How to Implement Practical Security Assessments

Introducing the Relational Security Model

© Rsam. All Rights Reserved.

Table of Contents

© Rsam. All Rights Reserved. | www.rsam.com | +1-800-920-Rsam (7726)

Introduction

Organizations are scrambling to identify security weaknesses before their adversaries do. Having a consistent, systematic, and scalable methodology to properly assess your environment is essential. To begin you need a solid understanding of the organization, its components, what it relies on, and what could cause it harm.

The Relational Security Assessment Model was developed as a guide for developing a proper and balanced perspective in the rather oblique world of assessments. Embracing good concepts behind risk evaluation and control assessment is vital for security-minded organizations. With this foundation in place, you're better positioned for a security audit.

This paper covers ways to gain perspective about your security based on:

- Objects
- Criticality levels
- Criticality factors
- Controls
- Control levels
- Risk control policies

What is an "Object"

Assessments can be conducted against truly anything in the organization. This includes tangible things you can touch (like a device) and intangible things you cannot touch (like a process). A good methodology should be able to cover all scenarios with all types of "things". It's important to have a neutral word to describe these different "things." In the Relational Security Assessment Model this word is "Object".

As you plan, inspect, test, interact, evaluate and do other activities, you will be targeting Objects. Empowered with this word you can now easily reference anything in the organization, be it a person, an asset, a process, etc.

Traditional Assessment Methodologies

Security professionals think in terms of risks and threats to ensure that the right security measures are deployed in the right places and to the correct degree. If the organization needs to make a decision about an application, network or device, you must understand the risks associated with each. In most situations, you can't simply spread security evenly across the organization. That's ineffective and costly. The device that controls the heartbeat of a patient will surely need to be more secure than the candy-dispenser down the hall.

Security teams need an evaluation process to help them determine whether an object is under-protected or over-protected. To do that, you must think and see objects in terms of threats and risks.

Sometimes the terms threats and risks are often used interchangeably but they're quite different.

A threat is a bad thing that can happen. A fire in a data center is a threat; so is a hacker who has gotten inside a sensitive database. A threat is some event outside of our control that could make our risk into a reality. In simple terms, if your house has a $1,000 risk policy to ensure against theft, it takes a thief breaking into the house to manifest the risk.

A risk speaks to the potential negative impact a threat can have on an environment. Every time an organization relies on something, there is a possibility that the 'something' will cease to function or become exposed. Using the house analogy again, if an event could happen that would cause damage to the house and cost you, at most, $1,000 in damages, that house is considered to carry a $1,000 risk adjusted for the actual chance of such an event happening and the effect it would have.

Assessing actual risk is one of the most difficult tasks in any security program. Typically it's done using qualitative and quantitative methods.

© Rsam. All Rights Reserved.

A quantitative assessment recognizes a series of common factors in each object to:

- Derive some dollar or numeric amount that represents how much we should spend to protect it
- Come to a conclusion about which objects are more at risk and which should be addressed first

A quantitative assessment follows a process like this:

1. Assign a value to the object
2. Take the major threats posed against that object and determine the damage that each could do
3. Calculate the likeliness of each threat occurring on an annual basis
4. Multiply these factors together to get the annual loss expectancy (ALE)

Table 1: Simplified Example of Quantitative Assessment

Object	Value	Threat	Chance per Year	Potential Loss	ALE
Server X	$50,000	Fire	5%	$35,000	$1,750
		Security compromise	15%	$22,000	$3,300
		Component failure	24%	$10,000	$2,500

If it works, then the ALE figure can help you determine how much per year to spend on security for Server X. For instance, if you're spending $10,000 a year to secure Server X, it may be too much since the ALE is $7,550.

A qualitative assessment serves a different purpose. It aims to weigh a series of educated opinions about an object's risks. Usually the organization will pull together several subject matter experts (SMEs) who will go through a process like this:

- Each person is presented with a list of objects or types of objects
- Each person is asked to comment on and rank a series of scenarios and how they would affect the object and organization
- The cumulative opinions are average, giving an overall ranking for the object

Table 2: Simplified Assessment for a Compromise on Server X

If Server X were compromised by a hacker, how could it affect the organization on a scale of 1-10?

Object – Server X	Damage to Productivity	Damage to Customers	Likelihood of Threat
SME John	9	7	5
SME Jane	3	2	3
SME Mike	3	3	4
Average	**5**	**4**	**4**

If you average the scores from each scenario, you can compare different risks within each object. You can also look at the risks of every object and compare them against each other, enabling you to rank and prioritize them when dealing with security issues.

© Rsam. All Rights Reserved.

Shortfalls of Traditional Assessments

Quantitative and qualitative assessments provide a formal and repeatable process but they have shortfalls that also make them less than ideal:

Quantitative Shortfalls	Qualitative Shortfalls	Shortfalls of Both
Difficult to reasonably assign a value to an object	Risk decisions are based on opinions	It's hard to evaluate security relationships
It's difficult to calculate the chance per year that a threat will occur	SMEs who don't participate or give little thought to responses will invalidate results	Don't scale well to large environments
Takes too much time and resources to perform an audit	Understanding how to interpret and take action on results is complicated	
	The work involved creates a time burden on SMEs	

A Better Way – The Relational Security Assessment Model

The relational security assessment model defines a series of meaningful values and assigns those values to different objects. Once done, you can create policies that dictate how to handle objects of specific risk values.

Criticality Levels & Criticality Factors

The basic components of the relational security risk assessment include criticality levels and criticality factors.

A **criticality level** is the degree of importance an object has within an environment and the level or risk we face should it be unable to perform. The goal of a criticality level is to qualify and quantify, on an enterprise-wide scale, a weighted risk value for each object.

Table 3: Sample Criticality Levels

Criticality Level	Description
None	This object and its services are inconsequential to the environment. If the object was compromised or disable without warned, there would be no noticeable impact.
Low	This object plays some minor role within the environment. If the object was compromised or disables without warning, there would be minimal effects to the organization.
Medium	This object plays a significant role within the environment. If the object was compromised or disabled without warning, there would be noticeable effects on the organization.
High	This object plays a very important role within the environment. If the object was compromised or disabled without warning, the effects would be quite harmful to the organization.
Extreme	This object is essential to the continued operation of the organization. If the object was compromised or disabled without warning, there could be disastrous effects on the organization.

Tips for Defining Criticality Levels

Consider the following when determining criticality levels; they should be:

- Universal to the organization
- Quantified with sample data, such as cost or recovery
- Kept to a minimum, ideally no more than six

Also, try to associate real-world data to each criticality level to help with consistent interpretation.

© Rsam. All Rights Reserved.

Table 4: Real-World Data for Criticality Levels

Criticality Level	Company X
Medium	Up to $3,000 in repairs, lost productivity, fines or lawsuits; or the loss of 5-10 customers or a partner.
Extreme	Up to $10,000 in repairs, lost productivity, fines or lawsuits; or the loss of 500-1000 customers or several partners.

A **criticality factor** is an individual detail about an object in relation to the organization. Each factor has a related criticality level that correlates the specific detail to the universal criticality levels. Most objects will have several criticality factors.

With criticality factors, you can derive the criticality level of any given object through a series of simple facts, not opinions. Instead of asking an administrator to choose a criticality level for each object, let the person choose from a group of factors. Based on the factors selected, you can derive a more meaningful criticality level.

Tables 5 and 6 provide examples of common criticality levels.

Table 5: Employee Downtime

Example Criticality Factor	Factor Value	Criticality Level
If this object was unavailable for a day, what would be the impact to employee downtime?	0-5 hours	None
	6-10 hours	Low
	11-10 hours	Medium
	21-35 hours	High
	36+ hours	Extreme

Table 6: Customer Impact

Example Criticality Factor	Factor Value	Level
How many customers use the object in a day? If it were unavailable for a day, how many customers would be impacted?	0-10	None
	11-30	Low
	31-50	Medium
	51-100	High
	100+	Extreme

The more variations of criticality factors you have, the more accurate the assessment should be. Determine your own criticality factors as related to defined levels. Table 7 shows other common types of criticality factors to consider.

Table 7: Common Types of Factors

Criticality Factor Type	Scoring Considerations
What types of data are stored in the Object	Does this object stores sensitive data, or data that is protected by compliance requirements?
What would be the effect if the object were defaced or vandalized?	If this object were vandalized, would it impact users – like an internal or external web server?
What would be the effect if the object's data were erased, corrupted or modified?	If all data was lost forever, how would it impact the organization?
What would be the effect if the object's data was stolen?	Does the stolen device contain financials, intellectual property, employee, health, or payment data? What are the legal, contractual or social implications?
How important is the object within the environment?	Is the system accessible by many? Would it be possible for someone to break into this system and attack other systems?

© Rsam. All Rights Reserved.

Tips for Creating Criticality Factors

Consider the following when determining criticality factors in your own environment:

- Remove opinion from the process as much as possible
- Choose a variety of criticality factors, covering key events that could affect your environment
- Think about each criticality factor and how it relates to the bigger picture
- Be sure to compare different criticality levels/factors to each to see if they make sense. For example, is losing 40 employee hours (critical) really as important as impacting 60 customers (also critical)?

By using criticality factors, you can easily assign a consistent and objective value to anything within the organization. Choose all factors for any object. Once you determine all related criticality factors, it's a matter of choosing the highest criticality level of all related factors. The factor with the highest level of criticality represents the greatest risk of any object within the environment.

A system that results in no hours of employee downtime (none) but affects 101 customers (critical) is a critical risk just the same as a router that causes 50 hours of downtime (critical) but affects only five customers (none).

Table 8: Determining Levels

Object	Criticality Factor	Overall Criticality to Organization
Server X	10 hours of employee downtime Impact 200 customers	Critical
WAN Link Y	30 hours of employee downtime No impact to customers	High
Application Z	10 hours of employee downtime Impact 40 customers	Medium

Review of Risk Assessment

So far, we've performed the following steps of the Relational Security Risk Assessment:

1. Defined universal criticality levels for the organization
2. Defined factors, each relating to a level
3. Assigned factors to objects we want to assess
4. Determined the highest level assigned to an object

Now we can assess and compare the criticality of individual objects. Once the levels of the objects are defined, it's easier to recognize where risks exist and which objects may or may not be adequately protected. We can also see correlations between different objects, which guides prioritization.

Table 9: Object-Weighted Levels

Object	Criticality
Server X	High
Server Y	High
WAN Link X	High
Server X	Medium
WAN Link Z	Low

Deriving Relational Risks for 'Containers'

During the assessment process, it will become evident that not all objects have direct risks. For example, the criticality of a room can only be assessed by looking at the objects within it. Similarly, the criticality of a router depends on which networks it is connecting. These objects are called ***container objects*** because their criticality completely depends on the criticality of the objects contained within them. Since we have already determined the criticality of our servers, WANS, and the like, we can use this information to evaluate relational risks.

© Rsam. All Rights Reserved.

Table 10: Determining Container Levels

Container Object	Objects Inside	Overall Risk to the Organization
Data center 1	Server X (critical) Server Z (low) Router Y (high)	Critical
Server Y	High	
WAN Link X	High	
Server X	Medium	
WAN Link Z	Low	

Determining the Level of Protection

The next part of the Relational Security Risk Assessment models delves into the degree to which you want to protect objects. For each object, you need to define a minimum level of protection based on criticality level. Objects that are of greater risk will most likely have higher control requirements than objects with no security risk.

Controls

Organizations have various types of controls. Also, different types of objects have different types of controls. For example, servers and routers provide logging and monitoring controls. A room has entrance controls, such as a key lock or biometric device. Every object has a series of controls that will help ensure its security.

Table 11: Sample Control Types

Object Type	Possible Types of Controls
Server	Logging, monitoring, authentication, authorization, hardening, drive redundancy
Router	Logging, monitoring, local authentication, remote authentication, hardening
Room	Monitoring, perimeter access control, power protection

Control Levels

For each type of control, there are various degrees to which the control can be implemented. One version of the control may be more secure than another. If we take the data center as an example, we can adjust the strength of the control used to protect to room based on its risk level. We could require rooms with low risk levels to implement a single key-lock while rooms with higher risk levels implement key-card access or biometrics.

Risk Control Policies

In most organizations, it's not possible or practical to apply the highest level of control to all objects. You may not have the resources or budget to place biometrics at every data center door. You must tailor security to place the strongest controls where they're needed most. With a control policy, you can specify that objects of a certain level require some minimum degree of controls to protect them.

Since we have already worked to define different levels of risks and controls, we simply need to combine the two to form policies. Risk control policies designate the minimal level of control in warranted for devices of a specific level. The security control for any given object should be at least as high as its level dictates.

Table 12: Sample Risk Control Policy in the Data center

Control Type	Level	Minimum Control Level Required
Entrance control	None Low Medium High Critical	No control Standard lock Standard lock Key-card access Key-card access
Entrance monitoring	None Low Medium High Critical	No monitoring No monitoring Must pass by staffed desk Recorded camera Recorded camera

© Rsam. All Rights Reserved.

Scoring an Object

After you develop a control policy, it's easy to score different objects. The score of any object is derived by comparing its required controls to the controls that are actually implemented and adjust this for the relative risk. Each time an object's control does not meet the minimum policy standard, it's considered a violation. Violations are totaled to give the object a violation score. Systems with higher scores are further out of compliance than systems with low or no scores.

Table 13: Scoring Objects

Object	Level	Control	Applied Level	Required Level	Violations
Room A	Low	Access Monitoring	1: Standard key 0: None	1: Standard key 0: None	0 0
Room B	Critical	Access Monitoring	1: Standard Key 2: Recorded camera	2: Magnetic card 3: Active camera	1 1

Scoring an object helps to see which objects are in violation of risk control policies as well as which objects have more violations and need to be given a higher priority. It also allows us to average scores for different facilities or departments and compare them with each other. Scores help to pinpoint trouble areas in the organization and track progress over time.

Weighting the Score for Risk

When calculating the score for an object, organizations can chose between simplified and more comprehensive modules. While all modules are more scalable than ALE and traditional qualitative modules, it's important to decide which model fits your organizations goals, maturity, and bandwidth. The model chosen will help strike the balance between creating a basic compliance assessment (counting the violations), or a risk assessment (weights for criticality levels, controls, control levels, and containers).

Table 14: Weighting factors in the Relational Security Methodology

Scoring Method	How This Effects Perception
Compliance Mode… just count the violations.	Application A has 6 violations **versus** Application B has 4 violations
Adjust the score by applying weights to the type of control and degree of implementation.	Application A has 6 violations. All of which are basic controls. **versus** Application B has 4 violations, 2 of which are critical controls.
Adjust the score by applying weights to the Criticality of the Object.	Application A, which is low impact to the organization, has 6 violations, all of which are basic controls. **versus** Application B, which is critical to the organization's ability to do business, has 4 violations, 2 of which are critical controls.

© Rsam. All Rights Reserved.

Summary

In this guide we have covered the basic building blocks of the Relational Security Assessment Model, including:

- Criticality levels
- Criticality factors
- Controls
- Control levels
- Risk control policies

The core concept behind the Relational Security Assessment Model is understanding how to properly assess security objects in your environment. With this foundation in place, you're better positioned for a security audit.

About the Relational Security Assessment Model

The Relational Security Assessment Model was developed by Kevin Day, CTO of Rsam. Kevin began his career as an information security and risk assessment consultant. His experience working with hundreds of large organizations, Kevin realized a new approach to security assessments was needed to simplify this very complex and often misunderstood process. He developed the Relational Security Assessment Model to help security-minded professionals make the best decisions possible when it comes to assessing risk in their environment. It has been successfully implemented at some of the largest organizations in the world.

About Rsam

Rsam helps organizations meet their security, risk and compliance goals quickly, even as requirements are always changing. Our enterprise software platform uses a relational architecture and captures data in a single, centralized repository. Unlike other systems, we don't hard-wire dependencies based on requirements that were probably outdated before implementation began. Instead, the Rsam platform is built to adapt and puts the user in control. Our vulnerability management and security incident response modules free you from the worry of "what have we missed?"

To learn more about Rsam, visit rsam.com.

About Rsam

Rsam is a leader in the field of Governance, Risk, and Compliance (GRC) solutions and is the fastest time-to-value GRC provider. The Rsam platform delivers unparalleled flexibility for companies to leverage out-of-the-box solutions and "Build Your Own" (BYO) applications for a wide range of GRC functional areas, including audit, business continuity management, compliance, enterprise risk, IT risk, incident management, operational risk, policy management, security risk intelligence, vendor risk management, regulatory change management and more. Learn more about Rsam at http://www.rsam.com

© Rsam. All Rights Reserved.