SECURITY AUDIT , MONITORING AND LEGAL ASPECTS

ITSM SESSION 10

SESSION OVERVIEW

SECURITY AUDIT

SECURITY MONITORING

ISO 2700
INFORMATION SECURITY COMPLIANCE

THE INFORMATION TECHNOLOGY ACT, 2000

SUMMARY

SECURITY AUDIT

WHAT IS AN IT SECURITY AUDIT?

- A security audit is the high-level description of the many ways organizations can test and assess their overall security posture, including cybersecurity.
- You might employ more than one type of security audit to achieve your desired results and meet your business objectives.


SECURITY AUDIT BENEFITS
• Verify that your current security strategy is adequate or not
• Check that your security training efforts are working
• Uncover any extraneous hardware and software
• Reduce cost by nixing the use of unnecessary resources
• Uncover flaws introduced by new technology or processes
• Prove the organization is compliant with regulations

AUDIT WORKFLOW

1. Define Assessment Criteria

- [ ] Determine the overall goals to be addressed in the audit
- [ ] Break those objectives down to departmental priorities
- [ ] Agree on how the audit will be performed and tracked

2. Prepare the Security Audit

- [ ] Prioritize your success criteria and business objectives
- [ ] Select the required tools and methodologies to meet goals
- [ ] Find or create a method to gather the correct data

3. Conduct the Security Audit

- [ ] Take care to provide appropriate documentation
- [ ] Monitor audit progress and data points for accuracy
- [ ] Use previous audits and new info to deep dive into findings

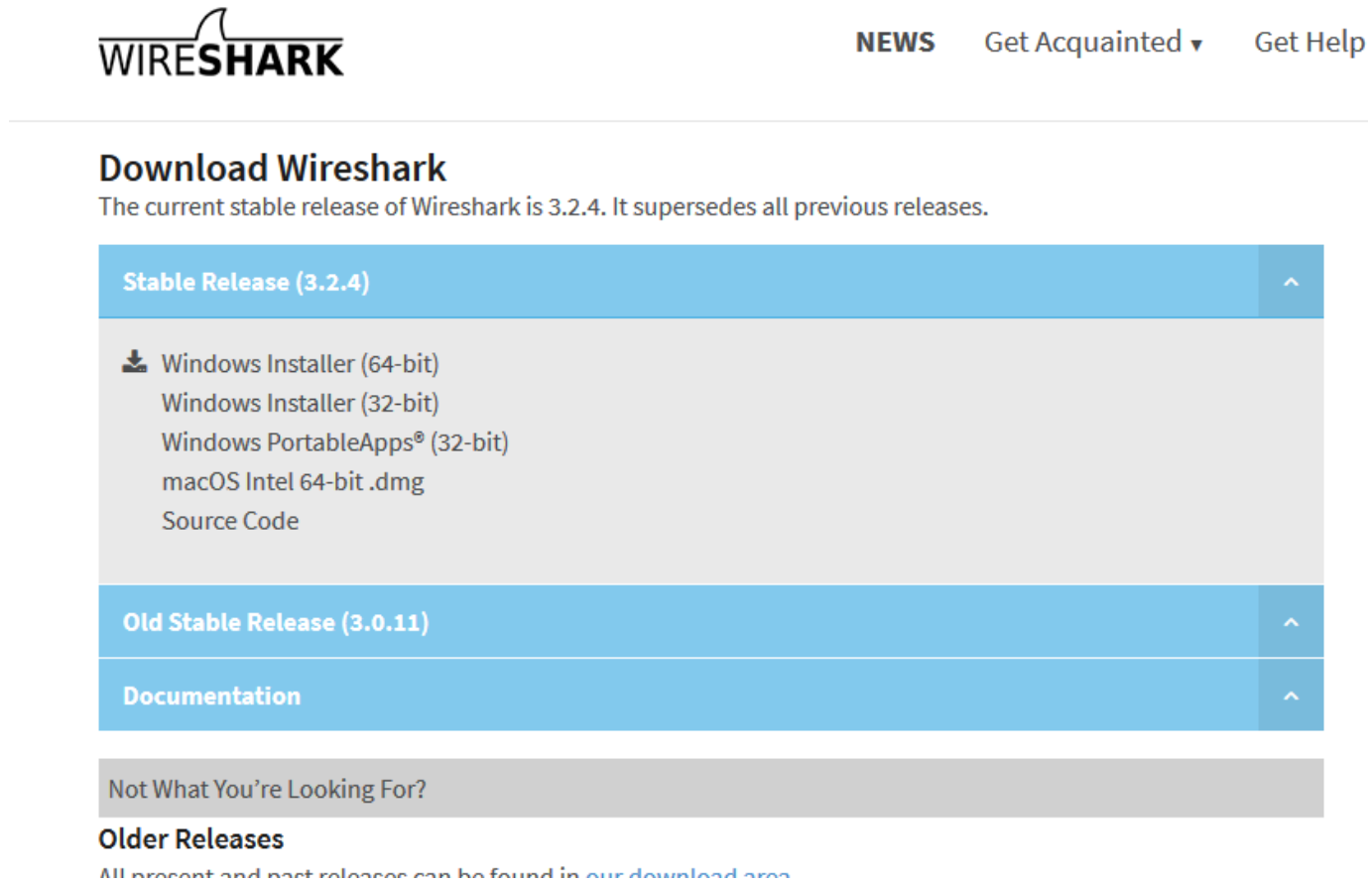
4. Complete and Share the Results

- [ ] Share results with all previously-determined parties
- [ ] Create a list of action items based on the audit findings
- [ ] Prioritize fixes to remediate the security items discovered

WHAT TO LOOK FOR IN AN IT AUDIT

- Insufficient password complexity
- Over permissive ACLs on folders
- Inconsistent ACLs on folders
- Non-existent or insufficient file activity auditing
- Non-existent or insufficient review of auditing data
- Correct security software and security configurations on all systems
- Only compliant software installed on systems
- Data retention policies followed
- Disaster recovery plans updated and tested
- Incident response plans updated and tested
- Sensitive data stored and protected correctly with encryption
- Change management procedures followed

SECURITY MONITORING



MONITORING TOOL: WIRESHARK

HTTPS://WWW.WIRESHARK.ORG/DOWNLOAD.HTML

ISO 2700

INFORMATION SECURITY COMPLIANCE

ISO 27000 Series	
ISO27001	ISMS Requirements
ISO27002	ISMS controls
ISO27003	ISMS implementation guidelines
ISO27004	ISMS Measurements
ISO27005	Risk management
ISO27006	Guidelines for ISO 27000 accreditation bodies

INFORMATION SECURITY COMPLIANCE: ISO 27000

SECTIONS OF ISO 27000

Risk assessment

- a quantitative or qualitative approach to determining the risks to organizational assets. The degree of risk is based on the impact to the asset and the likelihood of occurrence.

Security policy

- formal statements defining the organization's security expectations.

Asset management

- inventory and classification of information assets.

Human resources security

- security aspects for employees joining, moving within or for those leaving an organization.

Physical and environmental security

- physical/tangible systems used to protect systems and data such as alarm systems, guards, office layout, locked doors, keypads, cameras, etc..

Communications and operations management

- management of technical security controls in systems and networks.

Access control

- restriction of access rights to networks, systems, applications, functions and data; maintaining the confidentiality of access credentials and the integrity of access control systems.

Information systems acquisition, development and maintenance

- building security into applications when they are designed or purchased.

Information security incident management

- planning and responding appropriately to information security breaches.

Business continuity management

- protecting, maintaining and recovering business-critical processes and systems when they become unavailable.

ACHIEVING ISO 27001 CERTIFICATION SHOWS THAT A BUSINESS HAS:

Protected information from getting into unauthorised hands

Ensured information is accurate and can only be modified by authorised users

Assessed the risks and mitigated the impact of a breach

Been independently assessed to an international standard based on industry best practices

BENEFITS

- Increased reliability and security of systems and information
- Improved customer and business partner confidence
- Increased business resilience
- Alignment with customer requirements
- Improved management processes and integration with corporate risk strategies

THE INFORMATION TECHNOLOGY ACT, 2000

SECTION 65 TAMPERING WITH COMPUTER SOURCE DOCUMENTS

- If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.
- Imprisonment up to three years, or/and with fine up to ₹200,000

SECTION 66 HACKING WITH COMPUTER SYSTEM

- If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.
- Imprisonment up to three years, or/and with fine up to ₹500,000

SECTION 66A PUBLISHING OFFENSIVE, FALSE OR THREATENING INFORMATION

- Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine.
- Imprisonment up to three years, with fine.

SECTION 66B RECEIVING STOLEN COMPUTER OR COMMUNICATION DEVICE

- A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.
- Imprisonment up to three years, or/and with fine up to ₹100,000

SECTION 66C USING PASSWORD OF ANOTHER PERSON

- A person fradulently uses the password, digital signature or other unique identification of another person.
- Imprisonment up to three years, or/and with fine up to ₹100,000

SECTION 66D CHEATING USING COMPUTER RESOURCE

- If a person cheats someone using a computer resource or communication.
- Imprisonment up to three years, or/and with fine up to ₹100,000

SECTION 66E PUBLISHING PRIVATE IMAGES OF OTHERS

- If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.
- Imprisonment up to three years, or/and with fine up to ₹200,000

SECTION 66F ACTS OF CYBERTERRORISM

- If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.
- Imprisonment up to life.

SECTION 67 PUBLISHING INFORMATION WHICH IS OBSCENE IN ELECTRONIC FORM.

- If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.
- Imprisonment up to five years, or/and with fine up to ₹1,000,000

SECTION 67A PUBLISHING IMAGES CONTAINING SEXUAL ACTS

- If a person publishes or transmits images containing a sexual explicit act or conduct.
- Imprisonment up to seven years, or/and with fine up to ₹1,000,000

SECTION 67B PUBLISHING CHILD PORN OR PREDATING CHILDREN ONLINE

- If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child thus defined as anyone under 18. Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction.
- Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.

SECTION 67C FAILURE TO MAINTAIN RECORDS

- Persons deemed as intermediatary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.
- Imprisonment up to three years, or/and with fine.

SECTION 68 FAILURE/REFUSAL TO COMPLY WITH ORDERS

- The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.
- Imprisonment up to three years, or/and with fine up to ₹200,000

SECTION 69 FAILURE/REFUSAL TO DECRYPT DATA

- If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.
- Imprisonment up to seven years and possible fine.

SECTION 70 SECURING ACCESS OR ATTEMPTING TO SECURE ACCESS TO A PROTECTED SYSTEM

- The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.
- The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.

- Imprisonment up to ten years, or/and with fine.

SECTION 71 MISREPRESENTATION

- If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.
- Imprisonment up to three years, or/and with fine up to ₹100,000

SUMMARY

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to **www.ncsc.gov.uk** **@ncsc**

Stay protected

Firewalls

Surround your network with a top-line defense that detects and stops threats fast without slowing you down.

Endpoint and VPN security

No matter where users connect to your network, protect yourself against advanced threats at every endpoint.

Cloud security

Work anywhere. Protect your employees against threats no matter where they access the Internet.

Password security

Easily secure access to Virtual Private Network (VPN), email, and any app that employees value, using multi-factor authentication.

THANK YOU