

Everyone's Smart University

Project (Spring 2021)

Student Name	أحمد فهد أحمد آل شامر القحطاني	اسم الطالب
Students I.D	2021203241	الرقم الجامعي

Section

Master

Date

Thursday

18/03/2021

Course Code

(PMG506)

Definitions:

A Risk is:

An uncertain or potential future event or condition that, if it occurs, will have a positive or negative effect on a project's objectives.

A Risk is not:

- An Issue (i.e. has already happened).
- A Constraint or Assumption.
- An unexpected construction condition that is already covered by the project's Reserve or Contingency funds policy.

Project Risk Event

A discrete occurrence of a Project Risk that has impacted the project for better or worse.

Project Risk Management

The systematic process of identifying, analyzing, and responding to project risks, either in the present or through developing contingency plans that can be quickly implemented if the risk event occurs.

Risk Probability:

An estimate of the likelihood that a given risk event will occur.

NOTE: if the probability of a risk event is 100 %, it is no longer uncertain and is no longer a risk event. It is now an issue or a constraint.

Risk Impact:

An estimate of the gain or loss that will be incurred if a risk event occurs, also called consequences or results.

Risk Severity:

A numerical scoring of a risk (obtained by multiplying the risk probability and the risk impact together).

risk Management Process

The risk management process is a framework for the actions that need to be taken. There are five basic steps that are taken to manage risk; these steps are referred to as the risk management process. It begins with identifying risks, goes on to analyze risks, then the risk is prioritized, a solution is implemented, and finally, the risk is monitored. In manual systems, each step involves a lot of documentation and administration. Now let's look at how these steps are carried out in a more digital environment.

Step 1: Identify the Risk

The first step is to identify the risks that the business is exposed to in its operating environment. There are many different types of risks – legal risks, environmental risks, market risks, regulatory risks, and much more. It is important to identify as many of these risk factors as possible. In a manual environment, these risks are noted down manually. If the organization has a risk management solution employed all this information is inserted directly into the system. The advantage of this approach is that these risks are now visible to every stakeholder in the organization with access to the system. Instead of this vital information being locked away in a report which has to be requested via email, anyone who wants to see which risks have been identified can access the information in the risk management system.

See [Five Steps Towards a Better Risk Management Framework](#)



Step 2: Analyze the Risk

Once a risk has been identified it needs to be analyzed. The scope of the risk must be determined. It is also important to understand the link between the risk and different factors within the organization. To determine the severity and seriousness of the risk it is necessary to see how many business functions the risk affects. There are risks that can bring the whole business to a standstill if actualized, while there are risks that will only be minor inconveniences in the analysis. In a manual risk management environment, this analysis must be done manually. When a risk management solution is implemented one of the most important basic steps is to map risks to different documents, policies, procedures, and business processes. This means that the system will already have a mapped risk framework that will evaluate risks and let you know the far-reaching effects of each risk.

Step 3: Evaluate or Rank the Risk

Risks need to be ranked and prioritized. Most risk management solutions have different categories of risks, depending on the severity of the risk. A risk that may cause some inconvenience is rated lowly, risks that can result in catastrophic loss are rated the highest. It is important to rank risks because it allows the organization

to gain a holistic view of the risk exposure of the whole organization. The business may be vulnerable to several low-level risks, but it may not require upper management intervention. On the other hand, just one of the highest-rated risks is enough to require immediate intervention.

Go in more depth [Bringing Quantitative Risk Analysis to Enterprise Risk Management](#)

Step 4: Treat the Risk

Every risk needs to be eliminated or contained as much as possible. This is done by connecting with the experts of the field to which the risk belongs. In a manual environment, this entails contacting each and every stakeholder and then setting up meetings so everyone can talk and discuss the issues. The problem is that the discussion is broken into many different email threads, across different documents and spreadsheets, and many different phone calls. In a risk management solution, all the relevant stakeholders can be sent notifications from within the system. The discussion regarding the risk and its possible solution can take place from within the system. Upper management can also keep a close eye on the solutions being suggested and the progress being made within the system. Instead of everyone contacting each other to get updates, everyone can get updates directly from within the risk management solution.

Check our recent post: [Improving Risk and Compliance Results With Smarter Data](#)

Step 5: Monitor and Review the Risk

Not all risks can be eliminated – some risks are always present. Market risks and environmental risks are just two examples of risks that always need to be monitored. Under manual systems monitoring happens through diligent employees. These professionals must make sure that they keep a close watch on all risk factors. Under a digital environment, the risk management system monitors the entire risk framework of the organization. If any factor or risk changes, it is

immediately visible to everyone. Computers are also much better at continuously monitoring risks than people. Monitoring risks also allows your business to ensure continuity. We can tell you How you can create a risk management plan to monitor and review the risk.

The Basics of The Risk Management Process Stay the Same

Even under a digital environment, the basics of the risk management process stay the same. What changes is how efficiently these steps can be taken, and as it should be clear by now, there is simply no competition between a manual risk management system and a digital one. There are also many new risks that businesses are facing for the first time in 2019, and modern problems require modern solutions.

Risk Management Evaluation

Any business that wants to maximize its risk management efficiency needs to focus on risk management evaluations. These evaluations and assessments help businesses truly understand their own capabilities, strengths, and vulnerabilities. More evaluations result in more insights about where the business needs to improve its risk management framework. It can be difficult to carry out these evaluations manually, but risk management solutions and technology can simplify the evaluation and assessment workflow. It is important to do an evaluation before making any major changes to the risk management framework.

Risk Management

Risk management is an important business practice that helps businesses identify, evaluate, track, and improve the risk mitigation process in the business environment. Risk management is practiced by the business of all sizes; small businesses do it informally, while enterprises codify it. Businesses want to ensure stability as they grow. Managing the risks that are affecting the business is a critical part of this stability. Not knowing about the risks that can affect the business can result in losses for the organization. Being unaware of a competitive risk can result

in loss of market share, being unaware of financial risk can result in financial losses, being aware of a safety risk can result in an accident, and so on. Businesses have dedicated risk management resources; small businesses may have just one risk manager or a small team while enterprises have a risk management department. People who work in the risk management domain monitor the organization and its environment. They look at the business processes being followed within the organization and they look at the external factors which can affect the organization one way or the other. A business that can predict a risk will always be at an advantage. A business that can predict a financial risk will limit its investments and focus on strengthening its finances. A business that can assess the impact of a safety risk can devise a safe way to work which can be a major competitive advantage. If we think of the business world as a racecourse then the risks are the potholes which every business on the course must avoid if they want to win the race. Risk management is the process of identifying all the potholes, assessing their depth to understand how damaging they can be, and then preparing a strategy to avoid damages. A small pothole may simply require the business to slow down while a major pothole will require the business to avoid it completely. Knowing the severity of a risk and the probability of risk helps businesses allocate their resources effectively. If businesses understand the risks that affect them then they will know which risks need the most attention and resources and which ones the business can disregard. Risk management allows businesses to act proactively in mitigating vulnerabilities before any major damage is incurred. There are different types of risk management strategies and solutions for different types of risks.

Read also: [The Importance of Real Time Risk Appetite Tracking](#)

The Risk Management Process Model

The risk management process model (see figure 1) includes the following key activities, performed on a continuous basis:

- Risk Identification,
- Risk Analysis,
- Risk Mitigation Planning,
- Risk Mitigation Plan Implementation, and
- Risk Tracking.

Health and safety hazards and risks: Step 1: Identify the hazards

Biological (e.g. hygiene, disease, infection)			
☐ Blood/bodily fluid	☐ Virus/disease	☐ Food handling	
Other/details:			
Chemicals (note: refer to the label and safety data sheet (SDS) for the classification and management of all chemicals)			
☐ Non-hazardous chemical(s)	☐ Hazardous chemical (refer to a completed hazardous chemical risk assessment)		
Name of chemical(s)/details:			
Critical incident – resulting in:			
☐ Lockdown	☐ Evacuation	☐ Disruption	
Other/details:			
Energy systems – incident/issues involving:			
☐ Electricity (incl. mains and solar)	☐ LPG gas	☐ Gas/pressurised containers	
Other/details:			
Environment			
☐ Sun exposure	☐ Water (creek, river, beach, dam)	☐ Sound/noise	
☐ Animals/insects	☐ Storms/weather	☐ Temperature (heat, cold)	
Other/details:			
Facilities/built environment			
☐ Buildings and fixtures	☐ Driveway/paths	☐ Workshops/work rooms	
☐ Playground equipment	☐ Furniture	☐ Swimming pool	
Others/details:			
Machinery, plant and equipment			
☐ Machinery (fixed plant)	☐ Machinery (portable)	☐ Hand tools	☐ Vehicles/trailers
Other/details:			
Manual tasks/ergonomics			
☐ Manual tasks (repetitive, heavy)	☐ Working at heights	☐ Restricted space	
Other/details:			
People			
☐ Students	☐ Staff	☐ Parents/others	
☐ Physical	☐ Psychological/stress		
Other/details:			
Other hazards/details:			

Step 2: Assess the level of risk.

Consider the hazards identified in Step One and use the risk assessment matrix below as a guide to assess the risk level.

DoE Risk Management Matrix					
Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Critical
Almost certain	Medium	Medium	High	Extreme	Extreme
Likely	Low	Medium	High	High	Extreme
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Low	Medium

Consequence	Description of consequence
1. Insignificant	No treatment required.
2. Minor	Minor injury requiring first aid treatment (e.g. minor cuts, bruises, bumps).
3. Moderate	Injury requiring medical treatment or lost time.
4. Major	Serious injury (injuries) requiring specialist medical treatment or hospitalization.
5. Critical	Loss of life, permanent disability, or multiple serious injuries.

Likelihood	Description of likelihood
1. Rare	Will only occur in exceptional circumstances.
2. Unlikely	Not likely to occur within the foreseeable future, or within the project lifecycle.
3. Possible	May occur within the foreseeable future, or within the project lifecycle.
4. Likely	Likely to occur within the foreseeable future, or within the project lifecycle.
5. Almost certain	Almost certain to occur within the foreseeable future or within the project lifecycle.

Assessed risk level		Description of risk level	Actions
☐	Low	If an incident were to occur, there would be little likelihood that an injury would result.	Undertake the activity with the existing controls in place.
☐	Medium	If an incident were to occur, there would be some chance that an injury requiring first aid would result.	Additional controls may be needed.
☐	High	If an incident were to occur, it would be likely that an injury requiring medical treatment would result.	Controls will need to be in place before the activity is undertaken.
☐	Extreme	If an incident were to occur, it would be likely that a permanent, debilitating injury or death would result.	Consider alternatives to doing the activity. Significant control measures will need to be implemented to ensure safety.

Step 3: Control the risk

In the table below:

1. List the hazards/risks you identified in Step One.
2. Rate their risk level (refer to information contained in Step two to assist with this)
3. Detail the control measures you will implement to eliminate or minimise the risk.

Note: control measures should be implemented in accordance with the preferred **hierarchy of control**. If lower level controls (such as administration or PPE) are to be implemented without higher level controls, it is important the reasons are explained.

Hierarchy of controls	
Most effective (High level)  Least effective (Low level)	Elimination: remove the hazard completely from the workplace or activity.
	Substitution: replace a hazard with a less dangerous one.
	Redesign: changing a machine or work process to make it safer.
	Isolation: separate people from the source of the hazard.
	Administration: putting rules, signage or training in place to make a workplace safer.
	Personal protective equipment (PPE): protective clothing and equipment.

the Equipment/Process Risk Matrix

Below are the details of the manufacturing or production processes attributed to this item of equipment categorized by their assessed inherent risk levels (refer to the Equipment/Process Risk Matrix). The actions required for approval for each level of inherent risk are mandatory.

Inherent Risk Level		Details of Processes	Action Required/Approval
☒	Medium	- When spindle turning – parallel, taper or profile turning between a drive centre and the tail stock. - When spindle turning with the grain of the timber parallel to the lathe bed – and when the material to be turned is free of splits, cracks, loose knots or other defects. - When the spindle speed relative to the diameter of the material has been adjusted – and the tool rest has been correct adjusted and clamped securely. - When free hand sanding (with the tool rest removed) and when using appropriately sized sanding materials not likely to become entangled.	☒ Document controls in planning documents and/or complete this <i>Plant Risk Assessment</i>. ☒ Consider obtaining parental permission.
☒	High	- When rough turning larger, irregular or unbalanced stock. - When face plate or bowl turning. - When off-centre face plate turning. - When face-grain turning (chip-out is likely) - When turning green, unseasoned timber. - When drilling or boring from the tail stock.	☒ A Plant Risk Assessment is required to be completed. ☒ Principal or Classified Officer (i.e. DP, HOD, HOC, HOSES) approval prior to conducting this activity is required. ☒ Obtaining parental permission is recommended.

Previous studies of risk management:

DSMC Risk Management Guide for DoD Acquisition, February 2001

This DSMC guidebook provides acquisition professionals and program managers with a reference for dealing with system acquisition risks. The guide takes the reader from an introduction to basic risk management concepts through implementation and techniques that address the aspects of risk management.

AFMC Pamphlet 63-101: Acquisition Risk Management (ARM), 9 July 1997

This document describes the process and methods AFMC uses for managing program risk, proposal risk and performance risk. The guide also describes processes for establishing the impact of cost and schedule risk. The AFMC risk management processes can be used and adapted to meet the needs of any program.

DoD 5000.2-R: Recommended Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs, 10 June 2001

This Regulation is issued under the authority of Department of Defense (DoD) Instruction 5000.2, "Operation of the Defense Acquisition System," October 23, 2000 and is effective immediately. This Regulation sets forth mandatory procedures for MDAPs and MAIS acquisition programs; serves as a general model for other acquisition programs; implements DoD Instruction 5000.2, the guidelines of Office of Management and Budget (OMB) Circular A-11, and current statutes; and contains formats to be used to prepare various milestone documentation, periodic in-phase status reports, and statutory certifications

AF Instruction 90-901: Operational Risk Management, 1 April 2000

This instruction establishes the requirement to integrate and sustain operational risk management (ORM) throughout the Air Force. It assigns responsibilities for program elements and contains program management information. HQ Air Force staffs, major commands (MAJCOMs), direct reporting units (DRUs) and field operating agencies (FOAs) are responsible for establishing and sustaining their respective programs according to the program elements described in this instruction. It applies to all Air Force personnel and functional areas, including the Air Force Reserve and Air National

Guard. Do not supplement this instruction without prior review by the Air Force Chief of Safety (AF/SE).

AF Policy Direction 90-9, 1 April 2000

This directive establishes the Air Force Operational Risk Management (ORM) Program. The management of risk, all dimensions of risk, is key to maximizing mission effectiveness and sustainment of readiness. ORM principles, techniques, and tools will be used to increase mission success, strengthen job performance, and identify opportunities to expand mission capabilities in all areas and at all levels, thereby strengthening the Air Force's warfighting posture.

References

1. Garvey, Paul R.; "Risk Management", *Encyclopedia of Electrical and Electronics Engineering*, John Wiley & Sons, Inc., 1999; www.interscience.wiley.com:83/eeee/.
2. Garvey, Paul R.; *Probability Methods for Cost Uncertainty Analysis: A Systems Engineering Perspective*, Marcel Dekker, Inc., 270 Madison Avenue, New York, NY, 10016-0602, January, 2000; ISBN: 0824789660; www.dekker.com/e/p.pl/8966-0.
3. Garvey, Paul R., Phair, Douglas J., Wilson, John A.; "An Information Technology Architecture for Risk Assessment and Management", *IEEE Software*, May, 1997; www.computer.org/software/so1997/s3toc.htm.
4. Cho, C. C., Garvey, Paul R., Giallombardo, Robert J.; "RiskNav™: A Decision Aid for Prioritizing, Displaying, and Tracking Program Risk", *Military Operations Research*, V3, N2, 1997; www.mors.org.
5. Garvey, Paul R., Lansdowne, Zachary F.; "Risk Matrix: An Approach for Identifying, Assessing, and Ranking Program Risks", *Air Force Journal of Logistics*, Volume XXII, Number 1, June 1998; www.mitre.org/resources/centers/sepo/risk/risk_matrix.html.