12.3.4 Third-Party Integration Facts

In the modern business world, it is very common for one organization to work directly with another in either a vendor or partner relationship. These relationships frequently requires that each party's information systems connect and integrate with each other. This integration potentially exposes each network to a heightened degree of risk.

Before entering into such a relationship, take steps to ensure that the integration process maintains the security of each party's network. Pay careful attention to both the onboarding phase, when the relationship is initiated, and the off-boarding phase, when the relationship is terminated.

Integration Relationship Considerations

The following table lists integration issues you should consider for each phase of the relationship.

Relationship Phase	Considerations

	During the on-boarding phase of a relationship, consider the following issues and formulate a plan to address them:
	▪ Compare your organization's security policies and infrastructure against each partner organization's policies and infrastructure. Then answer the following questions.
	  ▪ Are the security policies for each organization similar?
	  ▪ Do both organizations have similar incident response procedures?
	  ▪ Are the each party's security controls similar?
	  ▪ Do both organizations have similar audit policies?
	  ▪ Are the security postures of each party compatible enough to work together, or will the integration expose vulnerabilities in one or more parties?
	  ▪ What are the risks associated with entering into this relationship?
	  If significant differences in the two policies are found, it might be necessary to resolve them or reconsider the relationship altogether.
	▪ Identify how data ownership will be determined. Will ownership be determined simply by the storage location, or will ownership be determined by patent, trademark, copyright, or contract law?
	▪ Identify who will be responsible for protecting data. Who will be responsible for performing data backups? Will ou use redundancy to ensure high availability?
	▪ If the data involved in the relationship contains personally identifying information, identify how you will protect privacy.
	▪ Identify how you will share data. In most relationships, there is only a limited subset of data that must be shared between parties. The rest of each organization's data must remain protected. How will you prevent unauthorized data? If unauthorized data sharing occurs, how will you detect it?

Onboarding	Prior to entering into a third-party agreement, it is critical that all aspects of the relationship are agreed upon in writing. To accomplish this, most organizations will utilize an *Interoperability Agreement* (IA). There are several key documents that may be included within an IA that you should be familiar with: ▪ A *Master Service Agreement* (MSA) defines terms that will govern future agreements between two parties. The purpose of this document is to allow the parties to quickly negotiate future agreements without having to repetitively renegotiate the same terms over and over. ▪ A *Service Level Agreement* (SLA) specifies exactly which services will be performed by the third party and what level of performance is guaranteed. An SLA may also define how disputes will be managed, provide warranties, outline disaster recovery procedures, and specify when the agreement will be terminated. ▪ A *Blanket Purchase Order (*BPO) is an agreement with a third-party vendor to provide services on an ongoing basis. BPOs are typically negotiated to take advantage of a preset discounted pricing structure. ▪ A *Memorandum of Understanding* (MOU) is a very important document that provides a brief summary of which party in the relationship is responsible for performing specific tasks. In essence, the MOU specifies who is going to do what and when each party will accomplish their tasks. ▪ An *Interconnection Security Agreement* (ISA) documents how the information systems of each party in the relationship will be connected and how they will share data. ▪ A *Statement of Work* (SOW) is a document used in the field of project management. An SOW defines project-specific activities, deliverables, and timelines for a vendor providing services to the client. ▪ A *Nondisclosure Agreement* (NDA) is a legally enforceable contract that creates a confidential relationship between a company and an employee to protect the company's assets from being disclosed to competitors and the public. An NDA has two main functions. The first is to protect sensitive information. By signing an NDA, employees promise to not give or release information shared with them by the company. If the information is leaked, the company can claim breach of contract. The second is to outline what information is private and what is okay to share with others. The agreement serves as a document that classifies exclusive and confidential information .

Ongoing Operations	During the ongoing operations phase of the relationship, you should: ▪ Regularly verify compliance with the IA documents. ▪ Conduct periodic vulnerability assessments to verify that the network interconnections created by the relationship have not exposed or created security weaknesses. ▪ Conduct regular security audits to ensure that each party in the relationship is following the security-related aspects of the IA documents. ▪ Communicate vulnerability assessment and security audit findings with all of the parties in the relationship to maintain risk awareness.
Off-Boarding	When the relationship with the third party ends, you need to ensure that all of the doors that were opened between organizations during the onboarding phase are closed. Consider the following: ▪ Reset or disable any VPN, firewall, router, or switch configurations that allowed access to your network from the third party network. ▪ Disable any domain trust relationships that were established between the organizations. ▪ Disable any user and group accounts used by third parties to access your organization's data. ▪ Reset any passwords used by the third party to access data or applications on your network.