Contribute to Personnel Security Policies

Humans are the weakest element in any security solution. No matter what physical or logical controls are deployed, humans can discover ways to avoid them, circumvent or subvert them, or disable them.

Important elements in constructing job descriptions that are in line with organizational processes include separation of duties, job responsibilities, and job rotation.

**Separation of Duties** Separation of duties is the security concept in which critical, significant, and sensitive work tasks are divided among several individual administrators or high-level operators.

**Think of separation of duties as the application of the principle of least privilege to administrators. Separation of duties is also a protection against collusion***,*

**Job Responsibilities** Job responsibilities are the specific work tasks an employee is required to perform on a regular basis

**Job Rotation** Job rotation, or rotating employees among multiple job positions, is simply a means by which an organization improves its overall security

Cross training is also important.

**When several people work together to perpetrate a crime, it’s called collusion.**

**Employment Candidate Screening.**

**Employment Agreements and Policies(NDA)**

The NDA has a common companion contract known as the noncompete agreement (NCA) . **The noncompete agreement attempts to prevent an employee with special knowledge of secrets from one organization** from working in a competing organization in order to prevent that second organization from benefiting from the worker’s special knowledge of secrets**. NCAs are also used to prevent workers from jumping from one company to another competing company just because** of salary increases or other incentives. Often

NCAs have a time limit, such as six months, one year, or even three years. The goal is to allow the original company to maintain its competitive edge by keeping its human resources working for its benefit rather than against it.

**Employment Termination Processes**

When possible, an exit interview should be performed. However, this typically depends on the mental state of the employee upon release and numerous other factors. If an exit interview is unfeasible immediately upon termination, it should be conducted as soon as possible.

In most cases, you should disable or remove an employee’s system access at the same time or just before they are notified of being terminated.

The following issues are commonly addressed in SLAs:

■ System uptime (as a percentage of overall operating time)

■ Maximum consecutive downtime (in seconds/minutes/and so on)

■ Peak load

■ Average load

■ Responsibility for diagnostics

■ Failover time (if redundancy is in place)

**Compliance**

Compliance is the act of conforming to or adhering to rules, policies, regulations, standards, or requirements.

Compliance is an important concern to security governance.

**Privacy**

When addressing privacy in the realm of IT, there is usually a balancing act between individual rights and the rights or activities of an organization.

There are many legislative and regulatory compliance issues in regard to privacy. Many US regulations—such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act of 2002 (SOX), and the Gramm-Leach-Bliley Act—as well as the EU’s Directive 95/46/EC (aka the Data Protection Directive) and the contractual requirement Payment Card Industry Data Security Standard (PCI DSS)—include privacy requirements. It is important to understand all government regulations that your organization is required to adhere to and ensure compliance, especially in the areas of privacy protection.

Security Governance

Third-party governance is the system of oversight that may be mandated by law, regulation, industry standards, contractual obligation, or licensing requirements. The actual method of governance may vary, but it generally involves an outside investigator or auditor. These auditors might be designated by a governing body or might be consultants hired by the target organization.

**Documentation review is the process of reading the exchanged materials and verifying them against standards and** expectations. The documentation review is typically performed before any on-site inspection takes place. If the exchanged documentation is sufficient and meets expectations (or at least requirements), then an on-site review will be able to focus on compliance with the stated documentation. However, if the documentation is incomplete, inaccurate, or otherwise insufficient, the on-site review is postponed until the documentation can be updated and corrected. This step is important because if the documentation is not in compliance, chances are the location will not be in compliance either

In many situations, especially related to government or military agencies or contractors, failing to provide sufficient documentation to meet requirements of third-party governance **can result in a loss of or a voiding of authorization to operate (ATO). Complete and sufficient documentation can often maintain existing ATO or provide a temporary ATO (TATO). However, once an ATO is lost or revoked, a complete documentation review and on-site review showing full compliance is usually necessary to reestablish the ATO.**

Understand and Apply Risk Management Concepts

**The possibility that something could happen to damage, destroy, or disclose data or other resources is known as risk. The process by which the goals of risk management are achieved is known as risk analysis.**

**Risk Frameworks**

**A risk framework is a guideline or recipe for how risk is to be assessed, resolved, and monitored. The primary example of a risk framework referenced by the CISSP exam is that defined by NIST in Special Publication 800-37.**

**…**