

Incident Response Team Basic Service Checklist

Area	Procedures	Status	Notes
User Enrollment	The process of creating, modifying, and removing user accounts and privileges on the computer systems. It also includes the definition of the authorizations, group memberships, and access profiles for users.		
Vulnerability Assessment	The process of searching for possible susceptibility for a system to be accessed in an unauthorized way or to have authorized access denied. Many commercial and free vulnerability assessment tools can help streamline this process, although these tools do require a certain amount of experience to use them effectively. There are many opinions regarding the frequency with which these assessments should be conducted, but nearly all security professionals agree that they're not done often enough.		
Penetration Testing	The process of attempting to gain unauthorized access to a computer system or facility. This focused attempt to break into a system or facility is usually conducted from the perspective of a "hostile" entity and attempts to measure how much effort must be expended to gain access. The network operations group or other entity that monitors the computer resources will typically not know ahead of time that the testing will be conducted. Therefore, the capability to detect and respond to an attack can be measured while searching for potential vulnerabilities.		
Risk Assessment	The process of rating and evaluating vulnerabilities, threats, value, and safeguards. It takes the results of a vulnerability assessment and adds in an analysis of threats, the value of the information, and the safeguards used to protect the information. Its purpose is to help make informed decisions based on the best balance between the risk that is posed to the organization's information and the benefit of protecting it. Although several different methodologies are used for this process, it can be a very valuable tool in making decisions about how much effort to protect a system is enough.		
Architectural Review	The process of evaluating the hardware, software, network, policy, and management of a system or group of systems to ensure they do what is intended, and do not do what is not intended. This service mirrors the thought that security should be part of everyone's effort—throughout the complete life cycle of information, from concept to disposal.		
User Awareness Training	The process of teaching and reinforcing knowledge of policies, procedures, and strategies while maintaining a computing environment. In terms of effectiveness, user awareness training can be one of the most valuable services that a team offers. Conversely, a lack of user awareness can represent a significant threat to any network. In this forum, users can learn effective password management, the organization's information-handling policies, procedures for sharing information, virus risks, tactics to defeat social engineering, and more.		

Advisory Notification	The process where security notifications are distributed to the constituency. Many teams keep an inventory of the computing platforms, software, network infrastructure, and services that their organization employs. As a manufacturer, software vendor, or other source of information publishes a notification that there may be a vulnerability in the product, a virus, or a security-related upgrade, the team would verify that the advisory is authentic and then forward it to the affected members of the constituency. Other teams (such as CERT CC and vendor teams) will be responsible for writing the advisory that is initially distributed.		
Research and Development	The process of creating, evaluating, testing, and integrating new products, policies, procedures, and strategies. A lab environment in which to test and discover methods of breaking into systems, techniques for securing systems, and ways to improve and implement the enforcement of company policies—and as a proving ground that enforcement can be done—can be a very valuable service to the organization.		