Improving Risk Decisions

Jack Jones, CISM, CISA, CISSP

Improving Risk Decisions

Too often, information security risk decisions fall victim to one or both of the following fundamental problems: decisions are made by the wrong people and/or they're made with inadequate information. Failure to understand and agree upon who should be making which risk decisions can lead to:

- Unmet expectations and objectives
- Lack of executive management support
- Impact to other business priorities

Making decisions without adequate information, on the other hand, generally results in spending on the wrong things, spending too much, or not spending enough.

This article will provide insight into the factors that drive risk decisions, the role of business management and security experts in decision making, as well as the information that's necessary in order to make well-informed risk decisions.

The decision landscape

The illustrations to the right step through a description of the risk decision landscape. The first illustration (**Figure 1**) highlights that risk decisions drive policies, priorities, initiatives, and actions. Note that existing policies, etc., which reflect earlier decisions, can also affect current decisions.

Figure 1

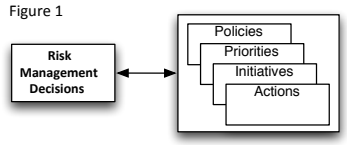


Figure 2 identifies three of the primary information inputs into the decision. (There's also a fourth input, which we'll cover further on.) It's important to note that we can already begin to identify who -- business management or security experts -- are likely to be most well-informed on each of the decision elements.

Figure 2

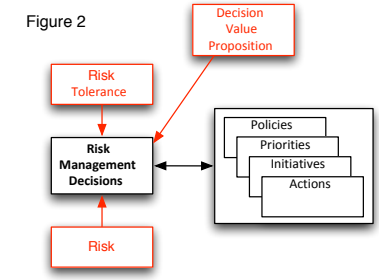
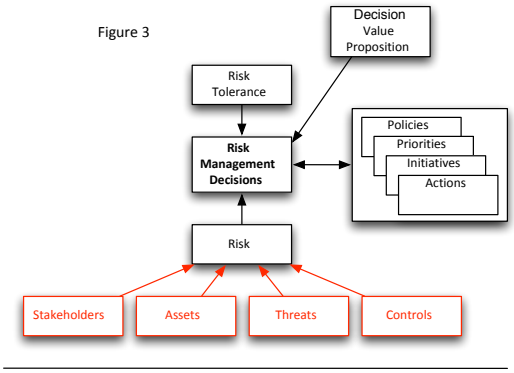


Figure 3 identifies four inputs that we must factor into any clear and useful articulation of risk:

- The key stakeholders that are involved, because impact must always be considered within the context of what they care about
- The assets that contribute value and/or liability to the stakeholders
- The threats against those assets, and
- The controls that are in place to protect stakeholder interests

Figure 3



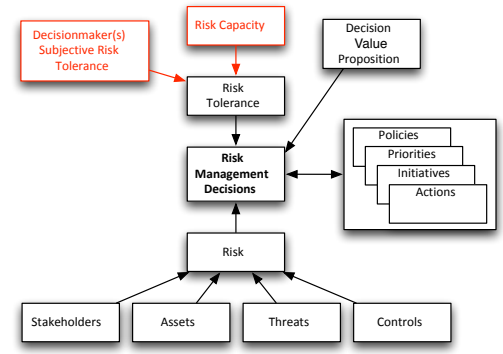
Note that we didn't describe controls as protecting assets. They do of course, but only as a means of protecting stakeholder interests. This subtle differentiation is critical if security efforts are going to align appropriately with executive management needs and expectations.

Another critical point to keep in mind is that information provided from audits and security assessments often focuses heavily on control conditions and doesn't explicitly (or sometimes even implicitly) take into consideration stakeholders, asset value/liability, or threat conditions. Some informal "gut" inclusion of those factors may have been considered by the assessor(s), but unless inclusion is explicit, risk ratings tend to

be inflated -- sometimes significantly. This risk inflation and the tendency to protect assets rather than stakeholder interests contribute significantly to overall cost-ineffectiveness.

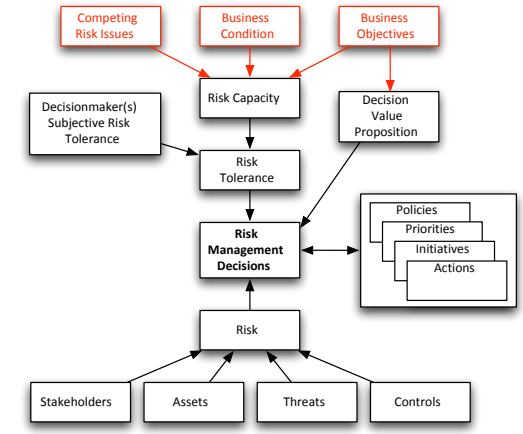
Risk Tolerance (**Figure 4**) has two contributing factors, Risk Capacity and the Decision-maker's Subjective Risk Tolerance. We'll cover risk capacity in the next paragraph, but it's important to recognize that subjective risk tolerance is unique to every individual. Furthermore, our individual tolerance for loss varies depending on the type of loss. For example, I may have a very low tolerance for financial loss, but be entirely willing to take up skydiving. As a result, risk decisions within an organization must reflect the risk tolerance of executive management regardless of whether security or someone else is empowered to make the decision. This is crucial in order to ensure management support.

Figure 4



Risk capacity (**Figure 5**) also has three inputs: the organization's current condition relative to its objectives, as well as the portfolio of competing risk issues. It's important to recognize, too, that these factors will often vary across the different types of loss (e.g., productivity, competitive advantage, resources, reputation, etc.). For example, an organization that has a significant stockpile of resources will have more capacity for resource loss than will an organization that operates on a shoestring. Likewise, an organization that is trying to build market share will have less capacity for reputation damage than will one that already leads the competition, has a very loyal customer base, or where a barrier to exit/change exists for its customer base. The point is, capacity will vary not only between organizations but also between types of loss within an organization.

Figure 5



With regard to competing risk issues, it's important to keep in mind that information-related risk is only one of many risk domains management has to deal with (e.g., market, insurance, investment, etc.). Combine this with complex organizational conditions and objectives, as well as limited resources, and it becomes clear how important (and difficult) it is to strike the right balance in applying risk management resources.

Available Resources and Capabilities (**Figure 6**) help to drive which risk management options (the 4th risk decision input referred to earlier) are feasible. These resources, of course, are dependent on the organization's condition. Note, too, that resources and capabilities can affect risk tolerance, as an organization with fewer resources for mitigating risk may be forced to accept more risk if, for example, a decision's value proposition is particularly compelling.

Figure 6

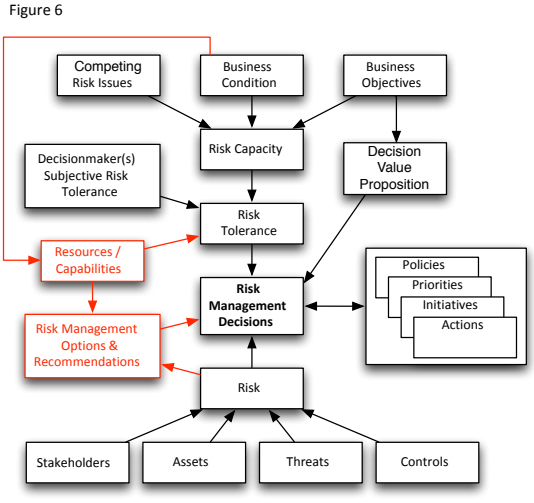
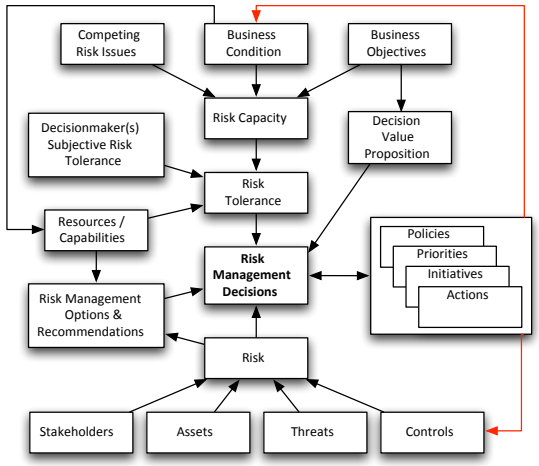


Figure 7



And finally (**Figure 7**), the policies, priorities, initiatives, and actions that result from risk decisions will have an effect on risk and the organization's condition (for good or ill). At the very least, expenditures made to manage information risk are no longer available to use on competing risk issues and opportunities.

Note, too, that this is where critical feedback occurs (or should occur) to decision makers regarding the effect risk decisions have on the risk condition as well as the business condition.

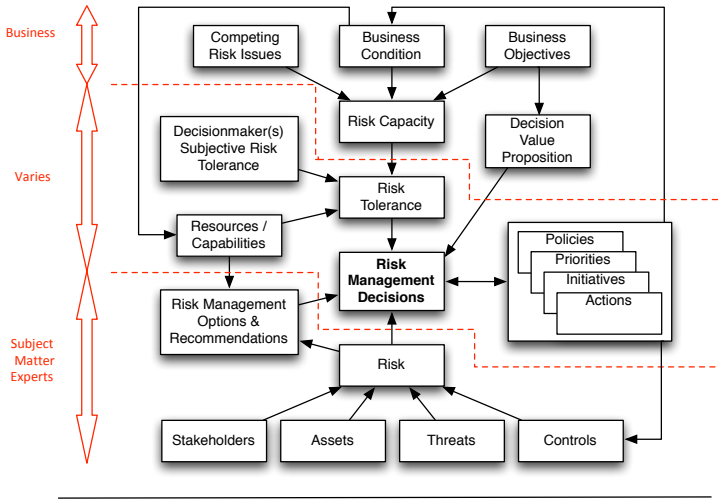
Carving it up

Using this illustration of the risk decision elements we can draw lines that carve the landscape into three parts (**Figure 8**) –

- Those elements that would appear to belong to business management,
- Those elements that would appear to belong to the subject matter experts, and
- Those elements in the middle that could go either way

Note that the decision element itself falls into the "could go either way" domain, which means there isn't always a definitive, "*This is how it should be*" answer.

Figure 8



Size matters

Of course what I mean is that the size (significance) of the risk decision also determines who can/should/will make the decision. Business management isn't usually going to be involved in day-to-day operational information risk decisions. Furthermore, security management can't personally be involved in each discrete risk decision that takes place throughout the organization.

At the end of the day, decision significance is a continuum rather than a binary or clearly differentiated scale. Consequently, some decisions fall into a grey area regarding who should make what call. For these issues, the question of who should make the decision will vary from organization to organization. An organization can, however, come up with some ground rules, for example; policies, policy exceptions, strategic initiatives, and significant expenditures fall into business management's court, and security management deals with the rest.

Other influences

Another critical issue many organizations wrestle with today is the effect of laws and regulations on information security. Laws and regulations don't (primarily) exist to protect organizations - they exist to protect consumers, investors, and/or the community at large. Consequently, rather than business management's risk tolerance, the government or other regulating entity (e.g., PCI) sets the risk tolerance.

Obviously, this can grate on management's nerves if the risk tolerance set by laws and regulations differs significantly from their own. It gets even more problematic if the laws and regulations are highly proscriptive, because management then not only has to meet a risk tolerance that isn't theirs, they also have to meet it in a way that may not be cost-effective or even feasible given their resources or other practical constraints.

Summing it up

The simple fact is, security leadership will never know as much about the business-related elements at the top of the illustration, and business management will never know as much about the risk elements at the bottom. Consequently, if security is empowered to make the major decisions, then they need to spend the time and effort to learn as much as they can about the business-related elements (including executive management's risk tolerances). On the other hand, if business leadership is making the major risk decisions, then security must provide clear, unbiased, and useful information about risk and risk management options so that decisions are well informed.

Regardless of how an organization structures its risk decision-making, it's critical that all stakeholders have a clear understanding of their roles and responsibilities. This risk decision illustration can be useful in facilitating that understanding.

About the author

Jack Jones has worked in technology for over 30 years, the past 25 in information security and risk management. He has a decade of experience as a Chief Information Security Officer (CISO) with three different companies, including a Fortune 100 financial services company. His work while at Nationwide Insurance was recognized in 2006 when he received the Information Systems Security Association (ISSA) Excellence in the Field of Security Practices award. In 2007, he was selected as a finalist for the Information Security Executive of the Year, Central United States, and in 2012, he was honored with the CSO Compass Award for leadership in risk management.

Jones currently holds the CRISC, CISM, CISA, and CISSP certifications and serves on the ISACA CRISC Certification Committee and the ISC2 Ethics Committee, and is the President and Co-founder of RiskLens.

He the author and creator of the Factor Analysis of Information Risk (FAIR) framework. He writes about that system his recently-released book Measuring and Managing Information Risk: A FAIR Approach.