



IT Solutions, Inc. Security Offerings

Does your business have a disaster recovery plan in process? Have you ever thought about conducting a security assessment? Do you know what assessments are readily available? What are the differences between each assessment?

IT Solutions, Inc. is here to ease your mind on security assessments. Our team will get to know you and your business to create recommendations based upon our findings. Listed below in order of complexity are security offerings that IT Solutions, Inc. has to offer.

- **Vulnerability Assessment:** A vulnerability assessment checks networks and computes platform items for any mis-configured or un-patched issues that would allow a security breach to occur. Vulnerability assessments do not factor the probability of these items being exposed. They simply recognize that they exist. A vulnerability assessment is, normally, performed with tools, such as port scanners and penetration testing software. These are also commonly referred to as a “Security Assessment” or a “Network Security Audit.”
- **Risk Assessment:** A risk assessment is similar to a vulnerability assessment, however it entails more factors. A risk assessment concentrates on what could happen, the likelihood of it happening, and the impact it would have if it happened. IT Solutions, Inc. utilizes the following formula, Risk =Likelihood x Impact, when discussing risk assessments. In this type of assessment, IT Solutions, Inc. will take into account environmental factors such as is the client’s facility in a flood plain, do they have a history of power problems, and are they located near hazardous environments. This type of assessment also defines the client’s “Critical Assets”. These critical assets are not only equipment and data, but also include people and services.
- **Compliance Audit:** A compliance audit, sometimes referred to as a 3rd party audit, involves comparing the standards of the governing body to the reality of the client’s configuration and reports the compliance differences. Most of the data, such as requirements and checklists are readily available from the different governing bodies to do these audits.
- **Disaster Recovery/ Business Continuity Planning:** Disaster recovery has different meanings to different people. On the technical side, disaster recovery means mitigating issues by providing backup/ redundant computer platform solutions. In a broader sense, disaster recovery means working with clients to create disaster recovery planning and procedures; as well as plan for how to keep business critical systems running in the event of a disaster. This type of offering has the potential to increase the size of the project. This offering must be preceded by, or include, a Risk of Assessment. Many companies that fall under any kind of compliance body, such as HIPAA, ISO 900, FDIC, and NCUA, require that the client have a formal Disaster Recovery plan in place.
- **Incident Response:** Incident response would be needed when there is a security breach or suspected security breach. Typically, IT Solutions, Inc. engineers would be asked to find the problem, correct it, and document the damage and cause. An example would be when a client requests IT Solutions, Inc. to perform a lockdown of a domain or network. Certain procedures to protect the chain must be followed should there be a chance of custody of evidence.