

Risk Management - It's Risky Business, but That's a Good Thing

March 27, 2014

1-2:30 p.m. (EDT)

Presenters

- **Mark Nunn**, Air Force Risk Management Program Manager
- **Dave Marciniak**, General Services Administration Safety and Health Manager
- **Chris Toms**, Coast Guard Senior Risk Management and Operations Research Analyst

Summary

Facilitator: Mike Lipka, Knowledge Officer, NASA Safety Center

Attendees: 103 (approximately)

Purpose of the Safety and Health Learning Alliance: Share experiences and collaborate ideas across various government and defense agencies, related industries, and professional organizations for the mutual goal of achieving high levels of safety and health.

Goal: Increase involvement, communication, and participation among safety and health professionals.

The [SHLA website](#) includes a video of the presentation. Please submit questions, comments, and event recommendations on the website or by emailing NASA-NSC@nasa.gov.

Questions

Round 1: What risk management tools do you use?

Nunn

We have a high level view of risk management—most of the programs and tools are expected to be used as a starting point for commanders and local agencies for developing their own personalized tools. One of the most common tool we use is the risk assessment matrix tools. We also look at exposure, severity, probability, but because of our military operations, we're not in a consistent mode all the time.

We don't limit our agencies to use one particular matrix due to the inherent differences in acquisition, test and evaluation, and operations. We have numerous programs to deal with mitigation, survey, data, analysis, and self recording type tools. We have a database repository of all our mishap investigations; data collection for risk management, risk factor, and causal factors; and trend analysis for future operations. We can't create guidance for every single operation the airframe does. We create a framework for others to modify it and use it at a lower level. This framework also requires adequate assessment of risk in relation to the danger and importance of certain operations.

With multiple weapons systems within the Air Force, separate units will modify assessment sheets for their particular situation. The big problem we face is standardization even between squadrons of a certain types of aircraft flying out of the same airbase with the same mission having different sheets. We're coordinating with other services on creating a web-based joint risk assessment tool.

Marciniak

We are fundamentally a real estate organization that provides space to federal tenants. As far as tools, we use a consolidated environmental health and safety survey on all of our buildings, which includes a baseline and an update every 5 years or sooner if the building is higher risk. It's not an occupational safety and health type evaluations, it's an owner operator risk survey of a building in its operation. We are addressing risk, but we have to make sure we cover the safety and environmental regulations.

These surveys address to help prioritize our investments. Historically, we've looked at physical things and processes, but we're shifting to an asset risk management approach based on the insurance industry and their loss protection approach (i.e., looking at facility conditions, but also recording attributes, such as location, purpose, and loss history).

What we use guidelines for loss control engineer and underwriters to identify typical hazards of a given type and give a number value to each of the risks. We use a 4x4 matrix, moving towards to 5x5. We're developing checklists for the surveys and a database with two groups—subjects and occupancies—and we match these subject matter issues to the occupancy so the surveyor can go through and address these minimum areas. We don't have a lot of loss data because losses don't happen often.

What we do with all of this info, is use a safety based inventory reporting system, which belongs to the facility people, which they use to put issues in for repair or for capital improvements. We're just one module within this system, but since we're integrated in it, resulting in more guidance for things getting fixed in the short term or remedying deficiencies in our projects

When buildings are broken down by subsystem, we can use a standardized statement of work (whether we use one of our people in house or contract out the work). We haven't yet figured out how to take the attributes and the losses to sum up all the risks. What we try to do instead of having separate surveys for fire or safety, is to have a combined survey and eventually become part of a larger survey that would include with the facility investigative people who do physical condition surveys. We should be part of that to be incorporated into what the core business function is.

We're starting to get into the point where we can go into their prioritizations system for repair alternations and long term asset planning.

Toms

The Coast Guard is mandated by the Department of Homeland Security to complete enterprise risk management—to assess risk from every aspect of the organization, from personal risk to mission support to procurement risks. However, I'll be speaking to operational risk at the strategic level.

The Coast Guard constantly reviews with academia and private consultants to analyze risk. Topics reviewed include game theory, different types of multi criteria decision analysis, and large scale optimization network analysis. We're trying to push the boundaries of risk assessment. Our main risk assessment currently is probabilistic risk assessments, which fall between threat vulnerability consequence functions or frequency in consequence functions.

We have many missions (involving fishery protection, ice breaking, and polar operations) with many outcomes we're trying to protect the public against. Any outcomes that could create societal loss, we try to minimize, including death and injuries, economic loss, and loss of maritime mobility.

Round 2: How does your organization accept risk?

- **How do you define acceptable risk?**
- **Who can accept the risk?**
- **Who owns the risk?**
- **Who tracks the risks?**

Nunn

Acceptable risk depends on the Air Force view on what is trying to be accomplished—leadership is key to that decision making process, and commanders are responsible for establishing the levels of risk within their operations. They can dictate that aircrews can accept risk up to a certain level. Some of those risk decisions can go quite far up the ladder. Once you've established that criteria, not only your commanders need to understand the rule, the crews need to understand what the risk tolerance is.

Beyond that, documentation is required to explain why you chose to take the risk or modify your acceptance level of risk for a given operation. Leadership gives the options, and if you can't get the risk factor down, you can either accept the risk or back off. Understanding the roles and values are key to success there. We try to instill this understanding in all levels.

Our off duty mishap rates far exceed our on duty mishap rates, so we're trying to make inroads to manage that risk and to mitigate that.

We are constantly (armed forces) redefining our risks. Evaluating those risks on the fly is extremely difficult. Communication wise, if you are encountering higher risks than anticipated, we ask for a go or a no-go. If the decision isn't time critical, we send those evaluations back up and request acceptance from superiors. Kicking risk decision making up the ladder is not uncommon in the armed forces. If we can't mitigate a risk at our level, we escalate it to a higher decision maker.

Toms

The Department of Homeland Security uses risk management fundamentals and it defines the risk management cycle. Simply put, you don't have any risks if you don't have any goals. There has to be some kind of goal or outcome. You have to analyze where those goals are going or to who the owner is and analyze how successful we will be in reaching those goals. At some level, there are overarching risks are defined at the administration level,

but for the more specific risks, commanders take ownership. Risks are always futuristic or potential probabilities. Tracking the changes of these probabilities is difficult.

Marciniak

The EHS officers track it, we usually only track the high end Rack 1 risks until they are either eliminated or have interim controls applied. We define risk and track it, but as far as owning it or accepting it, it goes to the property managers or the program/project managers.

Round 3: How is risk is communicated up the management chain?

- **How does your organization get risk management buy-in and participation?**
- **What type of documentation is required?**
- **What is the overall flow?**
- **Who has decision making authority/responsibility?**

Toms

There is a Department of Homeland Security risk lexicon, which helps communicate risk inside a department, but it is difficult to communicate risk up a chain.

The coast guard operates in a risk environment, and is used to take care of these risks. We handle as much as we can, but we communicate to our superiors anything we cannot handle. With so many risk scenarios, it's difficult to handle things we cannot predict.

In talking about multiple impacts to society, it's hard to trust the risk output to society. The buy in comes from the management of the coast guard and what they're doing to minimize societal loss.

Round 4: What are the key components of your risk training?

- **What have been the results of your risk training?**
- **Is it working for your organization?**
- **What part of your training program has made the biggest impact on risk management?**

Nunn

Our primary fundamentals course is distributed for the Air Force training website. It uses a process we took from the Navy and is required for all Air Force personnel and civil service workers (and some of our contractor workforce).

Our expert level course is for half level process managers. We also require one wing instructor be formally appointing to take the expert level course which goes into a lot more detail on how we go through conducting formal risk acceptance and defining hazards.

When we get into period briefings and presentations, we go to commanders and separate units and ask them to look at their local on and off duty operations and issues and have them create briefings on the issues and strategies they apply. This gets risk management back into the hands of the commanders and the people involved and has them look at what is really going on for and around them.

We don't specify times, we schedule them any time that they have downtime available for it.

It's about getting everybody involved in risk management, not just the leaders.

Final Key Points from Panelists

➤ **If people were to remember one thing about safety culture, it should be _____.**

Nunn

We're always worrying about risk management lower than us instead of up or sideways.

We've found that with the better technology we have, the more we've driving our mishaps down, but not on our off duty side. So we took off the operational part and now we need to emphasize it on both our on and off duty side. We statically lose about 10 people off duty to every 1 on duty. We look at risk from a personal standpoint, but we need to be watching out for the other guy—a common theme among armed forces guys. By keeping the people next to you alive, you're contributing to the overarching mission.

We need senior leadership involved in pressing risk management.

Toms

Risk management should be ubiquitous. Risk management manifests itself in everyday choices, all the way up to the most large scale organizational decisions. It's the decision support framework of trading off the investment you're willing to put forward versus the consequences that will take place either positive or negative.

Risk ignored is not disappeared risk. You have to manage it.

Marciniak

A year ago we were the environmental health and safety management division, and now we're the risk management division. How does this differ? If we need to deliver a building to you and that building needed an emergency generator, the fire safety guy would ask, "How do we protect that generator?" The environmental guy would ask, "How do we contain this is we have a spill?" The health guy would ask "How do we protect those confined spaces?" The risk manager doesn't get involved in the design review, but at the conceptual phase. They ask questions like, "Why are we using diesel?"

We're up front, proactive, and looking at alternatives before we get locked in.