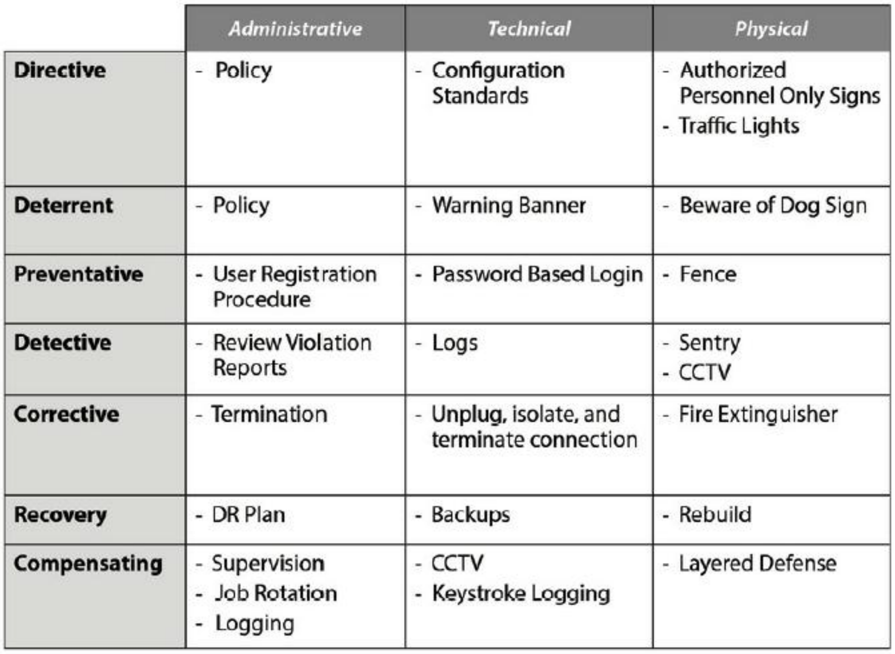
Personnel Security and Risk Management Concepts

1. Humans are the weakest element in any security solution.
2. The job description should define the type and extent of access the positionrequires on the secured network. Once these issues have been resolved, assigning a security classification to the job description is fairly standard.
3. Job descriptions are important to the design and support of a security solution.
4. Separation of duties is also a protection against collusion, which is the occurrence of negative activity undertaken by two or more people, often for the purposes of fraud, theft, or espionage.
5. Job rotation, or rotating employees among multiple job positions, is simply a means by which an organization improves its overall security. Job rotation serves two functions.
6. Job rotation also provides a form of peer auditing andprotects against collusion.
7. Employment candidate screening for a specific position is based on the sensitivity andclassification defined by the job description.
8. An NDA is used to protect the confidential information within an organization from being disclosed by a former employee.
9. When a person signs an NDA, they agree not to disclose any information that is defined as confidential to anyoneoutside the organization. Violations of an NDA are often met with strict penalties
10. The primary purpose of the exit interview is to review the liabilities an restrictions placed on the former employee based on the employment agreement, nondisclosure agreement, and any other security-related documentation.
11. Vendor, Consultant, and Contractor Controls through SLA
12. SLAs and vendor, consultant, and contractor controls are an important part of risk reduction and risk avoidance.
13. Compliance is an important concern to security governance.
14. Security governance is the collection of practices related to supporting, defining, anddirecting the security efforts of an organization.
15. Third-party governance focuses on verifying compliance with stated security objectives, requirements, regulations, and contractual obligations.
16. Security is aimed at preventing loss or disclosure of data while sustaining authorized access.
17. The primary goal of risk management is to reduce risk to an acceptable level
18. An asset is anything within an environment that should be protected
19. Asset Valuation Asset valuation is a dollar value assigned to an asset based on actual cost and nonmonetary expenses.
20. Threats Any potential occurrence that may cause an undesirable or unwanted outcome for an organization or for a specific asset is a threat
21. Vulnerability The weakness in an asset or the absence or the weakness of a safeguardor countermeasure is a vulnerability.
22. risk = threat * vulnerability
23. Threat Exploit > Vulnerabilities =>which result in Exposure =>which is Risk => and it is mitigate by safeguard which protect asset

24. Risk management/analysis is primarily an exercise for upper management.
25. There are two risk assessment methodologies: quantitative and qualitative.
26. Quantitative risk analysis assigns real dollar figures to the loss of an asset.
27. Qualitativerisk analysis assigns subjective and intangible values to the loss of an asset.
28. SLE = asset value (AV) * exposure factor (EF)
29. ALE = SLE * ARO
30. There are four possible responses to risk:
    a. Reduce or mitigate
    b. Assign or transfer
    c. Accept
    d. Reject or ignore
31. Selecting a countermeasure within the realm of risk management relies heavily on thecost/benefit analysis results.
32. The cost of the countermeasure should be less than the value of the asset.
33. The cost of the countermeasure should be less than the benefit of thecountermeasure.
34. Keep in mind that security should be designed to support and enable business tasks and functions. Thus countermeasures and safeguards need to be evaluated in the context of a business task.
35.



	Administrative	*Technical*	*Physical*
Directive	- Policy	- Configuration Standards	- Authorized Personnel Only Signs - Traffic Lights
Deterrent	- Policy	- Warning Banner	- Beware of Dog Sign
Preventative	- User Registration Procedure	- Password Based Login	- Fence
Detective	- Review Violation Reports	- Logs	- Sentry - CCTV
Corrective	- Termination	- Unplug, isolate, and terminate connection	- Fire Extinguisher
Recovery	- DR Plan	- Backups	- Rebuild
Compensating	- Supervision - Job Rotation - Logging	- CCTV - Keystroke Logging	- Layered Defense

36. A primary goal of risk analysis is to ensure that only cost-effective safeguards are deployed.
37. The goal of asset valuation is to assign to an asset a specific dollar value that encompasses tangible costs as well as intangible ones
38. Risk analysis is performed to provide upper management with the details necessary to decide which risks should be mitigated, which should be transferred, and which should be accepted.
39. Threats and vulnerabilities constantly change, and the risk assessment needs to be redone periodically in order to support continuous improvement
40. The goal of creating awareness is to bring security to the forefront and make it a recognized entity for users. Awareness

41. It is the responsibility of the security governance team to establish security rules as well as provide training and education to further the implementation of those rules.
42. A termination policy is needed to protect an organization and its existing employees

43. The process of identifying, evaluating, and preventing or reducing risks is known as riskmanagement.

44. Risk analysis is the process by which risk management is achieved and includes analyzing an environment for risks, evaluating each risk as to its likelihood of occurring and the cost of the resulting damage, assessing the cost of various countermeasures for each risk, and creating a cost/benefit report for safeguards to present to upper management