

SecureTrust[™] Information Security Risk Assessment

IDENTIFY AND PRIORITIZE RISKS TO ACHIEVING YOUR GOALS

Identifying and prioritizing risks to your organizations most critical assets and determining your organizations risk tolerance are essential elements of maintaining an effective security and risk management program.

Businesses, non-profits, governments and ventures around the globe depend on information systems to conduct their operations and fulfill their duties. Information systems are a varied lot of networks, financial and personnel systems as well as telecommunication and environmental control systems. It's important to recognize these systems serve important functions, each have sensitive data and they are inherently subject to risk.

Leaders must consider risks to their interests. Management is accountable for ensuring readiness and security to maintain operations. Through a risk management process, the people in charge must consider threats from attackers and vulnerabilities in business operations that might keep them from realizing their goals. To develop operational plans and apply resources to treat risk, organizations must evaluate the combination of threats and vulnerabilities as well as the likelihood and impact of a risk event occurring. SecureTrust can augment your risk management process by conducting complete and thorough assessments and by helping build processes for your staff to perform ongoing assessments.

Risk treatment may include elimination or reduction of threat capabilities or vulnerabilities. Alternatively, risk analysis may lead to acceptance of certain risks without treatment. In any case, management is responsible for ensuring the risk management process operates to appropriately identify risks and sufficiently reduce risks to achieving key objectives. A SecureTrust Information Security Risk Assessment (ISRA) can help you manage risk and lessen the probability or effect of risks to information systems that support your mission and vision.

Fundamentals of Risk Assessment

Risk assessment is an essential element of effective risk management. Risk assessments are used to identify and prioritize risk to people, operations and assets stemming from the use of information systems.

The purpose of risk assessment is to enlighten decision makers and support risk responses by identifying relevant threats, internal and external vulnerabilities, potential impact of threats exploiting vulnerabilities and the likelihood that a risk event will occur.

A risk assessment enables decision making at multiple levels including the organization level, the specific mission or business process level and at the information system level. Managers use risk assessment to evaluate information security risks related to their mission or business function as well as funding of security programs. And, at the information system level, organizations use risk assessment to better support security control selection, implementation and control monitoring.

Risk management is an ongoing process and risk assessments should be conducted throughout the system development lifecycle, prior to system acquisition and continue throughout system development, deployment, operations and support.

The end result of a risk assessment is a determination of risk, as a function of impact and the likelihood of a risk event occurring. The SecureTrust ISRA is designed to meet the various needs of your organization and to assist in establishing risk assessment activities that may be integrated into your organizations broader risk management processes.

Risk Assessment Applicability

A SecureTrust ISRA is designed to provide assistance and guidance for conducting risk assessments and to support the overall risk management process. The intent of the SecureTrust ISRA is to provide leaders with the knowledge necessary to decide the proper course of action and respond to identified risks.

The SecureTrust ISRA engagement helps your organization prepare for the assessment, conduct the assessment, communicate results and monitor the effectiveness of risk management activities. Perhaps the most impactful objective is to monitor the risk management process on an ongoing basis with the aim of gauging whether risks have increased to unacceptable levels, beyond your decided risk tolerance, and whether an alternate plan is necessary to continue to meet your goals.

We seek to reduce the burden on your organization to utilize risk assessment standards and promote risk assessment results. SecureTrust will provide guidance to your organization by presenting the general concepts and principles of risk assessment and will assist to identify risk factors, monitor your risk management program and help you consider guidelines to address risk.

A Strategic Opportunity

For an enterprise faced with multiple compliance requirements, and changing security needs of the business, risk is both a four letter word and an opportunity. Risk Assessments serve as the foundation for a strategic approach to marrying business goals with security and compliance requirements while helping to create an effective long term risk management program.

The SecureTrust ISRA is right for any organization looking to assess their risks and develop a risk management program. With our experience conducting risk assessments and assisting businesses of all sizes to stand up risk management programs, SecureTrust is the right partner to help you address evolving threats and vulnerabilities.

SecureTrust's risk assessment approach examines both the design and operational effectiveness of your information security program and security infrastructure through an iterative process of information gathering and analysis. We will identify threats and vulnerabilities for each of your identified critical assets and determine the likelihood and impact of a risk event affecting the asset's confidentiality, integrity and availability. With this information in hand, we can determine your current level of risk and recommend the appropriate and necessary safeguards. Your risk assessment can become a strategic turning point for improving your organizations approach to data security and risk management to protect your business.