and compliant with relevant regulations (like HIPAA or GDPR).

Key things to keep in mind:

→ Conducted by an independent third-party firm

→ Provides assurance to external stakeholders

→ Focuses on compliance with specific regulations

→ Verifies the accuracy of financial information related to IT

→ Enhances credibility and builds trust

What are the benefits of compliance audits?

→ **Risk mitigation**

- Identify vulnerabilities and weaknesses in IT systems and processes
- Proactively address security risks and prevent data breaches
- Minimize the impact of potential disruptions and downtime

→ **Compliance assurance**

- Verify adherence to relevant regulations and industry standards
- Avoid costly fines and penalties associated with non-compliance
- Demonstrate due diligence to stakeholders and regulators

→ **Operational efficiency**

- Evaluate the effectiveness of IT controls and processes
- Identify opportunities for improvement and optimization
- Enhance productivity and resource utilization

Talk to our team.

Or take a self-guided tour to learn more!

Try ConductorOne now

Get a demo