Photo Credit: Paul Cross (https://creativecommons.org/licenses/by/2.0/) photo cropped/resized

Taking Good to Great: 3 Factor Risk Assessment

By Bob Bretall
Enterprise Agile Coach

Risk [noun]: *exposure to the chance of injury or loss; a hazard or dangerous chance*

There has been increasing concern about information security around the world over the last decade. The information assets of many companies have been shown to be vulnerable to attack and breaches have occurred. We have been asked many times to help give our customers and other stakeholders assurance that their information assets and intellectual property are well protected.

Protecting your organization's information assets from exposure to risk is a wonderful goal, but do you try to protect from **ALL RISK**? Wisdom would indicate that it is not possible to protect from every conceivable risk. It is probably not even possible to protect your information assets from every reasonable risk. Many of our stakeholders have asked us to implement information security models that ensure the confidentiality, integrity and availability of their information assets. Compliance with regulations like HIPPA, PCI DSS and SOX drive various controls into our businesses.

The goal most organizations strive for is to identify and understand the risks facing their information assets and then establish a set of criteria that helps them decide which risks should be addressed in some kind of priority order. Address the risks with the highest priorities, and assumedly the highest impact to the organization if they are realized, and also define a process for accepting risks that cannot be addressed. Models like the international standard ISO 27001, Control Objectives for Information and Related Technology (COBIT), NIST SP 800, all have common elements.

THE DESARA GROUP

Adding that third factor into your risk assessment methodology can take it from good to great.

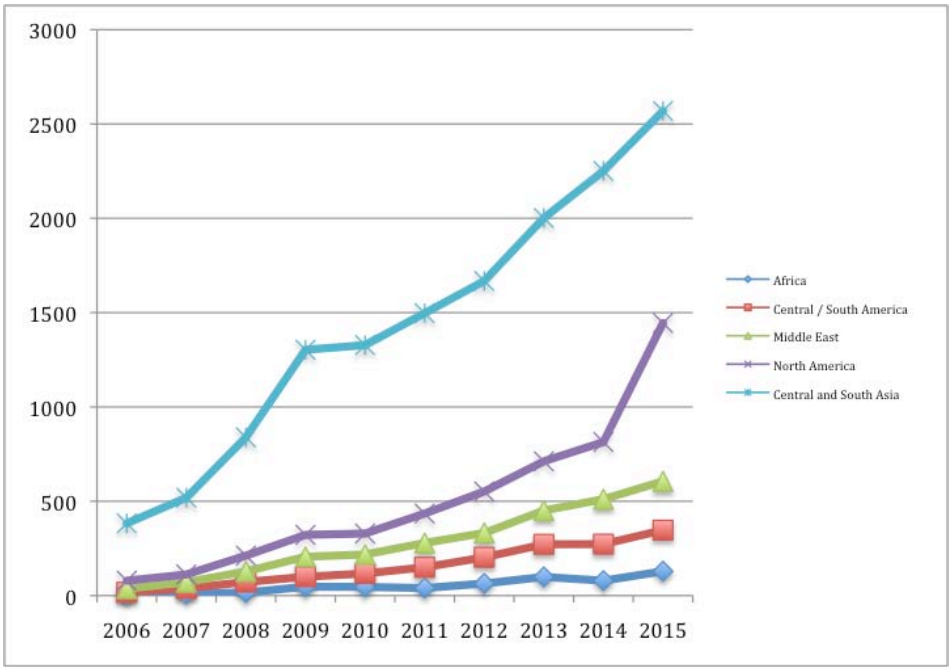
Some of the basic requirements of all models are risk assessment and mitigation. This article is one that speaks to information asset identification, risk analysis and risk mitigation in order to describe the overall risk management process. There is certainly more that can be said about these topics, but keeping it high level here allows some context while specifically outlining the framework for a more advanced method of risk assessment we feel is a better approach than normally applied. One that not only identifies and prioritizes risks, but one that models and is able to demonstrate to yourself and others that risk reduction is occurring.

It is common to see two factor methods that look at the probability that a risk will manifest itself combined with the impact that the risk would have on the organization if the risk occurred and an information asset were compromised. This is a good way to characterize the effect the risk could have, but it fails to take into account the mitigating factors your organization may already have in place to foil risks of that type.

Adding that third factor into your risk assessment methodology can take it from good to great.

The International Organization for Standardization (ISO) has just released its 2015 management system implementation statistics showing greater than 20% growth in ISO 27001 certifications for the past few years. If you are reading this article you may be someone who is interested in adding to that growth by achieving an ISO 27001 certification for your organization:

Figure 1 - ISO Certification Growth (http://www.iso.org/iso/iso-survey)



Let's look at the entire ***information risk management process*** so we can see where taking a third factor into account will make a difference:

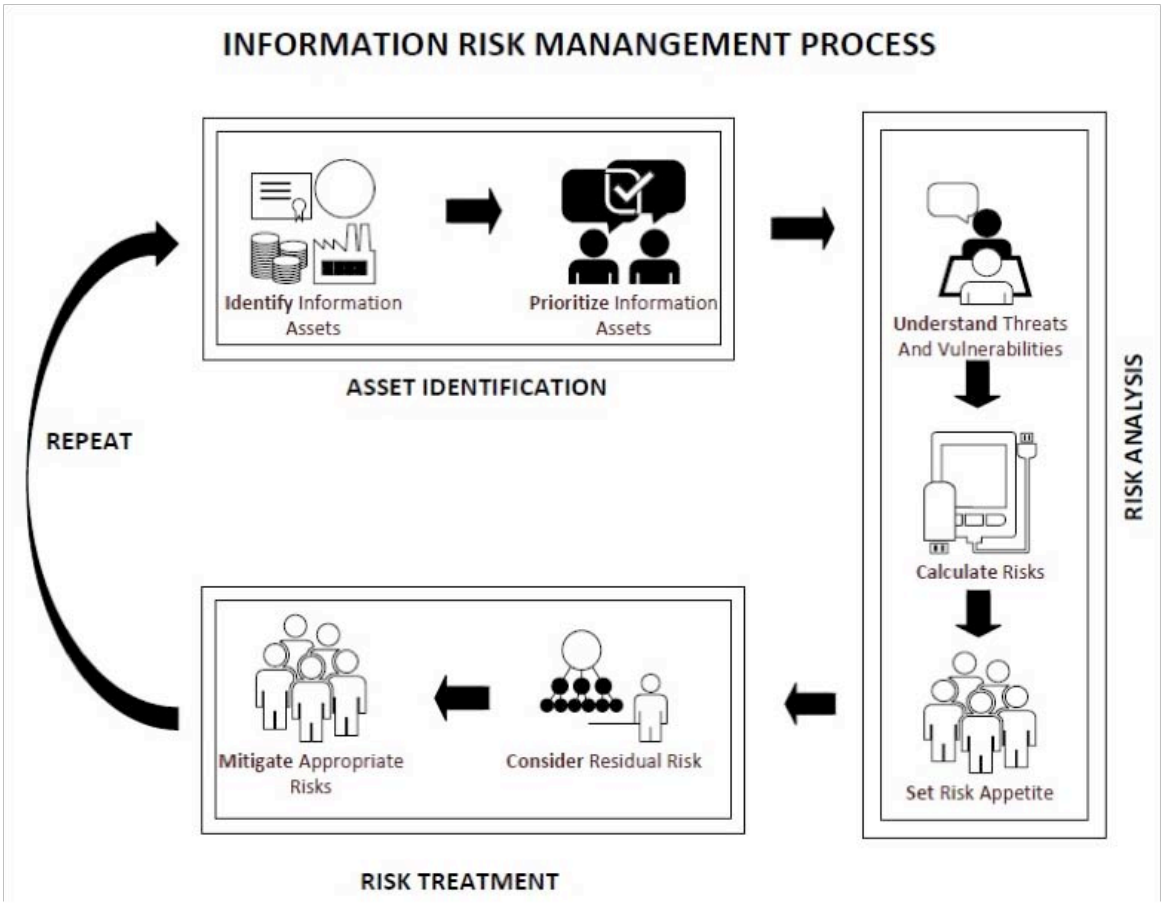


Figure 2: Sample Process Flow

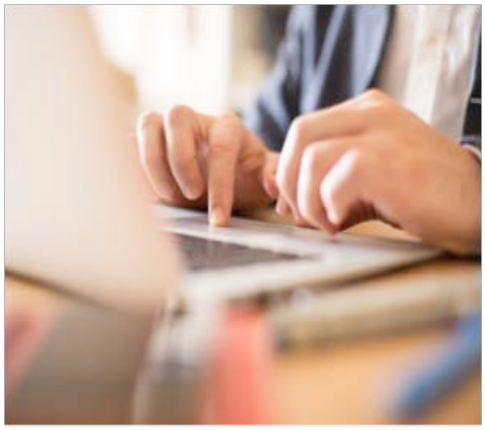
1. **Identify** all information assets in the organization - i.e. all assets which may affect the security of information in the organization.

2. **Prioritize** each information asset in terms of the worst-case impact the loss of confidentiality, integrity or availability of the asset may have on the organization.

3. **Understand** all threats and vulnerabilities associated with the assets. Every asset may be associated with several threats, and every threat may be associated with several vulnerabilities.

4. **Calculate** the risk score, also called the Risk Priority Number (RPN), for each asset/threat/vulnerability combination. This is where our 3 factor risk assessment comes into play:
   - ***Likelihood***: Measure of probability that a compromise will be attempted
   - ***Impact***: Measure of damage caused by a successful compromise
   - ***Countermeasures***: Measure of effectiveness of processes/technology in place to reduce the probability of a successful compromise

   RPN = L * I * C



An information asset is a body of knowledge that is organized and managed as a single entity. Like any other corporate asset, an organization's information assets have financial value.

5. **Set** Risk Appetite**.** Analyze the RPN values to determine a Risk Appetite for the organization. Risk Appetite is the level of risk that the organization is prepared to accept before action is deemed necessary to reduce it. It represents the cost of making changes to reduce risk against the negative impact of experiencing the risk event.

6. **Consider** residual risk, which is the danger of an action or event occurring even if all theoretically possible safety measures are applied.

7. **Mitigate** appropriate risks. All of the above feeds into the organization's Risk Treatment Plan process where risks, typically those with an RPN above the organization's Risk Appetite, are queued up for mitigation and tracked to resolution.

8. **Repeat** on a regular (typically annual) basis.

Now let's look at the Risk Management process in a bit more detail:

Asset Identification

An ***information asset*** is a body of knowledge that is organized and managed as a single entity. Like any other corporate asset, an organization's ***information assets*** have financial value.

Assessing every individual file, database entry or piece of information isn't realistic. You need to group your information into manageable groups; if the groups/categories are too large you won't have enough detail to accurately assess risks, too small (or even individual items) and you will have to make unnecessary redundant assessments.

Group your ***information assets*** according to business needs and objectives. Each asset can contain individual items that need different technology solutions to address the same business need. If something could logically belong within two different ***information assets***, choose one and move forward. It isn't necessary to be perfect. Strive to identify an initial set of ***information assets*** that are good enough to work with, and there will be plenty of opportunities to fine tune things as the process moves along. If a group of ***information assets*** have diverse threats, vulnerabilities and/or classifications we may need more granularity (e.g., 'employee laptop', 'manager laptop', and 'C-level laptop' instead of just 'laptop').

Information assets can be prioritized by assigning a classification level to the asset or alternately using a simple numeric value. The main point here is to identify which ***information assets*** are more important to the organization, or that would cause a greater impact to the organization if compromised.

Risk Analysis

Understand the ***threats*** and ***vulnerabilities*** that may affect your information assets, and use that information to calculate a numeric value for the risk facing your organization.

Threats

A ***threat*** is a potential event and does NOT include an element of probability. When a ***threat*** turns into an actual event, it may cause an unwanted incident that may harm the organization or its systems

Threats are generally external to the information asset or organization.

Vulnerabilities

At its simplest, a ***vulnerability*** is an exposure to attack or a weakness in an information asset or group of assets. This weakness could allow it to be exploited and harmed by one or more threats. A ***vulnerability*** could result from a design or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

Vulnerabilities are generally internal to the information asset or organization, whether they are features, deficiencies, or flaws.

Calculate Risk

Many risk methodologies look at the ***likelihood*** that the risk will occur and the ***impact*** that it may have on your organization. This two factor risk assessment calculation is very common, but it's not enough. Adding a third factor, the ***countermeasures*** that are in place that will serve to prevent the risk from occurring, is absolutely essential to augment the likelihood and impact that when considered on their own fail to paint a complete picture of risk.

Third Factor Difference

Utilizing the third factor, ***countermeasures***, gives you an idea of what measures you already have in place to protect your information asset. The baseline protection provided by existing countermeasures is important to take into account for a complete understanding of existing risk. It is often difficult to alter the likelihood that a risk will occur. It is similarly difficult to alter the business impact of a realized risk. But it is often very effective to reduce an unacceptable risk by adding new countermeasures that alter the ability of the risk to manifest. To understand this better, let's look at the 3 factors of risk in more detail on the following tables: **Likelihood**, **Impact**, and **Countermeasures**.

Likelihood

For each asset/threat/vulnerability combination, determine the probability of the specific risk happening. *Will it **be attempted**, not will it be successful*

Table 1: Likelihood Guidance

Likelihood	Guidance	Rating
Critical *(Certain)*	• History of regular occurrence • The event **will** occur (recur) • No special skills or determination required; information asset easily available	10
High *(Likely)*	• The event will occur (recur) in most circumstances	7
Medium *(Possible)*	• Has occurred in the past • The event may well occur (recur) at some time • No special skills required except for time and determination	5
Low *(Unlikely)*	• The event could occur (recur) at some time	3
Minimal *(Rare)*	• No history of occurrence • The event may only happen in exceptional circumstances • High level of technical or social engineering skill and determination required	1

Impact

For each asset/threat/vulnerability combination, consider the business impact should the risk happen:

Table 2: Impact Guidance

Business Impact Rating	Characteristics	Rating
Critical (Catastrophic)	The issue causes multiple severe or catastrophic effects on organizational operations, organizational assets or other organizations	10
High (Major)	Exploitation produces severe degradation in organizational capability to the point that the organization is not able to perform primary functions or results in damage to organizational assets	8
Medium (Moderate)	Threat events trigger degradation in organizational capability to an extent the application is able to perform its primary functions, but their effectiveness is reduced and there may be damage to organizational assets	6
Low (Minor)	Successful exploitation has limited degradation in organizational capability; the organization is able to perform its primary functions, but their effectiveness is noticeably reduced and may result in minor damage to organizational assets	3
Minimal (Insignificant)	The threat could have a negligible adverse effect on organizational operations or organizational assets	1

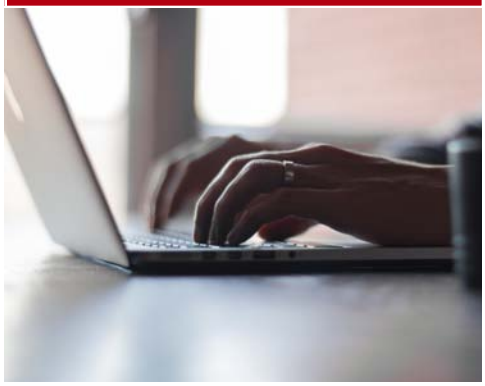
Countermeasures

For each asset/threat/vulnerability combination, consider the ***countermeasures*** that are already in place that would serve to reduce the likelihood and/or impact of the risk manifesting.

Countermeasures are rated on an inverse scale. The better the ***countermeasure***, the lower the number associated with it.

Table 3: Countermeasures

Countermeasure	Characteristics	Rating
Best in Class	The countermeasures in place have taken into account the threat and vulnerability in question and provide the best known protections. (These countermeasures are the best known, no one in any industry does it better)	1
Strong	The countermeasures in place have taken into account the threat and vulnerability in question and provide above average protections. (These countermeasures are strong)	3
Average	The countermeasures in place have taken into account the threat and vulnerability in question and generally provide good protections. (These countermeasures expected by general good practice)	6
Weak	Some countermeasures are in place, but confidence is not high that they will be effective in opposing the threat and vulnerability in question. (It is felt that these countermeasures could be improved)	8
None	None or very few countermeasures are in place to oppose the threat and vulnerability in question	10



Calculating the RPN is an easy way to understand this risk level on a numeric scale which, while not perfect, is a great way to understand relative levels of risk and concentrate our efforts at reducing the risks that will be of more value to the organization.

Calculate the RPN

Now we put these factors together to create a ***Risk Priority Number (RPN)*** that will help us numerically understand the level of risk as the product of the factors of the risk:

- **Likelihood**: Measure of probability that a compromise will occur
- **Impact**: Measure of damage caused by a successful compromise
- **Countermeasures**: Measure of effectiveness of processes/technology in place to reduce the probability of a successful compromise

RPN = L * I * C

Third Factor Difference: Think about likelihood. It is the measure whether an attempt will occur and is typically an external factor out of your control. Think about impact. It is what happens to your business in the face of a successful compromise and is in most respects primarily a function of the value of the information asset to your organization, which is generally not a variable. If we only consider likelihood and impact, we are taking measure of things that do not have much elasticity. The **third factor**, countermeasures, are almost completely under our control. By adding in this third factor we are able to affect a wide range of change to the risk level. Calculating the RPN is an easy way to understand this risk level on a numeric scale which, while not perfect, is a great way to understand relative levels of risk and concentrate our efforts at reducing the risks that will be of more value to the organization.

Once you have the RPN value calculated for all significant asset/threat/vulnerability combinations, take the following into consideration:

- High RPN values mandate an immediate and thorough response
- The range of expected RPNs is likely to go down each year as increasingly effective security measures are put into place
- Give some thought to whether similar assets were given similar or entirely different RPN ratings

Set Risk Appetite

Risk Appetite is the level of risk that an organization is prepared to accept, before action is deemed necessary to reduce it. It represents the cost of making changes to reduce risk against the negative impact of experiencing the risk event, or conversely a balance between the potential benefits of innovation and the threats that change inevitably brings. Senior management will be responsible for establishing the organization's Risk Appetite.

An organization will typically have enough risks that it cannot address all risks during a particular quarter/ year because of the resources required to do so. Risk Appetite should take resources into account and balance the maximum level of risk tolerable before action should be taken to lower it with the amount of work that can be realistically undertaken.

An organization may have a higher tolerance for some types of risk and an aversion to others, depending on the context and the potential losses or gains. ***Risk Appetite*** should be set by choosing an RPN value that will require risk mitigation when exceeded, taking all factors into consideration.

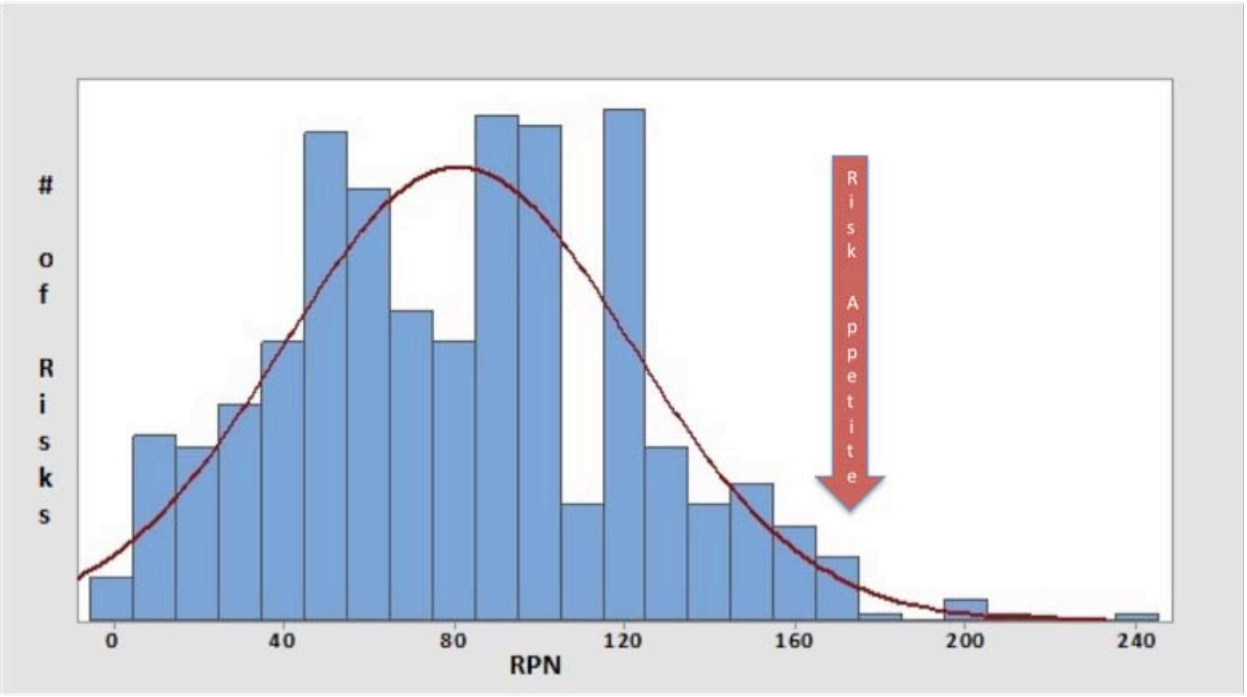


Figure 3: Sample Risk Priority Number (RPN) Distribution

Risk Treatment

Looking at a holistic view of the risks facing the organization, we will consider residual risk and treating the risks we face, but that is a topic for another time.

Suffice to say that there are a variety of ways to deal with risk:

- Avoiding Risk
- Transferring Risk
- Mitigating Risk
- Accepting Risk

The important thing is that we have a process for dealing with risk and ensuring it does not impact the organization in a negative way.

In Conclusion

Across multiple customer implementations, we have found this 3 factor approach to risk assessment to be:

1. A simple, repeatable methodology
2. Allows for numerical evaluation of various countermeasures
3. Easily understood by all levels of the organization

Hopefully you will find what has been outlined here to be a reliable and repeatable process for information risk management. Taking current countermeasures into account (in addition to the likelihood and impact of a risk) gives a more complete picture of the effect a risk could have on your organization. In addition, examining not only the current countermeasures in place, but playing around with “what if” scenarios on ways you could modify the countermeasures will allow you to see ways in which you can reduce your risk exposure.

THE DESARA GROUP

Bob Bretall

Enterprise Agile Coach

Bob Bretall has spent over 30 years in the software development field with hands-on experience in all aspects of the software development lifecycle. He has been a developer, designer, team lead, manager, trainer, mentor and consultant.

Read More **Bob.Bretall@DesaraGroup.com**