Cyber Security Checklist

The following is a comprehensive checklist to determine the level of Security controls within your organization. This guide is designed to measure your level of compliance with the basic set of standards for Network and security controls. At the end of each section, you will score the section, and at the completion of the survey, you will compile an overall score. This will determine your overall compliance rate.

Physical Security		
Item	***Yes***	***No***
Do you have policies and procedures to address authorized and limited access to facilities, including data centers		
Are visitors escorted in and out of controlled areas		
Are PC screens automatically locked after an idle period		
Do you have policies covering laptop, tablet, or mobile device security		
Do you have a current emergency evacuation plan		
Do you have an accurate up to date inventory of all electronic equipment		
Do you have an accurate up to date asset tag inventory of all essential equipment		
Are your data closets and/or server rooms equipped with intrusion alarms		
Are unused network access ports physically disabled		
Is your data center/server room locked at all times		
Do you have environmental controls dedicated to your data closets and server rooms		
Do you have fire suppressions systems dedicated to your data closets and server rooms		
Are default security setting changed on software and hardware before they are placed in operation		
Are policies and procedures in place to control equipment plugged into the network		
Is your physical facility monitored and reviewed via camera systems		
Totals		

Personnel		
Item	***Yes***	***No***
Does your staff wear ID Badges		
Do you check credentials of external contractors		
Do you have policies to address background checks of contractors		
Do you have policies addressing background checks of employees		
Do you have a policy for unauthorized use of “open” computers		
Do you have a policy and procedure in place to handle the removal of employees who retire, are terminated, or leave including passwords and access to systems		
Do you have an acceptable use policy that governs email and Internet access		
Do you have a policy governing Social Media use and access by employees		
Are employees required to sign an agreement verifying they have read and understood all policies and procedures		
Are these policies and procedures reviewed with employees at least annually		
Totals		

Account and Password Management		
Item	***Yes***	***No***
Do you have policies and procedures covering authentication, authorization, and access control of personnel and resources to systems		
Are policies in place to ensure only authorized users have access to PC’s		
Are policies and procedures in place to enforce secure, appropriate, and complex passwords		
Are information systems such as servers, routers, and switches protected with basic or better authentication mechanisms		
Has the default “Administrator” account been disabled and/or deactivated		
Are all access attempts logged and reviewed		
Are employees required to change their passwords on a routine schedule		
Are employees prevented from using previous passwords		
Are all passwords on network devices encrypted		
Do you have legal and/or policy notifications on all log-in screens that is seen and accepted prior to access to any network device		
Totals		

Data Security		
Item	***Yes***	***No***
Do you have policy for information retention		
Do you have policies and procedures for management of personal private information		
Do you have a policy for disposing of old and outdated equipment		
Do you have policies and procedures in place for the secure destruction or sanitation of media and/or drives before they are removed, sold or disposed of		
Is access to data or systems accessed remotely both from a dedicated link and encrypted		
Do you have policies and procedures in place to ensure that documents are converted into formats that cannot be easily modified before they are circulated outside the network		
Are documents digitally signed when they are converted to formats that cannot be easily modified		
Is access to critical applications restricted to only those who need access		
Are UPS batteries used on all critical equipment		
Totals		

Network Security

Item	***Yes***	***No***
Is Network traffic regularly monitored for patterns		
Do critical systems have redundant communication connections		
Does your network utilize redundant DNS servers in case of interruption to one server		
Is your DNS servers reviewed on a periodic basis for anomalies and consistency		
Is your Active Directory reviewed periodically for anomalies and consistency		
Are all unnecessary services disabled on servers		
Does your network utilize redundant domain controllers in case of interruption to one server		
Are there policies and procedures governing the use of wireless connections to your network		
Are wired and wireless networks within your organization segregated either physically or virtually through routers, switches, or firewalls		
Do you employ firewalls on your network to control access and traffic		
Are firewalls configured to only allow traffic from approved lists		
Are Network Security Logs reviewed regularly		
Are web filters used to restrict uploading of confidential information		
Are web filters used to restrict downloading of unapproved material		
Are content filters used to restrict web activity		
Are filters or firewalls used to filter executable or malicious email attachments		
Are policies and procedures in place for software patches and updates		
Are policies and procedures in place for hardware patches and updates		
Are your security polices reviewed on a yearly basis		
Are current and up to date Antivirus solutions loaded on all computers		
Are Antivirus and other security software updated with current patches on a regular basis		
Do you use Spyware and Malware Software		
Are all computers current with all security and operating system patches and updates		
Do you employee “Least Privilege” access and review access privilege periodically		
Do you have an accurate and up to date software inventory list		
Totals		

Disaster Recovery/Network Maintenance

Item	*Yes*	*No*
Do you have a current Continuity of Operations Plan (COOP)		
Do you have a current Continuity of Government Plan (COG)		
Do you have a current Disaster Recovery Plan		
Do you have an Emergency Management Communications Plan		
Do you have an Emergency Plan to cover Internal & External Communications		
Do you have an Emergency Response Plan		
Are all your Emergency Plans stored in a remote location		
Are your Emergency plans tested at minimum annually		
Do you have a current detailed network topology		
Do you have a current floor plan with all data equipment labeled		
Have all cables and equipment been physically labeling in wiring closets		
Totals		

Awareness and Education

Item	*Yes*	*No*
Do you provide training on a regular basis		
Do you provide training on computer security		
Do you provide training on data breaches		
Do you provide training on password security		
Do you provide training on email and social media security		
Are employees restricted from saving sensitive data on CD's, DVD's, Flash Drives, or other removable media unless it is required		
Do you have policies and procedures in place to prevent downloading and execution of executable files without being scanned and reviewed by IT		
Are all employees trained on the procedures for notification in case of a breach or attack		
Do you provide training on Social Engineering including phone and email solicitation		
Do you provide training on the use of data processing programs including security implications of document file types		
Totals		

Backups

Item	*Yes*	*No*
Are backups completed on a daily basis		
Do you have policies and procedures in place that govern backups		
Are operating systems, programs, and operating information backed up as well as data		
Are configurations of switches and routers backed up		
Are backups tested regularly – at least monthly		
Are backups transferred to a remote device or location that is kept offsite		
Do you have a process for creating backup copies of critical data		
Are backup solutions updated to the current firmware or software patches		
Are backup logs reviewed regularly for compliance and successful completion		
Do you have a policy in place governing who have access to backups		
Totals		

Scoring of the Cyber Security Checklist

Category	***Yes***	***Possible***
Physical Security		15
Personnel		10
Account and Password Management		10
Data Security		9
Network Security		25
Disaster Recovery/Network Maintenance		11
Awareness and Education		10
Backups		10
Grand Total		**100**

Scoring Scale

Score	Risk Level	Comments
0-50	High Risk	Network, policies, and procedures need immediate attention
51-70	Medium Risk	Network, policies, and procedures need addressing to improve compliance
71-80	Moderate Risk	A number of areas are where they need to be but others need addressing
81-90	Low Risk	Most of you procedures are in place, but a little tweaking needs to be done
91-100	Secure Network	Your network and its policies and procedures are in place. You need to address some fine details