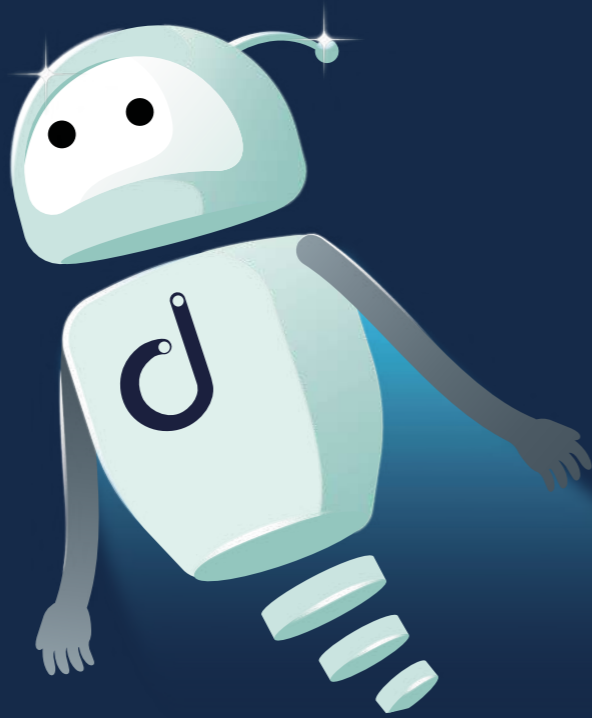


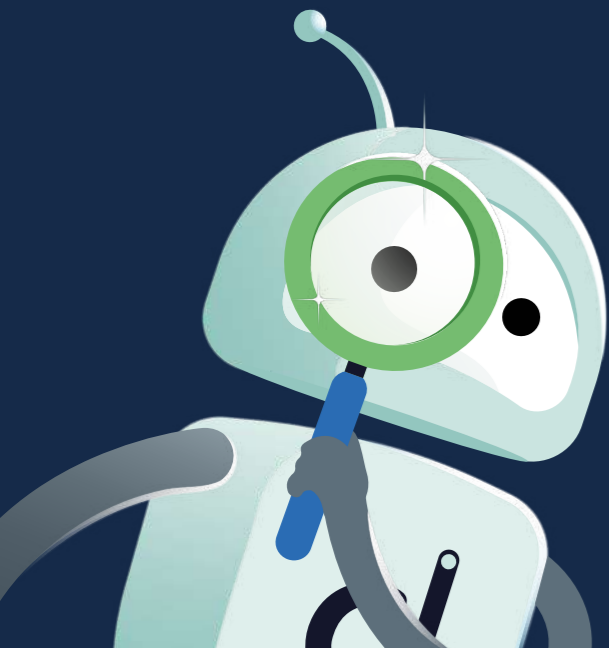


Audit a Network Checklist

Printable Whitepaper



What's covered in this **guide**:



Introduction

What is a Network Audit?

Why Audit a Network?

Benefits of auditing a Network

How often should you audit a network?

Network Audit Checklist

1. Company Policies
2. Password security
3. Network/LAN security
4. Workstations
5. Mobile devices
6. Critical Network Infrastructure
7. Routers/Firewalls

Introduction

Auditing a network is a hugely important task for MSPs, IT professionals, and any other service provider. That's why we wrote a completely free downloadable checklist on auditing a network.

Our handy checklist will help ensure you've got the important aspects of auditing a network covered.

Need to **onboard** a **new network?**

Check out our **free network onboarding template!**

Download our [MSP onboarding checklist with a free printable template](#). Our free onboarding template covers everything from A-Z you need to consider when onboarding a new network. Moreover, it's very useful for onboarding new networks.

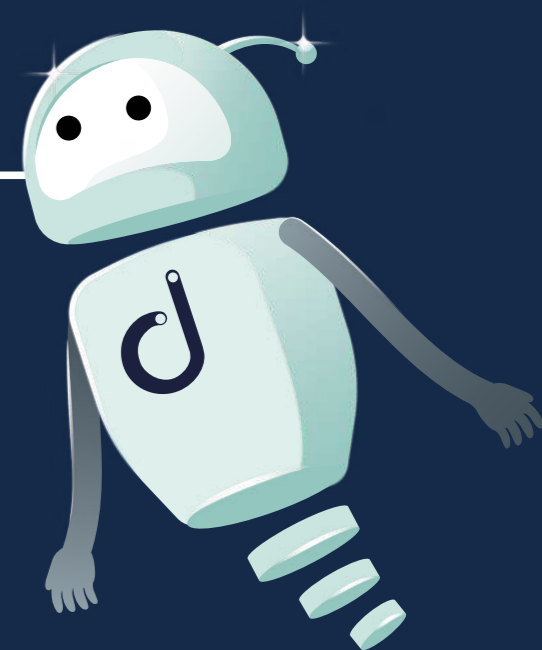
Read on to **learn all about Auditing a Network.**

What is a **Network Audit?**

01.

A network audit looks at all networked systems, devices, processes, and policies to **minimize potential issues and risks.**

Auditing a network involves several important components that ensure the overall **security** and **functionality** of the network infrastructure.



General Auditing:

General auditing involves assessing the overall security posture of the network. This includes evaluating the network's architecture, identifying potential vulnerabilities, and assessing compliance with security policies and standards. It may involve reviewing network diagrams, analyzing network configurations, and conducting interviews with network administrators.

Password Security Auditing:

Password security auditing focuses on assessing the strength and effectiveness of password policies and practices within the network. It involves reviewing password complexity requirements, password expiration policies, and the implementation of multi-factor authentication (MFA) where applicable. Password auditing may also include checking for the presence of weak or easily guessable passwords, identifying accounts with excessive privileges, and ensuring secure password storage mechanisms are in place.

Device Auditing:

Device auditing involves evaluating the security configurations and settings of network devices such as routers, switches, and access points. This includes reviewing device configurations to ensure they adhere to security best practices, identifying any unnecessary services or ports that could pose security risks, and verifying the implementation of encryption protocols. Device auditing also entails checking for firmware updates and patches to ensure devices are running the latest secure versions.

Network Auditing (LAN):

Network auditing for the local area network (LAN) focuses on assessing the security and performance of the internal network infrastructure. This involves reviewing network segmentation, access control mechanisms, and intrusion detection systems (IDS) or intrusion prevention systems (IPS). Network auditing also includes analyzing network traffic patterns, monitoring for unauthorized network access, and identifying any potential network bottlenecks or performance issues.

Workstation Auditing:

Workstation auditing involves evaluating the security configurations and practices of individual workstations within the network. This includes assessing operating system security settings, patch management, and antivirus/anti-malware solutions. Workstation auditing may also involve reviewing user permissions, software installations, and ensuring the presence of host-based firewalls and intrusion detection software.

Mobile Phone Auditing:

Mobile phone auditing focuses on assessing the security of mobile devices that connect to the network. This includes evaluating the implementation of mobile device management (MDM) solutions, enforcing strong authentication mechanisms, and ensuring devices are running the latest firmware and security updates. Mobile phone auditing may also involve reviewing app permissions, data encryption practices, and remote wipe capabilities in case of loss or theft.

Critical Network Infrastructure Auditing:

Critical network infrastructure auditing entails evaluating the security and availability of essential network components such as servers, firewalls, and routers. This includes reviewing server configurations, patch management processes, and access controls. Auditing critical network infrastructure also involves assessing the firewall rules and policies, reviewing network segmentation, and ensuring proper logging and monitoring mechanisms are in place.

Server/Firewall Auditing:

Server and firewall auditing specifically focuses on assessing the security of servers and firewalls within the network. This includes reviewing server configurations, hardening practices, and access controls. Firewall auditing involves evaluating firewall rule sets, checking for any misconfigurations or vulnerabilities, and ensuring that access control policies are effectively implemented. Server and firewall auditing may also involve reviewing log files and monitoring for any suspicious activities or unauthorized access attempts.

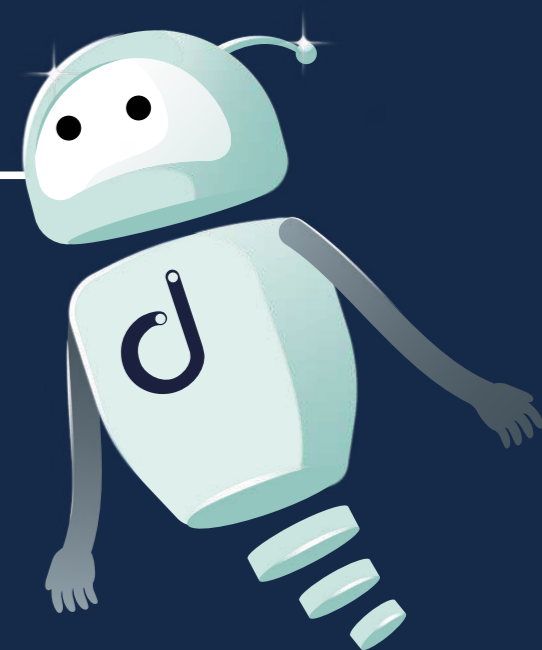
By performing comprehensive network audits across these different areas, organizations can identify potential security weaknesses, ensure compliance with industry standards, and implement necessary measures to enhance the overall security and functionality of their network infrastructure.



Why **Audit** a **Network**?

02.

If you're managing a network, you should be auditing it. Auditing a network will help you look out for threats and ensure compliance with processes such as CIS controls. Additionally, auditing a network can help with performance and detecting issues too.





Even more importantly, it can help with identifying potential areas of a business that could be at risk of network security issues and cyber attacks.

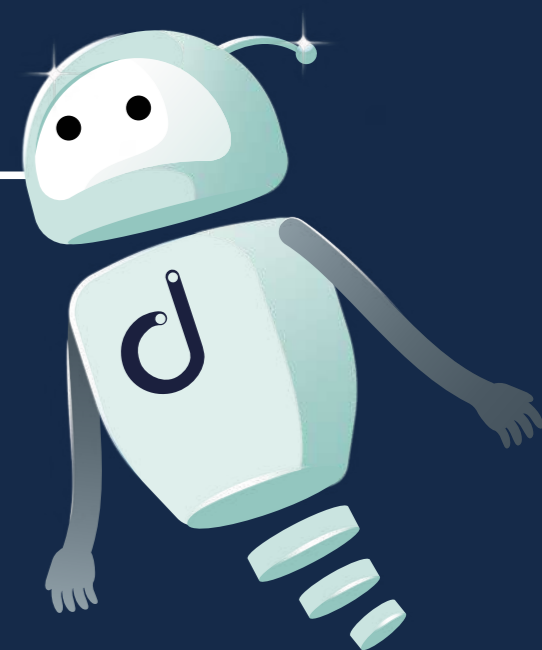
Moreover, the entire process of auditing a network will help you identify areas of the network that need proper practices in place. For example, you may be missing a BYOD policy or alerts on new devices. Auditing a network will help you identify your weaknesses and what is missing to further improve your network management and security processes. Check out [our handy document on CIS controls](#) for more details on this.

Auditing a network gives you an entire picture of your network, policies, and practices. You can use this picture to identify your strengths and weaknesses and areas that need improvement.

Benefits of auditing a Network

03.

Auditing a network has many benefits which are relevant to your organization, customers, policies and procedures. Here are some of the benefits of regularly auditing your networks.



Security

IT network audits help identify vulnerabilities and weaknesses in the network infrastructure, systems, and devices. They'll also help you identify cyber risks: malware, spyware, phishing, virus threats. This can be done through regular risk assessments and by implementing security measures such as firewalls, antivirus software, and intrusion detection systems. Additionally, regular audits of your IT systems and processes help you identify risks to accessing sensitive information and data.

Compliance/maintaining CIS control

Many industries and organizations are subject to regulatory requirements and compliance standards, such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), or General Data Protection Regulation (GDPR). IT network audits help assess whether the organization's network aligns with these regulations and standards. Audits provide evidence of compliance and help organizations avoid penalties, legal issues, and reputational damage associated with non-compliance. Check out our handy document on CIS controls for more details on this.

Performance and Efficiency

Network audits evaluate the network infrastructure, including hardware, software, configurations, and overall architecture. By assessing network performance, audits identify bottlenecks, congestion points, or outdated components that may hinder network efficiency. Audits also help optimize network resources, identify opportunities for improvement, and ensure that the network meets the organization's performance requirements.

Asset Management

IT network audits help organizations maintain an accurate inventory of their network assets, including servers, routers, switches, firewalls, and other devices. Audits ensure that assets are adequately documented, including their physical location, ownership, and relevant configurations. This information is crucial for effective IT asset management, license compliance, maintenance scheduling, and resource planning.

Business Continuity

Network audits assess the network's resilience and ability to handle unexpected events, such as power outages, hardware failures, or natural disasters. By identifying single points of failure, redundant systems, and backup strategies, audits help organizations implement robust business continuity plans. This ensures critical network services and operations can be quickly restored, minimizing downtime and potential financial losses.

Risk Management

IT network audits play a crucial role in identifying and managing risks associated with the network infrastructure. Audits help organizations identify and prioritize risks, develop mitigation strategies, and establish appropriate risk management frameworks by assessing the network's architecture, controls, and processes. This enables organizations to make informed decisions regarding risk tolerance, investment in security measures, and overall risk mitigation efforts.



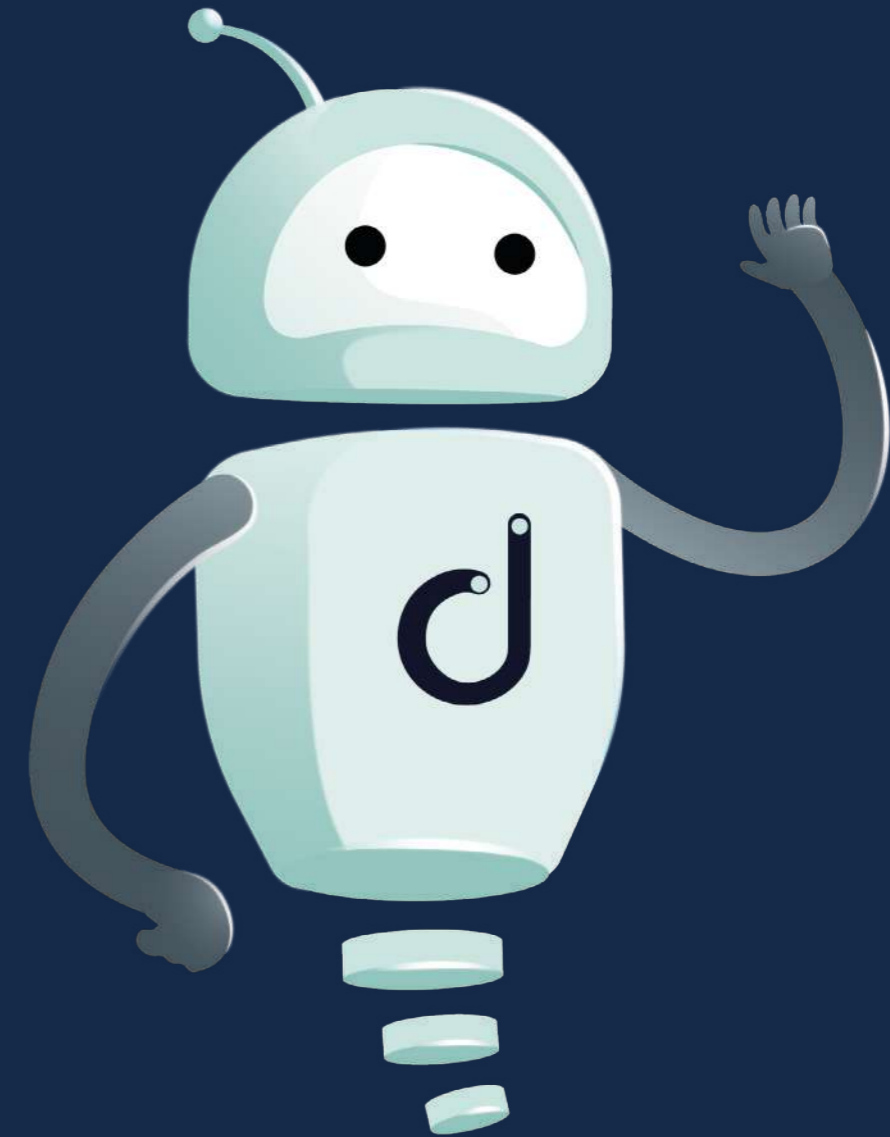
Identify Gaps and Improvements

A regular self-assessment can help you identify areas where you excel and areas where you could improve. This is crucial to improving your networking operations over time. A regular self-assessment can also help you review your current policies and procedures to identify any gaps or areas that need improvement. You can then work with your team to develop new policies and procedures.

Ensure Functioning and Set-up

A regular self-assessment will help you make sure that everything on your network has been set-up correctly and is functioning as it should be. Through each audit, you'll really dive into monitoring network traffic, ensuring that all devices are up-to-date with the latest security patches, and implementing firewalls and other security measures as part of the process. The end result is that you can ensure the functioning of a network is still being maintained. Additionally, you'll be able to regularly check that everything is set-up correctly.

Overall, IT network audits provide organizations with a comprehensive assessment of their network infrastructure, security posture, compliance status, and overall performance. By addressing vulnerabilities, ensuring compliance, optimizing resources, and managing risks, audits help organizations enhance their network's reliability, security, and efficiency, ultimately contributing to the business's overall success.



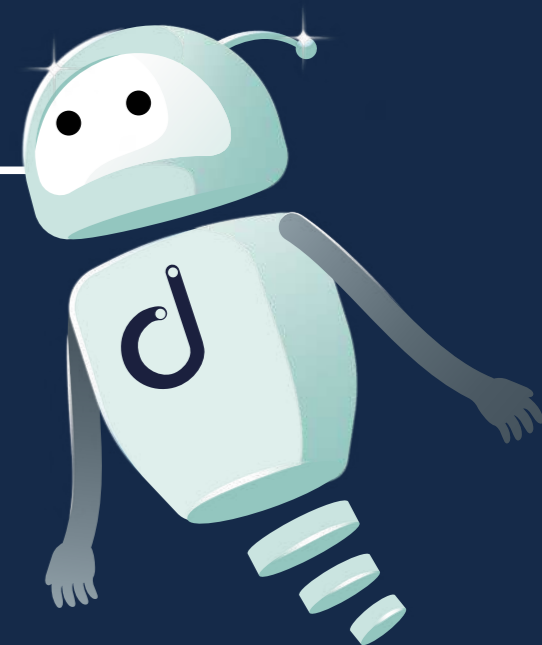
How often should you audit a network?

04.

How often you audit a network depends on various factors.

CIS controls recommend having in place [Continuous Vulnerability Management](#). As part of your continuous vulnerability management, you may set a maximum threshold for auditing a network. For example, once every 6 months or on an annual basis.

Regardless of how frequently you've chosen to audit the networks you're managing, we recommend auditing a network regularly and recurringly.



Who Performs a Network Security Audit?

MSPs

As an MSP, you may perform network audits to onboard a new network. Then after, you may perform them regularly for your clients.

Internal IT team

If you are part of an IT team, your team may be tasked with continuously auditing the networks you manage. This could be a single network or multiple, depending on the size of an organization.

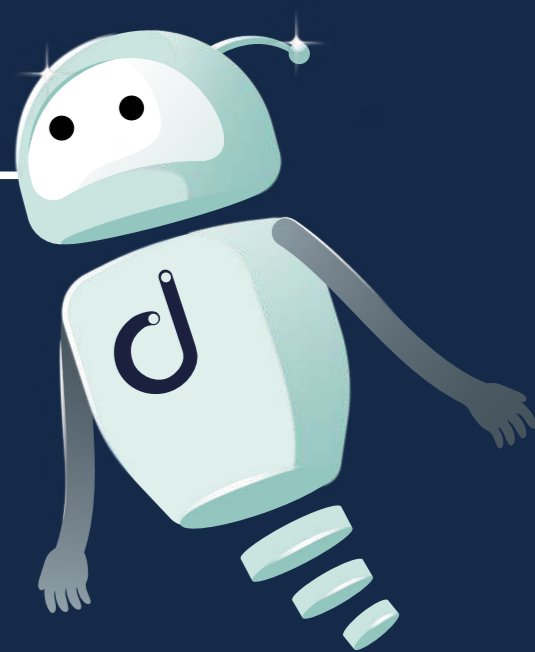
External auditors


Even if you are an MSP or part of an Internal IT team, you may choose to have an external auditor perform a network audit. Having an extra set of eyes on everything you're doing is always a good idea. External auditors will be thorough and objective. They aren't familiar with the network and will not have access to any shortcuts or bypassing of rules because they know the system. Additionally, often Security Frameworks require the need for external auditors to validate that your security process is being followed and up to the standards that you have set.

Network Audit Checklist

05.

To undergo a full network audit, we've compiled a checklist with all the steps you can follow for each area.





DESCRIPTION	STATUS
1 <h2 style="text-align: center;">Company Policies</h2> 	
<p>Network policy - ensure there is a network security policy. If no policy is available, draft one. Include the rights and responsibilities of all team members, employees, consultants, contractors, and guests in the policy. Review any existing policy and amend it as needed.</p>	<input type="checkbox"/>
<p>Data sharing policy - ensure there is a data sharing policy. If no policy is available, draft one. Review any existing policy and amend it as needed.</p>	<input type="checkbox"/>
<p>Acceptable use policy - ensure there is an acceptable use policy. If no policy is available, draft one. Review any existing policy and amend it as needed.</p>	<input type="checkbox"/>
<p>Bring Your Own Device (BYOD) policy - ensure there is a BYOD policy. If no policy is available, draft one. Review any existing policy and amend it as needed.</p>	<input type="checkbox"/>
<p>Security training - ensure all employees have completed security training and reviewed and accepted all critical documentation: data sharing, acceptable use, BYOD, etc.</p>	<input type="checkbox"/>
<p>Information sharing training - ensure all employees have completed training on information sharing.</p>	<input type="checkbox"/>
<p>Vendor policy acceptance - review the vendor security agreement. Ensure that all vendors have signed the security agreement.</p>	<input type="checkbox"/>
<p>Data security/breach plan - ensure there is a plan in place for a data or security breach happens. If no plan is drafted, this is a great time to draft one.</p>	<input type="checkbox"/>


DESCRIPTION	STATUS
<h2 data-bbox="468 512 528 590">2</h2> <h1 data-bbox="783 512 2184 590">Password security best practices</h1>	
<p data-bbox="468 716 2208 793">Password security policy - ensure there is a written password security policy. If no policy is available, draft one. Review any existing policy and amend it as needed.</p>	<input data-bbox="2451 720 2522 791" type="checkbox"/>
<p data-bbox="468 951 1843 987">Password training - ensure all users have completed appropriate password training and know the risks.</p>	<input data-bbox="2451 934 2522 1005" type="checkbox"/>
<p data-bbox="468 1152 1955 1230">Inspect physical environments - physically inspect the workstations of employees and check for passwords that may be written down.</p>	<input data-bbox="2451 1157 2522 1228" type="checkbox"/>
<p data-bbox="468 1409 2258 1444">Documenting password requirements - keep a document of password requirements somewhere accessible anytime for all employees.</p>	<input data-bbox="2451 1392 2522 1463" type="checkbox"/>


DESCRIPTION	STATUS
<h1>3 Network/LAN Security</h1>	
Strengthen the internal network servers.	<input type="checkbox"/>
Remove unused and unnecessary services and applications on the network.	<input type="checkbox"/>
Check server permissions - ensure they are appropriate for all users and circumstances.	<input type="checkbox"/>
Remove unnecessary files.	<input type="checkbox"/>
Check to make sure there are no anonymous users. Remove as needed.	<input type="checkbox"/>
Ensure there is a remote administration policy in place. Review and amend as needed.	<input type="checkbox"/>
Disable remote access when it is not needed.	<input type="checkbox"/>
Disable guest access when it is not needed.	<input type="checkbox"/>
Create appropriate AD-privileged user groups. Monitor them as necessary. You can Monitor AD-privileged user groups with Domotz.	<input type="checkbox"/>
Create appropriate Windows GPOs. Monitor them as necessary. You can Monitor Windows GPOs with Domotz.	<input type="checkbox"/>

DESCRIPTION	STATUS
3 Network/LAN Security	
Set up Windows security events and monitor them as necessary. You can Monitor Windows security events with Domotz.	<input type="checkbox"/>
Monitor and audit administrator login attempts.	<input type="checkbox"/>
Track access to files/systems/folders/accounts.	<input type="checkbox"/>
Ensure wireless security protocols are configured and in place.	<input type="checkbox"/>

DESCRIPTION	STATUS
<h1>4 Workstations</h1>	
<p>Lock Screen - ensure there is a lock screen on all computers.</p>	<input type="checkbox"/>
<p>Passwords - ensure all computers require passwords.</p>	<input type="checkbox"/>
<p>Implement two-factor authentication where possible.</p>	<input type="checkbox"/>
<p>Remove unnecessary apps and programs from endpoints.</p>	<input type="checkbox"/>
<p>Ensure that anti-virus software is installed and working for each user.</p>	<input type="checkbox"/>
<p>Ensure that RMM software is installed and working for each user.</p>	<input type="checkbox"/>
<p>Ensure that software updates are automatically implemented on workstations through Windows Update Agent (WUA). You can use Domotz for WUA monitoring.</p>	<input type="checkbox"/>
<p>Ensure that RMM is implementing OS and security patches.</p>	<input type="checkbox"/>
<p>Enable pop-up blockers.</p>	<input type="checkbox"/>

DESCRIPTION	STATUS
5 <h2 style="text-align: center;">Mobile Devices</h2>	
<p>Ensure that you have new device alerts set up on the network. Get real-time alerts when new devices connect. Hint: you can use Domotz for new device alerts.</p>	<input type="checkbox"/>
<p>Ensure there is a BYOD policy in place. Review any existing policy and amend it as needed.</p>	<input type="checkbox"/>
<p>Secure Wireless Access points.</p>	<input type="checkbox"/>
<p>Enforce the BYOD policy through new device alerts and blocking devices at the firewall level.</p>	<input type="checkbox"/>

DESCRIPTION	STATUS
<h1>6 Critical Network Infrastructure</h1>	
<p>Ensure that critical network infrastructure is being continuously monitored. You can use Domotz for network infrastructure monitoring.</p>	<input type="checkbox"/>
<p>Ensure network configuration management is in place for critical network infrastructure where possible. You can use Domotz for network configuration management.</p>	<input type="checkbox"/>
<p>Ensure that firmware upgrades occur regularly.</p>	<input type="checkbox"/>
<p>Document network configurations. You can also use Domotz to back up/restore your network appliance configurations.</p>	<input type="checkbox"/>
<p>Document network topology. You can use Domotz for automated network topology mapping.</p>	<input type="checkbox"/>
<p>Document user accounts and passwords.</p>	<input type="checkbox"/>
<p>Perform LAN perimeter scans and external WAN perimeter scans. You can use Domotz for your LAN/WAN scans.</p>	<input type="checkbox"/>

DESCRIPTION	STATUS
<h1>7 Routers/Firewalls</h1> 	
<p>Ensure a firewall is being used.</p>	<input type="checkbox"/>
<p>Ensure all public-facing services are segmented.</p>	<input type="checkbox"/>
<p>Ensure that all external IP addresses are not allowed on the LAN and only on the segmented network.</p>	<input type="checkbox"/>
<p>Configure firewall policies. You can also monitor firewall policies with Domotz using our pre-configured SNMP templates for Watchguard, Sophos, and Fortinet.</p>	<input type="checkbox"/>
<p>Scan for opened ports and close them as needed. You can use Domotz TCP Open Port Scanner for this.</p>	<input type="checkbox"/>
<p>Identify whether UPnP is enabled on the Router / Modem and whether any device on the network is leveraging UPnP to open ports and redirect the traffic. You can use Domotz network security scanner for this.</p>	<input type="checkbox"/>
<p>Deny inbound access to unused ports.</p>	<input type="checkbox"/>
<p>Review firewall policies and identify any risks.</p>	<input type="checkbox"/>
<p>Implement NAT configuration where possible.</p>	<input type="checkbox"/>

DESCRIPTION	STATUS
7 Routers/Firewalls	
Implement packet inspection of network traffic where possible.	<input type="checkbox"/>
Use network configuration management for router and firewall. Ensure firmware and software are updated regularly and automatically where possible. You can use Domotz for network configuration management.	<input type="checkbox"/>
Perform penetration tests to identify further weaknesses.	<input type="checkbox"/>



www.domotz.com

