baramundi

BARAMUNDI CHECKLISTS provide concise, step-by-step expert advice for handling common IT challenges in a straightforward way. You can find more checklists at: www.baramundi.com/checklists

IT Audits: Optimize Cybersecurity with these 7 steps

Given the slightest opportunity, hackers will lurk in the dark corners of your network looking for open vulnerabilities and outdated technologies to exploit, to steal data or to damage your business and enrich themselves with ransomware and other attacks. A systematic and thorough IT audit can uncover these potential risks and shortcomings so you can take the necessary steps to protect your organization's users and systems, ensure compliance and support company productivity.

Plan

From hardware to data management, identify areas and systems to audit. Define specific objectives such as ensuring compliance, documenting existing security practices, or maintaining cybersecurity awareness among users.

Document

Maintain a current and complete inventory of all hardware, software, network components and system configurations. This will help you provide a clear assessment of status now and progress later.

Audit security effectiveness

Engage trusted resources for pentesting and vulnerability analyses of existing IT cybersecurity measures such as firewalls and antivirus programs. Be sure to review configurations of servers and network components.

Check compliance

Make sure your IT infrastructure complies with all applicable regulations, industry standards or your own internal requirements for security, data protection and business continuity. Take extra care to protect business-critical data appropriately so that normal operations can resume quickly after an emergency, incident or disaster.

Optimize performance

Analyze whether system performance and network infrastructure meet ongoing business needs and are sufficiently scalable to support periods of high demand including during recovery.

Create and action plan

Define actions and needed resources based on priority or urgency, designate clear responsibilities and deadlines, then address identified weaknesses and deficiencies.

Reporting

The final step is the audit report, which records findings, recommendations, priorities for improvement. It is the basis for all subsequent measures. Make the report available to the relevant stakeholders.

In short: In regular IT audits, you identify risks to your cybersecurity. Whether inventory, vulnerability scanner or update management: You can count on the baramundi Management Suite to ensure that your audit succeeds in every IT subarea.