Outcomes of Risk Management

Table of Contents

Risk Management in a Nutshell ...................................................................................................... 2
Outcomes of Risk Management...................................................................................................... 3
Summary ......................................................................................................................................... 5
Notices ............................................................................................................................................ 9
**022 Risk management in a nutshell, this is the process that you'll follow. You're basically going to start with identifying the assets, the threats, and the vulnerabilities. Here is part of your risk assessment. Then you're going to start thinking about what's most likely to happen to me. What are the threat scenarios? Then I'm going to start coming up with risk mitigation plan. So, down here at the bottom, I'm looking for how do I address these risks. What do I do about them? And then, monitoring, reviewing, assessing, evaluating, the whole notion of if I create this plan, I can't just leave it on the shelf. So, I want to do something with it.
Outcomes of Risk Management

Outcomes of Risk Management

An understanding of

- The organization’s threat, vulnerability and risk profile
- Risk exposure
- Potential consequences of compromise
  - Awareness of risk management priorities based on potential consequences

A risk mitigation strategy sufficient to achieve an acceptable level of residual risk

Organizational acceptance/deference based on an understanding of potential consequences of residual risk

Integration as “business as usual”

**023 Outcomes of risk management, what should you get out of this process?**
Well, the first thing that you should get is an understanding of what could go wrong with my organization. I’m looking for the threats, the vulnerabilities, what’s my risk exposure, what are the potential-- what are the outcomes of a realized vulnerability or a realized risk.

The next thing that I should get out of this process is a risk mitigation strategy, meaning how am I going to do something about this. I understand I have potential problems. I understand that something could go wrong. Well, with risk mitigation, what do I do about it? How do I address that particular risk?
Then you're going to worry about-- or one of the other outcomes you're going to get is organizational acceptance or deferring risk. So, you understand what the risk is. You've done something about it. Now, your organization goes I'm going to live with the fact that there's risk here. I have to. I have to accept it because I can't get rid of it.

And then the last point up here, integration as business as usual, you shouldn't view risk management as a process that happens over here, somewhere over there. Bob in the risk management office is doing a risk management plan. Great, just don't worry about Bob. He's over there. He'll-- two years from now, he'll spit out this process, and we'll have a risk management plan. It can't work that way. It has to be part of your business. It has to be ingrained in what you do, otherwise it won't be effective.
**024 So, what I wanted to do here is let’s take a look at understanding a notional company.

So, we are in charge of the Princess Pizza Company. And it is our mission in life to serve the tastiest non-cardboard looking pizza that we can. And we have a couple stores, but it’s really just a small business.

What would our business actually look like? Remember the diagram that we did earlier showing the tiers of risk management? Well, let’s kind of draw the same sort of thing for our pizza company here.
So, at the top level, tier one of risk management is focused on what? Strategy, right? So, I have up here company strategy. And at this level, I would be concerned about what sorts of things? At a very high level from the strategy perspective of the company, what am I really worried about?

Well, I think there are a couple of things we can just brainstorm really quick. I might be worried about things like reputation.

Student: Money.

Chris Evans: I'm sorry?

Student: Money, making money.

Chris Evans: Yep, absolutely. We want-- I'll throw in an extra one because we want to make lots of money.

Student: Competitors.

Chris Evans: Competitors, that's a great one.

Student: Good pizza.

Chris Evans: Yep. Yep, all the things that should be reflected in our vision statement for the company or the mission statement for the company. Yep. Actually there's another one here, growth of the company.

So, risk management from this perspective is going to focus on these types of things. Have we done anything about how do I keep a fire from burning down a store? How do I keep my people
from eating the pizza before they actually
deliver it and cutting into my profits? It
could be a legitimate strategy. Well, we
haven't actually addressed those, right,
because we haven't gone through and
said what are the functions or what are
the processes of the company.

So, at this point, what sorts of things
could we do as a pizza company? I think
for simplicity we ought to pick two and just
say at a really notional level, we do two
things. We make pizza. And we deliver
pizza. Right. Now, I know this is
extremely simplistic. However, what you'll
see with this is as we develop this
example, and we'll use it throughout the
discussions, you'll see that with any
regular business where you have so
many different functions, the risk
management process get huge. It's-- this
is not a trivial task. This is also another
reason why you have the tiered risk
management. So, you've got somebody
focusing on what to do here. You have
somebody focusing on the delivering the
pizza process. You have somebody
focusing on the making the pizza process.

So, there's probably one other area in
here. And I think it's probably a kind of a
cross area. It kind of crosses between the
two. And that's the order system. So,
somewhere in here I have to be able to
take orders from-- I apologize for the
handwriting. I know it's terrible. I've lost
the ability to write by hand. I type
everything. So, at some point in here, you
need to have the ability to take orders
from customers, turn that order into a
ticket, which goes to the make pizza
people, and an address that goes to the
delivery crew.
Student: That could be very sophisticated. It could be whether you just take it by phone or that over the computer, as well. Same with the delivery, some places only have a few-- you pick up yourself. Others, they do the delivery. So, that could be a lot different directions.

Chris Evans: Now, it's actually good that you mention that. It's getting a little bit ahead in the risk management process here. But what you're starting to think of is what do we actually have in the order system that is critical or necessary for the-- for us to take orders? Do we have an Android app? Do we have a website? Oh crap, do we take credit cards? Now, soon as I mention credit cards, there are twenty other different things that go in here that are important to me.

But let's focus on kind of the make pizza here and the order system. Excuse me. So, if these are our functional areas with strategy and making pizza and delivering pizza, we can start looking at things that are required for this. So, start thinking about what do I actually need to make pizza. What does that process look like? What are the people, the information, the technologies, the facilities, what sorts of things go into making pizza? How does making pizza interact with the ordering system? How does the making pizza interact with the delivery function? What are the dependencies between the two?

So, just based on this little framework we have here, you're going to start thinking about what happens in this process. What do I need to make that process happen? And then you'll start thinking about what can go wrong with it and what are the
risks from it. And if it does go wrong, how does that affect the business? And so, we'll come back to this example when we start talking about those particular functions.

Any questions on the risk management process? Okay.

**Notices**

© 2014 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Altimate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN “AS IS” BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.