MODULE 6E: AUDITING NEW TECHNOLOGIES

BACKGROUND

- Fortunately, when you break it down, the same basic concepts apply no matter what you're auditing. Accounts need to be created and managed. You need to have some method for authenticating those accounts, and you need to manage what those accounts are authorized to do. Systems need to be configured securely and monitored. Methods for connecting to the technology need to be secured and managed.

NEW/OTHER TECHNOLOGY AUDITING ESSENTIALS

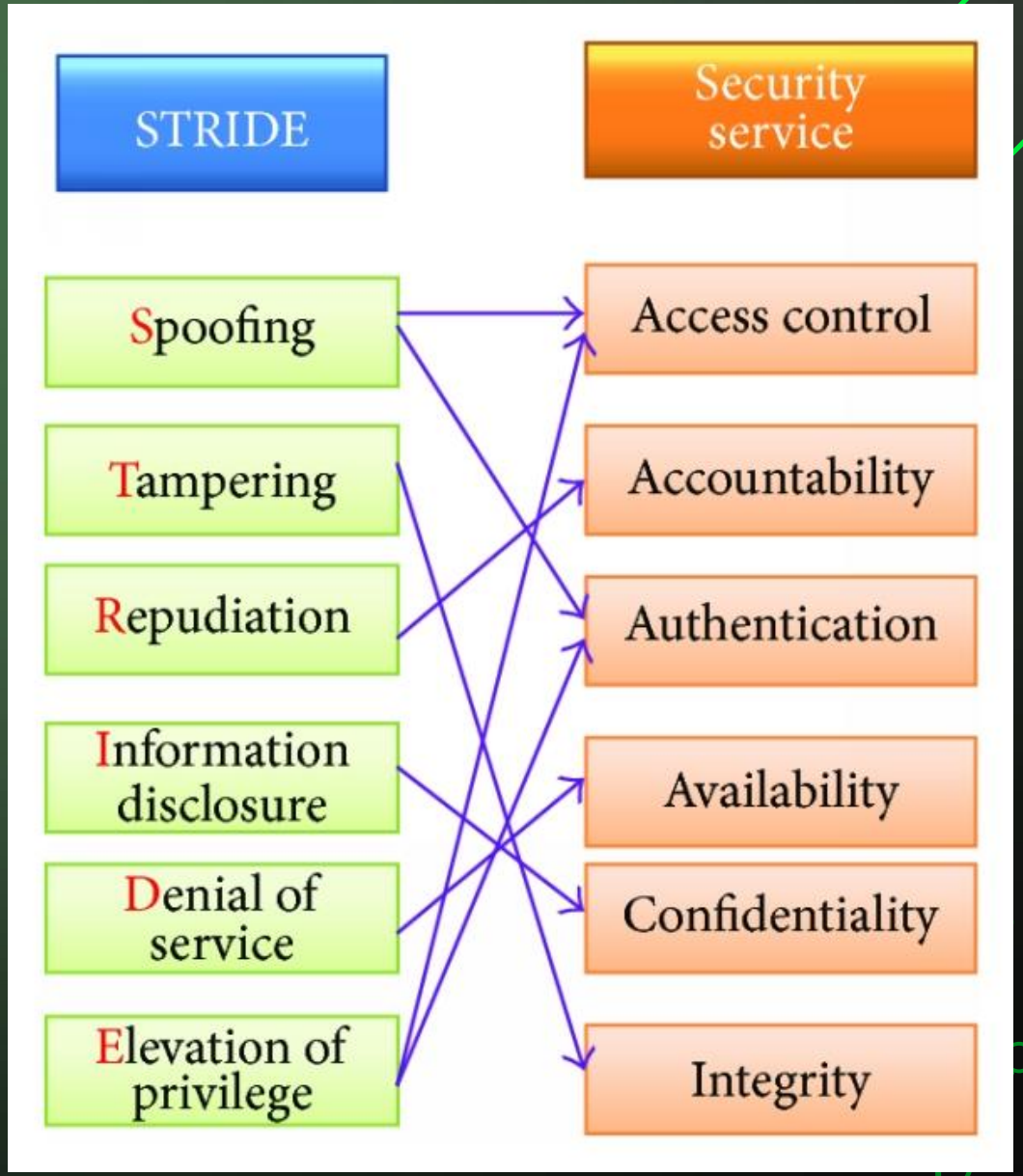
- As you begin exploring new technologies, some frameworks and best practices can assist you in structuring your thoughts.
- Generalized frameworks are useful in meetings when you've been put on the spot to come up with questions and possible risks associated with an application, technology, or project. You might even find yourself walking into a meeting, taking out a blank sheet of paper, and writing "PPTM," "STRIDE," and "PDIO" (as explained in the following sections) at the top before the meeting starts. Then, as you discuss the system or project under review, you can ask questions and take notes regarding how each element of each framework is being addressed. At the end of the meeting, if you find "blanks" by any of the framework elements, it's possible that you've discovered a gap in the controls.

PPTM

- People, Processes, Tools, and Measures (PPTM) is a great brainstorming framework for examining a system from the macro level.
- PPTM helps you come up with your own steps quickly and efficiently as they apply to your unique situation.

STRIDE

- The STRIDE acronym stands for the following: Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. STRIDE is a methodology used for identifying known threats. It is an example of a simplified threat-risk model that is easy to remember and apply. When assessing a system, you can use the acronym to develop steps that address how each of the following risks is mitigated.



https://www.researchgate.net/figure/Relation-between-STRIDE-security-attributes-and-security-service-for-HTN_fig6_283205029

PDIO

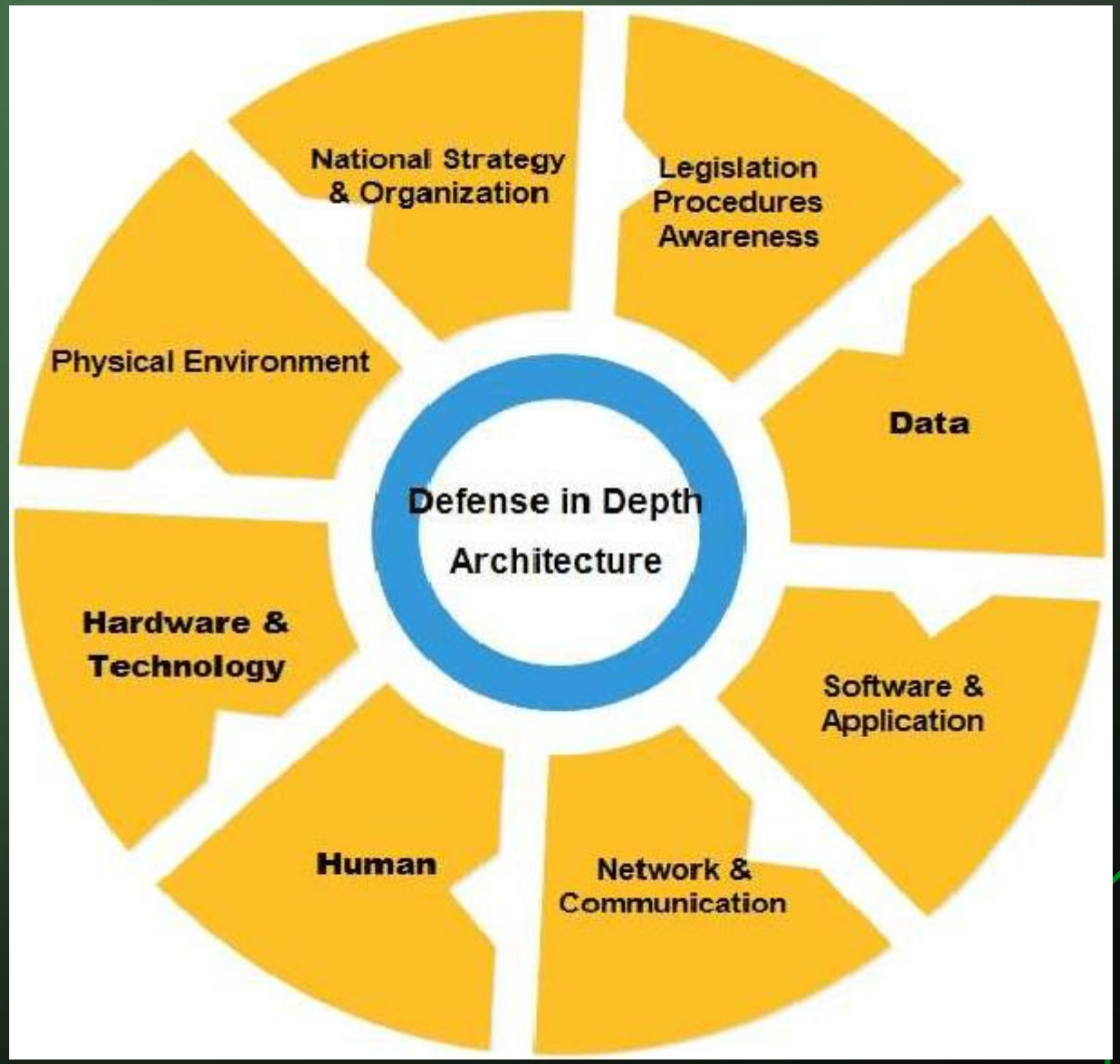
- PDIO comes from Cisco Systems and stands for Planning, Design, Implementation, and Operations. Sometimes you need to consider the potential challenges at each stage of a project. You might find this framework useful as you look at a new system and think ahead to the upcoming challenges. A problem might occur, for example, if system administrators are tossing around ideas in a planning or design session for a network solution and the senior networking engineer isn't in the room. If you, as an auditor, are asked to look at the implementation of a new solution, you should immediately ask questions about the ongoing operations of the solution.

COMMON BEST PRACTICIES

- As an auditor, if an organization is seeking to implement any new technologies, it's always best to remind them of some common security best practices.
  - These best practices also apply to existing technologies. Security is a mindset that should be undertaken by the company in their day to day activities, as well as their future plans.
  - Auditors can help to remind the company and it's employees (even security professionals) of best practices.

DEFENSE IN DEPTH

- Layered approaches provide more security over the long term than one complicated mass of security architecture.
- This approach significantly lowers the overall risk of compromise to the system, because you quickly eliminate access to services, ports, and protocols that otherwise would be accessible to compromise.



USE A POSITIVE SECURITY MODEL

- Positive (whitelist) security models allow only what is on the list, excluding everything else by default. However, negative (blacklist) security models allow everything by default, eliminating only the items you know are bad. This is the challenge for antivirus programs, which you must update constantly to keep up with the number of new possible attacks (viruses) that could affect your system. The problem with this model, if you are forced to use it, is that you absolutely must keep the model updated. Even with the model updated, however, a vulnerability could exist that you don't know about, and your attack surface is much larger than if you used a positive security model. The preferred practice is to deny by default and allow only those things that you consciously permit.

FAIL SAFELY

- When a system fails, it can be dealt with in three ways: allow, block, or error. In general, system errors should fail in the same manner as a disallow (block) operation as viewed from the end user. This is important, because it means the end user doesn't have additional information to use that may help him or her compromise the system. Log what you want and keep any messages that you want elsewhere, but don't give the user additional information he or she might use to compromise your system.

RUN WITH LEAST PRIVILEGE

- The principle of least privilege mandates that accounts have the least amount of privilege possible to perform their activity. This encompasses user rights and resource permissions such as CPU limits, memory capacity, network bandwidth, and file system permissions.

AVOID SECURITY BY OBSCURITY

KEEP SECURITY SIMPLE

- Simple security mechanisms are easy to verify and easy to implement correctly. Cryptographer Bruce Schneier is famous for suggesting that the quickest method to break a cryptographic algorithm is to go around it. Avoid overly complex security mechanisms, if possible. Developers should avoid the use of double negatives and complex architectures when a simple approach would be faster and easier. Don't confuse complexity with layers. Layers are good; complexity isn't.

NEVER TRUST EXTERNAL INFRASTRUCTURE AND SERVICES

- Many organizations use the processing capabilities of third-party partners that more than likely have differing security policies and postures than yours. It is unlikely that you can fully control any external third party, be they home users or major suppliers or partners. Therefore, implicitly trusting externally run systems is dangerous.

ESTABLISH SECURE DEFAULTS

- Your systems should arrive to you or be presented to the users with the most secure default settings possible that still allow business to function. This may require training end users or communications, but the end result is a significantly reduced attack surface, especially when a system is pushed out across a large population.

SECURITY MINDSET

- User Awareness Training is one thing – it teaches individuals to recognize common attacks and how to avoid them.
- Security Mindset Education - Teaches employees to think about their everyday actions through a security lens.
  - **Should be the focus!**