MEGAPLANIT

R Is For RISK Assessments

Implementing Risk Assessments & Making Informed Decisions

www.MegaplanIT.com

Table of Contents

1. Executive Summary / Abstract

Many organizations struggle to effectively manage risk. Risk assessments play a critical role in risk management. Where do we begin? What factors do we need to consider? Assessing an organization's risk requires more than a standard template or online questionnaire. It begins with an understanding of the organization – the business. Executing formalized risk assessments can lead to a more complete view of relevant threats and vulnerabilities, in addition to potential negative business impacts and appropriate countermeasures. Successful executive leadership teams leverage risk assessments to proactively assess and manage identified risks, based on acceptable and agreed upon risk levels. A Risk assessment is not intended to occur as a single, isolated event. Rather, it is part of an ongoing risk management process that ultimately supports business resilience to adverse events.

2. Introduction

Risk assessments involve multiple components, with specific definitions and examples below:

An "**Asset**" can include people, processes, or technology. For example, machine instances running in a public cloud may be an asset.

A "**Threat**" refers to a potential threat source and threat event. For example, social engineering or unauthorized system access by an external attacker.

A "**Vulnerability**" is a flaw or weakness that is susceptible to attack or exploit by a potential threat. For example, unpatched software or weak password authentication settings exploited by an attacker using a published exploit.

The "**Likelihood**" of an adverse event is the probability of a vulnerability being exploited by a potential threat. For example, if an internet-facing system had an unpatched vulnerability that could be easily exploited by an attacker using a published exploit, may result in a "high" likelihood.

The "**Impact**" refers to the magnitude of a realized threat. For example, if a business-critical system were exploited and resulted in a loss of unencrypted confidential data the impact could be considered high.

A "**Risk**" refers to the potential loss or damage to an organization, when an identified threat successfully attacks a potential vulnerability. It takes into consideration the likelihood of the adverse event and impact of the realized threat. For example, an unpatched vulnerability with a high likelihood and high impact would be considered high risk. High risks often require corrective measures to be put in place.

3. Problem Definition

Before embarking on a risk assessment, an organization should consider key pre-assessment elements, such as:

Targeted Level or Tier (organization, process, system)

External and internal requirements (regulatory, compliance, contractual)

Business type and size

Policy-defined requirements

Security requirements

Identifying these pre-assessment elements sets a level of expectation on the scope and results of the assessment. Risk assessments may be performed across multiple levels or tiers: organizational, business process, or information system.

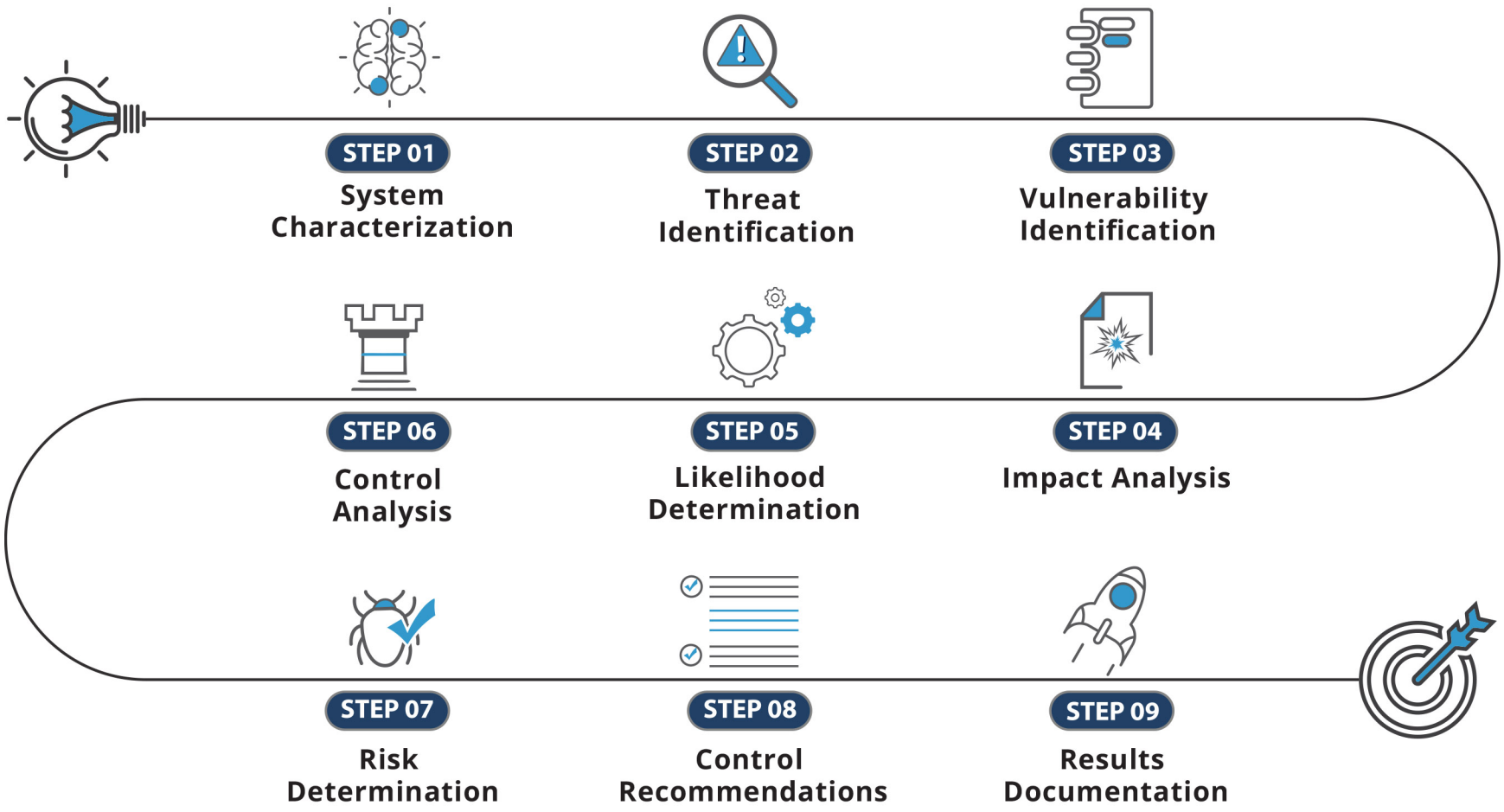
For example, a risk assessment solely focused on PCI DSS scoped systems, processes, and personnel could be too narrow for an organization that handles electronic protected health information (ePHI) and must comply with HIPAA. The business type and size often play an important role when executives consider the cost-effectiveness of countermeasures. The value of a business asset or amount of revenue generated could be less than the cost of implementing or remediating a particular control. A practical approach needs to be considered, rather than arbitrarily applying unrealistic controls that could be addressed through alternate means. Existing policies and security requirements should be reviewed, to determine what baseline requirements exist within the organization, prior to initiating the risk assessment. The results of the risk assessment may then inform leadership on opportunities to more closely align internal policy and security requirements with the go-forward plan. For example, if an organization determined that it needed to more broadly adopt multi-factor authentication (MFA) and stronger password requirements based on NIST, policies and security settings may need to be updated to reflect those revised requirements.

4. High-level Solution

Risk assessment methods can vary, based on industry, assessment type, and purpose. Assessments may also occur at different phases within an organization's lifecycle. For example, prior to deploying a new, internally developed business application or as part of an annual cadence. Risk assessments generally follow a four-phase process:

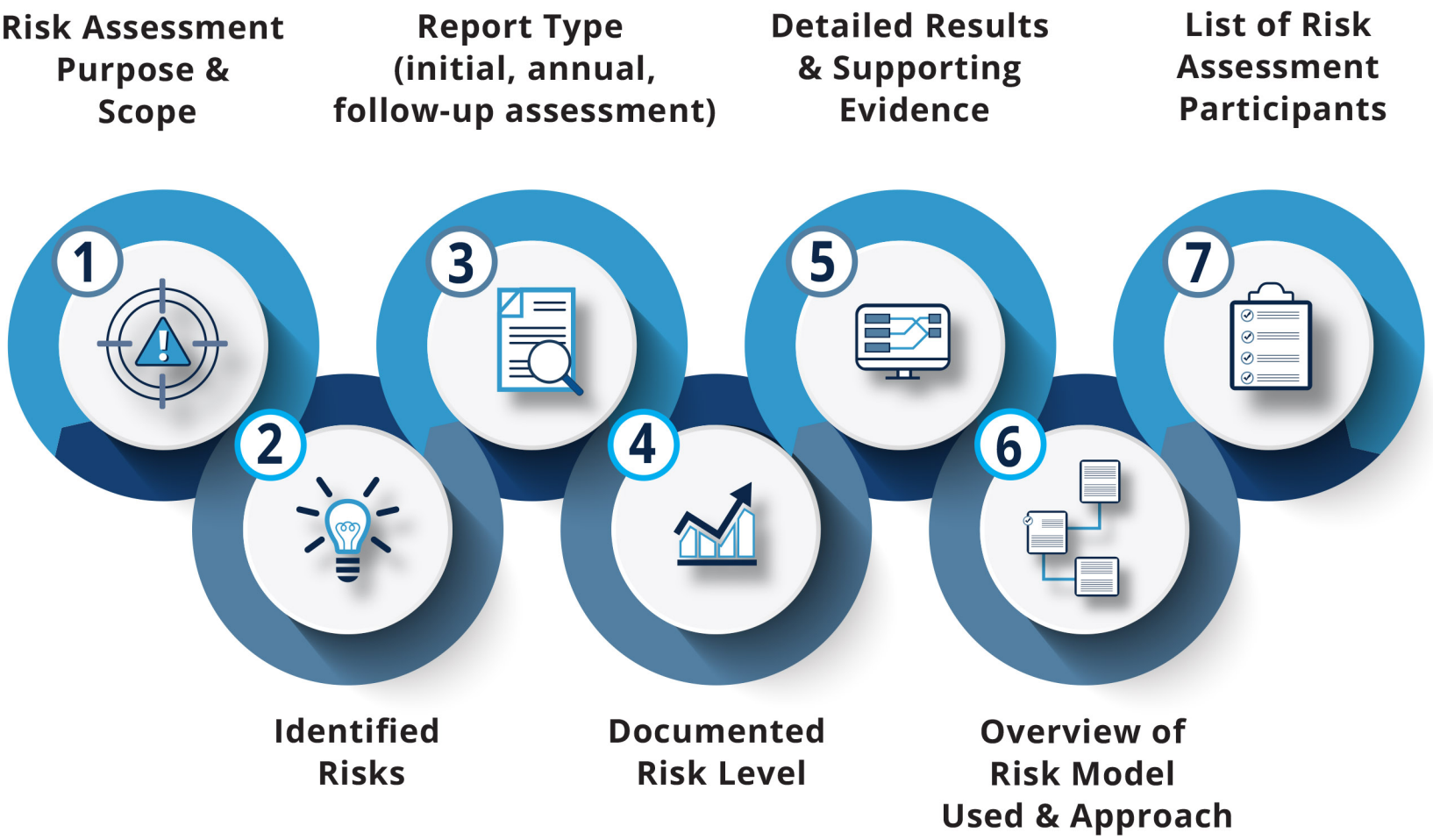
5. High-level Solution (continued)

One of the common risk assessment methodologies in use today is the NIST SP 800-30 (Risk Management Guide for IT Systems). The NIST methodology follows a Nine-Step Process:



6. High-level Solution (continued)

While each step is critical to the success of the assessment process, publication and presentation of the risk assessment results is paramount. Results should be documented and presented using clear, concise language to leadership and relevant stakeholders. At a minimum, the following topics should be addressed in a risk assessment report:



7. Solution Details & Business Benefits

MegaplanIT Holdings, LLC provides risk assessment services to businesses of varying sizes, across multiple verticals. Our services build on industry standard methodologies, internally developed tools, and our team's years of experience conducting assessments to address internal and external client requirements. We tailor our suite of services and product offerings to your organization's specific needs, providing relevant insight and guidance in an efficient and cost-effective way.

Your business will benefit from MegaplanIT's unique approach by providing you with a relevant and precise direction for your risk management program. We partner with our clients and take the time to understand your business, enabling us to deliver concise deliverables thatillustrate measurable risks and identified threats to upper management. Conducting an effective risk assessment, as part of your risk management program, supports business resilience and the ability to prioritize and focus resources on critical areas of risk. Developing appropriate internal risk management processes and procedures can also reinforce your incident response, disaster recovery, and business continuity plans.

At MegaplanIT we understands the demands of your business. You need your data to be accessible to your organization, yet impenetrable from the outside. You also have to comply with increasingly stringent information security regulations, which are vital not only to your security but to your success. On top of that, you're still, well—running a business. Our innovative IT security and compliance solutions are designed to deliver customized, cost-effective service on time—because your priorities are our priorities. With a highly qualified team of PCI-DSS QSAs, Penetration Testers, and Information Security Consultants here at MegaplanIT, we will assess your unique company and business environment and design a path to security that will fit all of your needs.

Have A Question?

A MegaplanIT Expert Is Here To Help

Contact Us