
Defining business objectives

Based on the assessment requirements and the endorsement of services, it is vital to define the business objectives. This will ensure that the testing output benefits a business from multiple aspects. Each of these business objectives is focused and structured according to the assessment requirements and can provide a clear view of the industry achievement. We have formatted some general business objectives that can be used to align with any penetration testing assignment. However, they can also be redesigned according to the change in requirements. This process is important and may require a pentester to observe and understand the business motives while maintaining the minimum level of standard before, during, and after the test is completed. Business objectives are the main source to bring the management and technical team together in order to support a strong proposition and an idea of securing information systems. Based on the different kinds of security assessments to be carried out, the following list of common objectives has been derived:

- Provide industry-wide visibility and acceptance by maintaining regular security checks.
- Achieve the necessary standards and compliance by assuring business integrity.
- Secure the information systems holding confidential data about the customers, employees, and other business entities.
- List the active threats and vulnerabilities found in the network infrastructure, and help to create security policies and procedures that should thwart known and unknown risks.
- Provide a smooth and robust business structure that will benefit its partners and clients.
- Retain the minimum cost for maintaining the security of an IT infrastructure. The security assessment measures the confidentiality, integrity, and availability of the business systems.
- Provide greater return on investment by eliminating any potential risks that might cost more if exploited by a malicious adversary.
- Detail the remediation procedures that can be followed by a technical team at the concerning organization to close any open doors, and thus, reduce the operational burden.
- Follow the industry best practices and best-of-breed tools and techniques to evaluate the security of the information systems according to the underlying technology.
- Recommend any possible security solutions that should be used to protect the business assets.