DATACENTERS

CYBERSECURITY CHECKLIST

DATACENTERS.com

Cybersecurity Controls Checklist

This is a simple checklist designed to identify and document the existence and status for a recommended basic set of cyber security controls (policies, standards, and procedures) for an organization. Security controls are designed to reduce and/or eliminate the identified threat/vulnerabilities that place an organization at risk.

Personnel Security	Yes	No
Does your staff wear ID badges?		
Is a current picture part of the ID badge?		
Are authorized access levels and type (employee, contractor, and visitor) identified on the Badge?		
Do you check the credentials of external contractors?		
Do you have policies addressing background checks for employees and contractors?		
Do you have a process for effectively cutting off access to facilities and information systems when an employee/contractor terminates employment?		
Physical Security	**Yes**	**No**
Do you have policies and procedures that address allowing authorized and limiting unauthorized physical access to electronic information systems and the facilities in which they are housed?		
Do your policies and procedures specify the methods used to control physical access to your secure areas, such as door locks, access control systems, security officers, or video monitoring?		

 (877) 406-2248 | info@datacenters.com | www.datacenters.com

Is access to your computing area controlled (single point, reception or security desk, sign-in/sign-out log, temporary/visitor badges)?		
Are visitors escorted into and out of controlled areas?		
Are your PCs inaccessible to unauthorized users (e.g. located away from public areas)?		
Do you have a process for effectively cutting off access to facilities and information systems when an employee/contractor terminates employment?		
Are your PCs inaccessible to unauthorized users (e.g. located away from public areas)?		
Are visitors escorted into and out of controlled areas?		
Are your PCs inaccessible to unauthorized users (e.g. located away from public areas)?		
Are there procedures in place to prevent computers from being left in a logged-on state, however briefly?		
Are screens automatically locked after 10 minutes idle?		
Are modems set to Auto-Answer OFF (not to accept incoming calls)?		
Do you have procedures for protecting data during equipment repairs?		
Do you have policies covering laptop security (e.g. cable lock or secure storage)?		
Do you have an emergency evacuation plan and is it current?		

Does your plan identify areas and facilities that need to be sealed off immediately in case of an emergency?		
Are key personnel aware of which areas and facilities need to be sealed off and how?		

Account & Password Management	Yes	No
Do you have policies and standards covering electronic authentication, authorization, and access control of personnel and resources to your information systems, applications and data?		
Do you ensure that only authorized personnel have access to your computers?		
Do you require and enforce appropriate passwords?		
Are your passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?		
Are you computers set up so others cannot view staff entering passwords?		

Confidentiality of Sensitive Data	Yes	No
Do you classify your data, identifying sensitive data versus non-sensitive?		
Are you exercising responsibilities to protect sensitive data under your control?		
Is the most valuable or sensitive data encrypted?		
Do you have a policy for identifying the retention of information (both hard and soft copies)?		

Do you have procedures in place to deal with credit card information?		
Do you have procedures covering the management of personal private information?		
Is there a process for creating retrievable backup and archival copies of critical information?		
Do you have procedures for disposing of waste material?		
Is waste paper binned or shredded?		
Is your shred bin locked at all times?		
Do your policies for disposing of old computer equipment protect against loss of data (e.g.. by reading old disks and hard drives)?		
Do your disposal procedures identify appropriate technologies and methods for making hardware and electronic media unusable and inaccessible (such as shredding external HDs, thumb drives, CDs and DVDs, electronically wiping drives, burning tapes) etc.)?		

Disaster Recovery	Yes	No
Do you have a current business continuity plan?		
Is there a process for creating retrievable backup and archival copies of critical information?		
Do you have an emergency/incident management communications plan?		
Do you have a procedure for notifying authorities in the case of a disaster or security incident?		
Does your procedure identify who should be contacted, including contact information?		

Is the contact information sorted and identified by incident type?		
Does your procedure identify who should make the contacts?		
Have you identified who will speak to the press/public in the case of an emergency or an incident?		
Does your communications plan cover internal communications with your employees and their families?		
Can emergency procedures be appropriately implemented, as needed, by those responsible?		

Security Awareness & Education	Yes	No
Are you providing information about computer security to your staff?		
Do you provide training on a regular recurring basis?		
Are employees taught to be alert to possible security breaches?		
Are your employees taught about keeping their passwords secure?		
Are your employees able to identify and protect classified data, including paper documents, removable media, and electronic documents?		
Does your awareness and education plan teach proper methods for managing credit card data (PCI standards) and personal private information (Social security numbers, names, addresses, phone numbers, etc.)?		

Compliance & Audit	Yes	No
Do you review and revise your security documents, such as: policies, standards, procedures, and guidelines, on a regular basis?		
Do you audit your processes and procedures for compliance with established policies and standards?		
Do you test your disaster plans on a regular basis?		
Does management regularly review lists of individuals with physical access to sensitive facilities or electronic access to information systems?		

Checklist Response Analysis

For each question that is marked "No," carefully review its applicability to your organization. Implementing or improving controls decreases potential exposure to threats/vulnerabilities that may seriously impact the ability to successfully operate.

Contact us at (877) 406-2248 for cybersecurity audits, penetration testing, vulnerability testing, encryption, DDoS protection, and more.

Threat and Vulnerability Assessment I

A threat is the potential for a person or a thing to exercise (accidentally trigger or intentionally exploit) a flaw or weaknesses (vulnerability) within an organization. There are several types of threats that my occur within an information system or operating environment Threats are usually grouped into general categories such as natural, human, and environmental, for example:

Natural Threats			
Storm Damage	Fire	Lightning Strikes	Tornado
Human Threats			
Computer Abuse	Unauthorized Access	Terrorism	Sabotage
Vandalism	Tampering	Spoofing	Fraud
Impersonation	Social Engineering	Hacking	Human Error
Theft	Falsified Data		
Environmental Threats			
Power Failure	Chemical Leakage	Pollution	

Determine Your Risk

The desired outcome of identifying and reviewing (assessing) threats and vulnerabilities is determining potential and actual risks to the organization. Risk is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organizations.

Risk is established by considering the potential impact and likelihood of a vulnerability being exploited by a threat. Risk only exists when threats have the capability of triggering or exploiting vulnerabilities. The following formula is used to determine a risk score:

Risk = Impact x Likelihood

For this assessment, numeric rating scales are used to establish impact potential (0-6) and likelihood probability (0-5).

Impact Scale	Likelihood Scale
1. Impact is negligible	0. Unlikely to occur
2. Effect is minor, major agency operations are not affected	1. Likely to occur less than once per year
3. Organization operations are unavailable for a certain amount of time, costs are incurred. Public/customer confidence is minimally affected	2. Likely to occur once per year
4. Significant loss of operations, significant impact on pubic/customer confidence	3. Likely to occur once per month

5. Effect is disastrous, systems are down for an extended period of time, systems need to be rebuilt and data replaced	4. Likely to occur once per week
6. Effect is catastrophic, critical systems are offline for an extended period; data are lost or irreparably corrupted; public health and safety are affected	5. Likely to occur daily

When determining impact, consider the value of the resources at risk, both in terms of inherent (replacement) value and the importance of the resources (criticality) to the organization's successful operation.

Factors influencing likelihood include: threat capability, frequency of threat occurrence, and effectiveness of current countermeasures (security controls). Threats caused by humans are capable of significantly impairing the ability for an organization to operate effectively. Human threats sources include:

Source	Source Description
Insiders	Employees, owners, stock holders, etc.
General contractors and subcontractors	Cleaning crew, developers, technical support personnel, and computer and telephone service repair crew
Former employees:	Employees who have retired, resigned, or were terminated

Unauthorized users:	Computer criminals, terrorists, and intruders (hackers and crackers) who attempt to access agency/enterprise resources.

Finally, use the following table to determine and understand the potential criticality (risk level) of each threat/vulnerability based on the calculated risk value.

Score	Risk Level	Risk Occurrence Result
21-30	High Risk	Occurrence may result in significant loss of major tangible assets, information, or information resources. May significantly disrupt the organization's operations or seriously harm its reputation.
11-20	Medium Risk	Occurrence may result in some loss of tangible assets, information, or information resources. May disrupt or harm the organization's operation or reputation. For example, authorized users aren't able to access supportive data for several days.

1-10	Low Risk	Occurrence may result in minimal loss of tangible assets, information, or information resources. May adversely affect the organization's operation or reputation. For example, authorized users aren't granted access to supportive data for an hour.

Threat and Vulnerability Assessment II

Human Threats	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
Human Error			
Accidental destruction, modification, disclosure, or incorrect classification of information			
Ignorance: inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge			
Workload: Too many or too few system administrators, highly pressured users			
Users may inadvertently give information on security weaknesses to attackers			
Incorrect system configuration			
Security policy not adequate			
Security policy not enforced			
Security analysis may have omitted something important or be wrong.			

Dishonesty: Fraud, theft, embezzlement, selling of confidential agency information			
Attacks by “social engineering”			
Attackers may use telephone to impersonate employees to persuade			
users/administrators to give user name/passwords/modem numbers, etc.			
Attackers may persuade users to execute Trojan Horse programs			
Abuse of privileges/trust			

General Threats	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
Human Error			
Unauthorized use of “open” computers/laptops, mobile devices			
Mixing of test and production data or environments			
Introduction of unauthorized software or hardware			
Time bombs: Software programmed to damage a system on a certain date			
Operating system design errors: Certain systems were not designed to be highly secure			
Protocol design errors: Certain protocols were not designed to be highly secure.			
Protocol weaknesses in TCP/IP can result in:			
Source routing, DNS spoofing, TCP sequence guessing, unauthorized access			
Hijacked sessions and authentication session/transaction replay, data is changed or copied during transmission			
Denial of service, due to ICMP bombing, TCP-SYN			

flooding, large PING packets, etc.			
Logic bomb: Software programmed to damage a system under certain conditions			
Viruses in programs, documents, e-mail attachments			
Identification Authorized Threats			
Attack programs masquerading as normal programs (Trojan horses).			
Attack hardware masquerading as normal commercial hardware			
External attackers masquerading as valid users or customers			
Internal attackers masquerading as valid users or customers			
Attackers masquerading as helpdesk/support personnel			

Privacy Threats	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
Eavesdropping			
Electromagnetic eavesdropping / Ban Eck radiation			
Phone/fax eavesdropping (via “clip-on” telephone bugs, inductive sensors, or hacking the public telephone exchanges			
Network eavesdropping. Unauthorized monitoring of sensitive data crossing the internal network, unknown to the data owner			
Subversion of ONS to redirect email or other traffic			
Subversion of routing protocols to redirect email or other traffic			
Radio signal eavesdropping,			
Rubbish eavesdropping (analyzing waste for			

confidential documents, etc.)			
Integrity/ Accuracy Threats			
Malicious, deliberate damage of information or information processing functions from external sources			
Malicious, deliberate damage of information or information processing functions from internal sources			
Deliberate modification of information			
Access Control Threats			
Password cracking (access to password files, use of bad – blank, default, rarely changed – passwords)			
External access to password files, and sniffing of the networks			
Attack programs allowing external access to systems (back doors visible to external networks)			
Attack programs allowing internal access to systems (back doors visible to internal networks)			
Unsecured maintenance modes, developer backdoors			
Routers, switches, modems easily connected, allowing uncontrollable extension of the internal network			
Bugs in network software which can open unknown/unexpected security holes (holes can be exploited from external networks to gain access. This threat grows as software becomes increasingly complex)			
Unauthorized physical access to system			
Repudiation Threat			
Receivers of confidential information may refuse to acknowledge receipt			
Senders of confidential information may refuse to			

acknowledge source			
Legal Threats			
Failure to comply with regulatory or legal requirements (ie, to protect confidentiality of employee data)			
Liability for acts of internal users or attackers who abuse the system to perpetrate unlawful acts (ie, incitement to racism, gambling, money laundering, distribution of pornographic or violent material)			
Liability for damages if an internal user attacks other sites.			
Reliability of Service Threats			
Major natural disasters, fire, smoke, water, earthquake, storms/hurricanes/tornadoes, power outages, etc			
Minor natural disasters, of short duration, or causing little damage			
Major human-caused disasters: war, terrorist incidents, bombs, civil disturbance, dangerous chemicals, radiological accidents, etc.			
Equipment failure from defective hardware, cabling, or communications system.			
Equipment failure from airborne dust, electromagnetic interference, or static electricity			
Denial of Service			
Network abuse: Misuse of routing protocols to confuse and mislead systems Server overloading (processes, swap space, memory, “tmp” directories, overloading services)			
Email bombing			
Downloading or receipt of malicious Applets, Active X controls, macros, PostScript files, etc			
Sabotage: Malicious, deliberate damage of			

information or information processing functions.			
Physical destruction of network interface devices, cables			
Physical destruction of computing devices or media			
Destruction of electronic devices and media by electromagnetic radiation weapons (HERF Gun, EMP/T Gun)			
Deliberate electrical overloads or shutting off electrical power			
Viruses and/or worms. Deletion of critical systems files			

Next Steps

After completing a review of current security controls and along with a review and rating of potential threats/vulnerabilities, a series of actions should be determined to reduce risk (threats exploiting vulnerabilities) to and acceptable level. These actions should include putting into place missing security controls, and/or increasing the strength of existing controls.

Security controls should ideally reduce and/or eliminate vulnerabilities and meet the needs of the business. Cost must be balanced against expected security benefit and risk reduction. Typically, security remediation efforts and actions will be focused on addressing identified high risk threat/vulnerabilities

Contact us at (877) 406-2248 for cybersecurity audits, penetration testing, vulnerability testing, encryption, DDoS protection, and more.

Example Recommended Security Risk Remediation Actions

The following table identifies a set of remediation activities designed to focus on the commonly identified High risk threats and vulnerabilities. Actions are ranked in priority order of effectiveness.

No.	Remediation Action	Cost	Benefit	Risk
1	Develop a foundation of Security Policies, Practices and Procedures, especially in the area of Change Control	Low	High	High
2	Establish and enforce a globally-accepted password policy	Low	High	High
3	Address vulnerability results in order of high risk to low risk	Low	High	High
4	Establish an Operations group facilitated discussion to improve processes and communications, and to eliminate any misunderstandings	Low	High	High
5	Establish router configuration security standards, forming baseline practice	Low	High	High
	Harden servers on the internal network			

6	More closely integrate worker termination activities between HR and IT. Incorporate new-hire orientation and annual security “refresher” for all employees.	Low to Moderate	High	No
7	Redesign the internet perimeter, incorporating concepts of N-tier architecture and “defense in depth” into the redesign of the Internet perimeter and Enterprise Architecture	Low to Moderate	High	High
8	Migrate to a more centralized and integrated model of operations management, including centralized logging, event correlation, and alerting Low to Moderate	Low to Moderate	High	High
9	Complete the intrusion detection infrastructure	Moderate to Expensive	High	High
10	Install encryption on mobile computers to protect the confidentiality and integrity of data.	Moderate to Expensive	High	High
11	Perform data classification to determine security levels to protect that data Moderate to Expensive	Moderate to Expensive	High	High

12	Institute vulnerability scanning as a regular scheduled maintenance task Moderate to Expensive	Moderate to Expensive	High	High
13	Reclassify email as a mission critical application	Low	Moderate	High
14	Complete security staffing for the ISO Security Group	Expensive	High	High
15	Complete Computer Security Incident Response Team (CSIRT) capability	Moderate to Expensive	High	High

About Datacenters.com

Datacenters.com is the world's resource for accurate, detailed and up-to-date information on data center companies, facilities and markets globally. Since 2009, Datacenters.com has focused on making it easy for website users to find, compare and shop data center, cloud and related technology solutions.

In addition to being a powerful online resource, Datacenters.com operates in four key strategic segments including consulting and advisory, sourcing of technology services, industry research, and commercial real estate listings. Datacenters.com provides independent consulting services with a team of in-house and outside consultants, solution architects and engineers.

The company is headquartered in Englewood, Colorado, and has a large regional, US and International footprint.

Contact us at (877) 406-2248 for cybersecurity audits, penetration testing, vulnerability testing, encryption, DDoS protection, and more.