hyperproof

# IT Compliance Audit Checklist: A Practical Guide for Beginners

Below is a checklist to help you get started on an IT compliance audit. We've outlined the key steps you should take to get started to help expedite the process.

- [ ] **Meet with relevant internal stakeholders to set priorities and recommendations**
- [ ] **Review the NIST CSF as a starter framework to base your work on**
  - [ ] Identify your scope for systems, processes, and assets
  - [ ] Review NIST CSF categories and subcategories
    - [ ] Identify
      - [ ] Asset management
      - [ ] Business environment
      - [ ] Governance
      - [ ] Risk assessment
      - [ ] Risk management strategy
      - [ ] Supply chain risk management
    - [ ] Protect
      - [ ] Identity management
      - [ ] Awareness and training
      - [ ] Data security
      - [ ] Information protection processes
      - [ ] Maintenance
      - [ ] Protective technology
    - [ ] Detect
      - [ ] Anomalies and events
      - [ ] Continuous security monitoring
      - [ ] Detection processes
    - [ ] Respond
      - [ ] Response planning
      - [ ] Communication
      - [ ] Analysis
      - [ ] Mitigation
      - [ ] Improvements
    - [ ] Recover
      - [ ] Recovery planning
      - [ ] Improvements
      - [ ] Communications

NEXT PAGE

- [ ] Evaluate each control in your organization against each subcategory
- [ ] Select the tier your organization wants to be at for each function:
  - [ ] Tier 1: Partial
  - [ ] Tier 2: Risk informed
  - [ ] Tier 3: Repeatable
  - [ ] Tier 4: Adaptive

- [ ] **Identify gaps and improvement areas (examples follow)**
  - [ ] Access control gaps
    - [ ] Does your organization lack a consistent process for revoking access rights when employees leave?
  - [ ] Incident response plan gaps
    - [ ] Is your incident response plan outdated and not regularly tested?
  - [ ] Continuous monitoring improvement area
    - [ ] Do you have a continuous monitoring system in place to detect and respond to security threats in real-time?

  - [ ] Develop a plan of action
    - [ ] Outline specific steps to address identified gaps
    - [ ] Set timelines and milestones for each action item
    - [ ] Assign responsible parties to each task

  - [ ] Implement your plan
    - [ ] Update or create policies to align with NIST CSF best practices
    - [ ] Implement technical controls such as access management, encryption, and monitoring tools
    - [ ] Ensure proper documentation of changes

  - [ ] Regularly reassess and adjust as needed
    - [ ] An IT compliance tool like Hyperproof enables organizations to automate continuous monitoring. Continuous control monitoring allows organizations to see updates in real-time and keep their finger on the pulse of potential threats. This ultimately allows organizations to monitor IT compliance status more closely and adjust proactively.