BridgeView

Comprehensive IT Audit Checklist

Tech, Organization, People Enablement

This checklist is designed to help SVPs and VPs of Technology conduct a thorough audit of their IT operations using the People, Process, Technology (PPT) approach. Each section contains detailed items to assess, ensuring a comprehensive evaluation of your IT infrastructure and operations.

01 People Assessment

1.1 Skills and Competencies

- □ Conduct skills assessment for all IT staff
- □ Identify skill gaps in relation to current and future technology needs, including AI/ML, cybersecurity and cloud computing
- □ Evaluate technical certifications and their relevance to job roles
- □ Assess soft skills (communication, problem-solving, teamwork)

1.2 Roles and Responsibilities

- □ Review job descriptions for all IT positions
- □ Ensure clear definition of roles and responsibilities
- □ Check for overlaps or gaps in responsibilities
- □ Audit role-based access control (RBAC) as part of IT governance
- □ Assess the effectiveness of the current organizational structure

1.3 Collaboration and Communication

- □ Evaluate internal communication tools and their effectiveness
- □ Assess cross-functional collaboration within IT teams
- □ Evaluate virtual team collaboration practices, if you have a prevalence of remote work
- □ Review communication processes between IT and other departments
- □ Check for regular team meetings and their productivity

1.4 Training and Development

- □ Review existing training programs and their effectiveness
- □ Identify areas requiring additional training
- □ Assess the budget allocated for professional development
- □ Evaluate mentorship and knowledge transfer processes

1.5 Employee Engagement and Satisfaction

- □ Conduct anonymous employee satisfaction surveys
- □ Review turnover rates in IT departments
- □ Assess work-life balance and stress levels
- □ Evaluate career growth opportunities within the organization

02 Process Assessment

2.1 Efficiency and Effectiveness

- □ Map out key IT processes (e.g., incident management, change management)
- □ Measure process cycle times and identify bottlenecks
- □ Assess the use of automation in processes to reduce manual work and error-prone tasks, especially in incident management and monitoring
- □ Assess adherence to industry standards (e.g., ITIL, COBIT)
- □ Evaluate process documentation and its accessibility

2.2 Alignment with Business Objectives

- □ Review IT strategy and its alignment with overall business goals
- □ Assess IT's involvement in business planning processes
- □ Evaluate how IT projects are prioritized and selected
- □ Check for regular business-IT alignment reviews

2.3 Risk Management and Compliance

- □ Review IT risk assessment processes
- □ Evaluate compliance with relevant regulations (e.g., GDPR, HIPAA)
- □ Assess incident response and disaster recovery plans
- □ Assess cyber resilience strategies for compliance and the ability to respond to Advanced Persistent Threats (APT)
- □ Review data protection and privacy processes

2.4 Service Level Agreements (SLAs) & Performance Metrics

- □ Review existing SLAs with internal and external customers
- □ Assess the process for monitoring and reporting on SLAs
- □ Evaluate key performance indicators (KPIs) for IT services
- □ Check for regular service review meetings with stakeholders

2.5 Continuous Improvement

- □ Assess processes for gathering and implementing improvement suggestions, including feedback loops
- □ Review the effectiveness of post-incident reviews and lessons learned
- □ Evaluate the adoption of agile and DevOps practices
- □ Check for regular process audits and optimization efforts

03 Technology Assessment

3.1 Infrastructure and Architecture

- □ Review current IT infrastructure (hardware, software, network)
- □ Review of legacy system modernization efforts to assess cost efficiency and resilience
- □ Assess scalability and flexibility of the infrastructure
- □ Evaluate the effectiveness of cloud adoption strategy
- □ Review disaster recovery and business continuity infrastructure

3.2 Security and Data Protection

- □ Conduct a comprehensive security audit
- □ Assess implementation of security best practices
- □ Review access control and identity management systems
- □ Evaluate data encryption practices for data at rest and in transit
- □ Evaluate adoption of a zero-trust security model, if applicable

3.3 Integration and Interoperability

- □ Assess integration between key systems and applications
- □ Evaluate API management and usage
- □ Review data flow and consistency across systems
- □ Check for redundant or legacy systems that could be consolidated

3.4 Innovation and Emerging Technologies

- □ Assess adoption of emerging technologies (e.g., AI, IoT, blockchain)
- □ Evaluate how emerging technologies and green IT infrastructure might align with corporate sustainability goals
- □ Review processes for evaluating and piloting new technologies
- □ Evaluate the innovation budget and its utilization
- □ Check for partnerships with technology vendors and startups

3.5 User Experience and Accessibility

- □ Assess the usability of IT systems for employees, including internationalization/localization if IT systems serve global users
- □ Review mobile accessibility of key applications
- □ Evaluate help desk and user support effectiveness
- □ Assess the end-user feedback collection processes in support of continuous improvement
- □ Check compliance with accessibility standards for all users

04 Prioritization Framework

This section offers a framework to help SVPs and VPs of Technology prioritize remediation efforts based on risk, impact, and resource availability.

4.1 Risk-Based Prioritization

□ Assign a risk rating (high, medium, low) to each identified issue

□ Evaluate the potential impact of each issue on business continuity and operational efficiency

□ Prioritize issues that expose the organization to the highest risk, such as data breaches or non-compliance with regulations

4.2 Business Impact

□ Identify which areas of the business are most affected by each issue (e.g., customer service, finance, operations)

□ Prioritize issues that impact revenue generation, customer satisfaction, or regulatory compliance

□ Evaluate how IT dependencies affect key business outcomes (e.g., if a process bottleneck impacts time-to-market for products)

4.3 Resource Allocation

□ Assess the internal and external resources required to address each issue

□ Prioritize issues that can be resolved with available resources without impacting critical business projects

□ Evaluate whether outside expertise (consultants, vendors) is needed for complex issues like infrastructure overhaul or major software integrations

4.4 Time Sensitivity

- □ Assign timeframes for each audit finding based on the severity of impact and the organization's risk tolerance
- □ Address issues that may become more costly or problematic if left unaddressed (e.g., legacy system failures, unpatched security vulnerabilities)

4.5 Quick Wins

- □ Identify audit findings that can be resolved quickly with minimal effort and expense
- □ Prioritize these quick wins to build momentum and demonstrate early success in the audit process