IT Security Audit
& Risk Assessment Checklist

Duck Technologies
Information Security

Practical guidance identifying and
eliminating risks to your IT operation

IT Security Risk Assesment

Assign each area a risk rating from 0 to 10, 10 being a perfect score in that area

Operational Security

Business Operations □

Do comprehensive maps of your IT infrastucture and diagrams of your physical network exist?

Policies & Procedures □

Do staff members clearly understand their responsibility for company computer security?

Are there policies governing the usage of instant messaging in place?

Are there restrictions on the types of web content accessible from inside the network?

Is unencrypted transmission of sensitive data via memos or emails discouraged or regulated?

Are Vendors Holding Service Level Agreements Identified and Regulated □

Identify the current vendors for your organization. What level of access do they have?

Change Management Policy □

Is a plan and policy in place for executing major changes in IT infrastructure or vendors?

System Monitoring Procedure, Company Security Software □

Are procedures currently in place which ensure active system monitoring?

Is there currently any security monitoring software in use on your network?

Backup and Recovery □

Are regular backups performed of all critical data and in what interval?

Is Restoration of data files periodically tested to verify backup integrity?

Is at least one copy of essential data stored in a secure, off-site location?

Are backup requirements periodically reviewed?

IT Staff □

Are staff members acquinted with the identities of authorized IT specialists?

Is there more than one IT specialist knowledgable in the essential structure and functionality of your network?

Operational Security Total Score □

Physical Security

Building Access □

Is the building secured by lock and alarm with restricted access?

Private or Shared Physical Network □

Is the ethernet cabling, firewall and outside Internet connectivity shared with one or more other businesses?

Tape or Other Backup Media Access □

Is physical access to backup media regulated?

Operating System and Application Installable Media Location and Access □

Do you know the location of installation discs and media?

Is the media stored in a secure location?

Server Room Environment □

Is the server room a stable and climate controlled environment?

Server Room Access □

Is server room access restricted to a select few authorized individuals?

Critical Systems Secured □

Are user and server terminals themselves secured to prevent unauthorized access?

Physical Security Total Score □

IT Security Risk Assesment

Assign each area a risk rating from 0 to 10, 10 being a perfect score in that area

Network Security

ISP Router Configuration and Access □

Who is your provider? What is the age of the router(s) and what is their replacement policy?

Firewall(s) Analysis □

Do configuration backups exist? Does documentation exist?
Are you confident that your firewall(s) is/are configured properly?
What is the age of the appliance(s) and firmware version? Are admin passwords non-standard?

Traffic Analysis □

Is incoming and outgoing network traffic being monitored and logged?

DMZ Analysis □

Is the network DMZ sufficiently secured and separated from the rest of the network?

Remote Connectivity Security □

Are SSL Security Certificates in use? Does communication occur on non-standard ports when possible? Are remote access policies in place? Are VPN configurations secure and logged? Is the use of security software mandated on outside terminals which connect via VPN?

Operating System Security □

Have all Service Packs been applied? Are updates and patches current?

Wireless Services □

Are wireless communications secure? What encryption protocals are in use?

Network Security Total Score □

Domain Security

Auditing □

Has the domain had security auditing software such as Belarc run on it recently?
Is auditing enabled to monitor file operations and logins?

Event log monitoring □

Are event logs regularily monitored for errors or concerns?

Active Directory and Forest Analysis

Does the Organizational Unit design in Active Directory make sense □
with regards to organizational needs?

Domain Administrator Password Complexity □

Has the Domain Admin password ever been run through a cracking program to check its security? Is there a possibility anyone outside of the organization may know it? How often is it changed?

Password Policy □

Have history, minimum length, complexity and minimum age requirements been configured?

Domain Trusts □

Is filtering and authorization properly configured?

Security Groups and User Accounts □

Are administrative, general use and guest account rights all assigned to the appropriate users?
Are policies for creation, deletion and disabling user accounts in place?

Domain Security Total Score □

IT Security Risk Assesment

Assign each area a risk rating from 0 to 10, 10 being a perfect score in that area

Domain Analysis

Server Auditing □

Are the production server purposes and the services running on them mapped?
Does a baseline and documentation for each server type exist?

IT Assets Auditing □

Does a comprehensive IT inventory exist of all computer equipment, software and critical files?

Windows Client Analysis □

Are user PCs secure? Is there standardization of user PCs? Are all patches and updates current?

Windows Updates and Patches □

What method is used to apply Microsoft updates?
Have third party applications been checked for patches and are they current?
Is MS Office current with updates?

Group Policy □

Has a Resultant Set of Policy report been run and evaluated? Is the end result satisfactory?

Network Shares □

Is network share security appropriately assigned? Are shares accounted for and make sense?

Documented Security Hardening Performed □

Applies to domain controllers, infrastructure servers, file servers, production servers, mail servers, print servers, IIS servers and miscellaneous servers.

Domain Analysis Total Score □

Security and Business Concerns

Anti Virus □

Is the current antivirus solution in place both up to date and sufficient?
Is staff aware they are only to open attachments they expect?
Do users know what to do if they become infected with a virus?

Loss of Remote Connectivity Devices (Laptops, PDAs, Connected Home PCs, etc.,) □

Have policies been outlined regarding what data is acceptable to store on remote devices?
Are any special tracking, theft deterrant, recovery, or data protection measures in place?
Has an assessment been done regarding potential impact to the company of losing one of these devices?

Disaster Recovery □

Does a written continuity plan exist in the event of a major disaster?
Is there an organization downtime estimate in place for the impact of a disaster recovery?
What level of redundancy exists in the system to absorb server or other IT failures?

Licensing □

Have all copies of your software been properly licensed and registered?
Is there documentation available to reflect this?

Active Aggressive Security Vulnerability Testing □

Has an agency working alongside your company ever attempted a controlled attack on your network from the outside? Were the results used to patch any vulnerabilities?

Security and Business Concerns Total Score □

Overall Security Score (maximum = 400) □

IT Security Risk Assesment

Assign each area a risk rating from 0 to 10, 10 being a perfect score in that area

Overall Risk Assessment:

Improvement Recommendations: