SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit IV- SECURITY ELEMENTS

TOPIC: Security monitoring and Auditing

Security Monitoring and Auditing

- A **security Monitoring** and audit is a **systematic evaluation** of the security of a company's information system by measuring how well it conforms to an established set of criteria.
- A thorough audit typically assesses the security of **the system's physical configuration** and **environment, software, information handling processes and user practices.**
- Security audits are often used to determine compliance with regulations such as the **Health Insurance Portability and Accountability Act**, the **Sarbanes-Oxley Act** and the **California Security Breach Information Act** that specify how organizations must deal with information.

These audits are **one of three main types of security diagnostics**, **along with vulnerability assessments and penetration testing**.

- **Security audits measure** an information system's performance against a list of criteria.
- **A vulnerability assessment** is a comprehensive study of an information system, seeking potential security weaknesses.
- **Penetration testing** is a covert approach in which a security expert tests to see if a system can withstand a specific attack. Each approach has inherent strengths and using two or more in conjunction may be the most effective approach.

Why are security audits important?

There are several reasons to do a security audit. They include these six goals:

- Identify security problems and gaps, as well as system weaknesses.
- Establish a security baseline that future audits can be compared with.
- Comply with internal organization security policies.
- Comply with external regulatory requirements.
- Determine if security training is adequate.
- Identify unnecessary resources.

Types of security audits

Security audits come in two forms, internal and external audits,

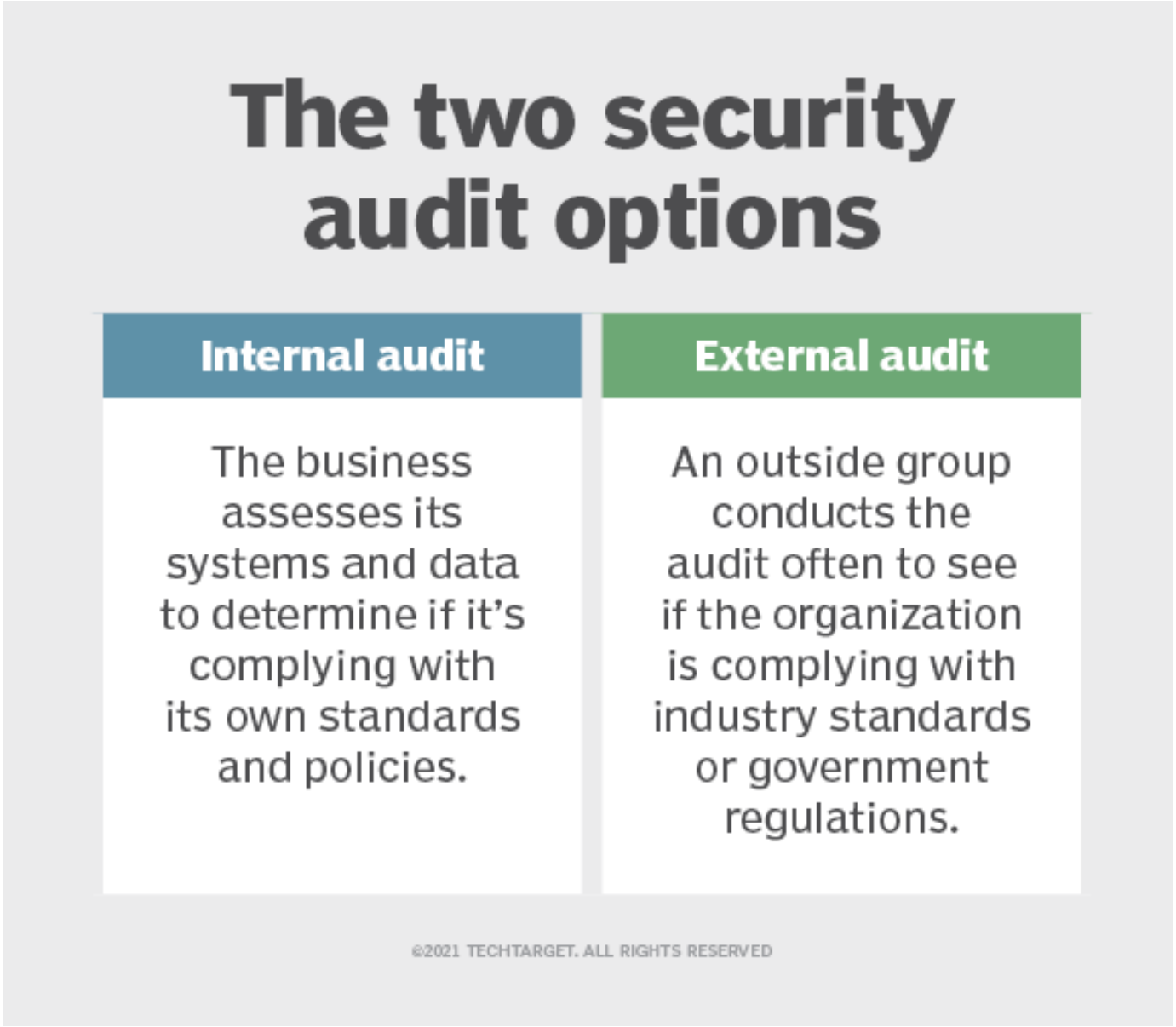
that involve the following procedures:

Internal audits:

In these audits, a **business uses its own resources and internal audit department**. Internal audits are used when an **organization wants to validate business systems for policy and procedure compliance.**

External audits:

With these audits, an **outside organization is brought in to conduct an audit**. External audits are also conducted when an organization needs to confirm it is conforming to industry standards or government regulations.


The two security audit options
Internal audit
The business assesses its systems and data to determine if it's complying with its own standards and policies.
External audit
An outside group conducts the audit often to see if the organization is complying with industry standards or government regulations.
©2021 TECHTARGET. ALL RIGHTS RESERVED

What systems does an audit cover?

During a security audit, each system an organization uses may be examined for vulnerabilities in the following areas:

- **Network vulnerabilities**
- **Security controls**
- **Encryption**
- **Software systems**
- **Architecture management capabilities**
- **Telecommunications controls**
- **Systems development audit**
- **information processing**

Steps involved in a security audit

These five steps are generally part of a security audit:

- **Agree on goals:** Include all stakeholders in discussions of what should be achieved with the audit.
- **Define the scope of the audit:** List all assets to be audited, including computer equipment, internal documentation and processed data.
- **Conduct the audit and identify threats:** List potential threats related to each Threats can include the loss of data, equipment or records through natural disasters, malware or unauthorized users.
- **Evaluate security and risks:** Assess the risk of each of the identified threats happening, and how well the organization can defend against them.
- **Determine the needed controls:** Identify what security measures must be implemented or improved to minimize risks.

Any Query????

Thank you……