

Risk Management

Prepared by Dr. Dalia Hosni

Lecture5



MGM 510

Risk Management



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Risk Response Strategy is an action plan on what you will do a Risk on your project.

The main risk response strategies for threats are Mitigate, Avoid, Transfer, Actively Accept, Passively Accept, and Escalate a Risk.

Plan Risk Responses

Quick Quiz: Look at the next table and see if you can quickly identify what type of risk response strategy is being employed in each situation:

QUIZ!

Plan Risk Responses

Risk Description	Response Strategy?
There is a risk your lead architect may leave the project before her job is completed. As a result you cross-trained one of the developers to handle lead architect responsibility	mitigate
The database for your software project is expected to run into multiple terabytes. After consulting with the infrastructure team you discover there are terabytes of available storage in the data center that can be secured at a much lower cost than purchasing new equipment.	exploit
An out-of-state vendor on your project has expressed concerns about meeting delivery due dates. You engage a local vendor that can easily meet the delivery dates without issue.	Avoid
Staffing up for customer service on your project will take too long and be too expensive. You identify a vendor that will exceed your customer service requirements and will pay penalties if their service falls below stated quality levels.	transfer,



Risk Register Updates

The risk register is completed at this point and can include:

- ☐ Identified risks and descriptions
- ☐ Triggers
- ☐ Response strategy
- ☐ Specific actions taken if risk occurs

تحديد المخاطر
ووصفها

المحفزات

إستراتيجية
الإستجابة

إتخاذ إجراءات
محدده في حالة
حدوث مخاطر



Lecture 5

Risk Register Updates Sample

INFORMATION SECURITY RISK REGISTER

Company: Cyber Kuryber
Risk Register #: 2022-ITS
Last Change: 05-06-2022

IT SECURITY MANAGER:
Gordon Thyess

RISK DESCRIPTION	DATE ADDED	LIKELIHOOD	IMPACT	RESPONSIBLE	MITIGATION STRATEGY	CLOSURE DATE
RISK # 1						
Not all workstations have backup	5/5/2022	HIGH	LOW	B.Braner	Make all workstations backup within one month period	6/5/2022
RISK # 2						
Unmanaged workstations in inventory	5/5/2022	HIGH	MEDIUM	J.Doe	Organize inventory check	

محطات العمل
غير المدارة في
المخزون



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

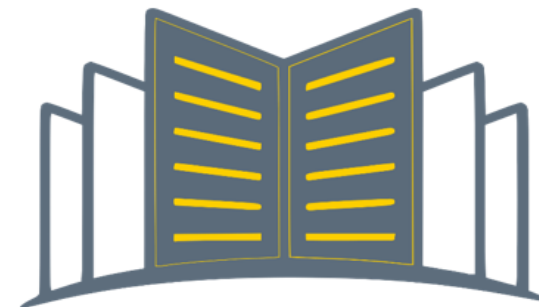
Lecture 5

Risk Register Updates Sample

Members of the internal audit committee:

Anastasia Worowchuk	Leader
John Doe	Deputy
Mila Lloyd	Member
Barbara Ford	Recorder

INTERNAL AUDIT RISK REGISTER



Date: 5/17/2022

Risk #	Description	Probability	Impact	Risk Score	Mitigation	Responsible Person
1	Code of Procurement not followed	3	4	12	Perform trainings - quarterly	Julia Mason / Procurement
2	Collection of household waste	7	2	14	Emails with reminders. Leaflets on main building door.	Peter Orban / HR
3	Civil emergency	1	8	8	Revision of emergency plan	Harry Gallagher / Security Officer
4						
5						
6						
7						
8						
9						
10						
11						

Lecture 5

Risk Register Updates Sample



MARKETING RISK REGISTER

#	RISK DESCRIPTION	POTENTIAL IMPACTS	LIKELIHOOD	RISK SCORE
R1	Third party service providers are not managed correctly because of lack of communication, trust, transparency, and formal contract.	Financial costs (estimate up to \$100,000, poor service standards.	3	9
DATE			IMPACT	
10/21/2022			3	LOW
STATUS	CONTROLS APPLIED		R. LIKELIHOOD	RESIDUAL RISK
In Process	Clear terms of reference for any new project		1	2
CLOSURE	Sign-off all new projects		RES. IMPACT	
	Use of single select list for services		2	VERY LOW
#	RISK DESCRIPTION	POTENTIAL IMPACTS	LIKELIHOOD	RISK SCORE
R2	Lorem Ipsum	Lorem Ipsum	4	20
DATE			IMPACT	
10/21/2022			5	SIGNIFICANT
STATUS	CONTROLS APPLIED		R. LIKELIHOOD	RESIDUAL RISK
Finished	Lorem ipsum dolor sit amet, consectetur adipiscing elit.		2	10
CLOSURE			RES. IMPACT	
10/25/2022			5	MEDIUM
#	RISK DESCRIPTION	POTENTIAL IMPACTS	LIKELIHOOD	RISK SCORE
DATE			IMPACT	
STATUS	CONTROLS APPLIED		R. LIKELIHOOD	RESIDUAL RISK
CLOSURE			RES. IMPACT	
#	RISK DESCRIPTION	POTENTIAL IMPACTS	LIKELIHOOD	RISK SCORE
DATE			IMPACT	
STATUS	CONTROLS APPLIED		R. LIKELIHOOD	RESIDUAL RISK
CLOSURE			RES. IMPACT	



Risk Register Updates Sample



PROJECT RISK REGISTER

PROJECT NAME: M65 LABELLING MACHINE PROTOTYPE	PROJECT #: M65-2022	PROJECT VALUE:
CLIENT NAME: HERRMA LTD	START DATE: 01/04/2022	\$125,000.00
PROJECT MANAGER: JOHN DOE	END DATE: 01/12/2022	

DATE	#	RISK DETECTED	PROJECT IMPACT	CATEGORY	RISK RATING	RESPONSIBLE	STATUS	CLOSURE DATE
4/5/2022	R000	Chip manufacturing worldwide crisis	Electronic boards delay - more than 3 weeks	Supplies	HIGH	John Richardson	Ongoing	
4/9/2022	R001	Emergency equipment renovation	Closing offices for 2 days - delay	Infrastructure	MEDIUM	Isabella Grey	Finished	04/14/2022
4/10/2022	R002	Additional permits related to RoHS	Not able to deliver products w/o certificate	Permits	HIGH	John Forester	Not Started	



Here are the most important elements to include in your risk register template

- **Risk Category**

Here, you categorize the risks you come up with. Some common categories include time, resources, environmental, scope, and cost. Using categories allows you to think of the likeliest risks which may occur and group them together for your reference.

- **Risk Description**

This refers to a short description of each of the risks. It's important to include this so anyone else who reads your project risk register template knows what each risk is all about.

Here are the most important elements to include in your risk register template

- **Risk ID**

This refers to a unique ID number you use to identify and to keep track of the information in your template. Assigning Risk IDs allows you to find them easily when the situation arises.

Here are the most important elements to include in your risk register template

▪ **Project Impact**

For this, you provide a short description of how the risk might impact the project. Including this description allows you to determine which are the most urgent risks to deal with them several occur at the same time.

Here are the most important elements to include in your risk register template

- **Likelihood**

Come up with an estimation of the probability or likelihood that each of the risks would occur and become an issue. You can use qualitative estimations but if you have enough information, quantitative estimations work well too.

- **Consequence**

This refers to the potential impact or consequence of a particular risk if it becomes a reality. Including this information allows you and everyone else on your team to know how severe the risks are and how to deal with them

Here are the most important elements to include in your risk register template

■ Risk Rank

This is the level or the magnitude of each of the risks. You can come up with the ranking by combining the consequence and the likelihood of each risk.

$$\text{Risk} = \text{Likelihood} \times \text{Severity} \times \text{Detection}$$

الإحتمالية

الشدة

الكشف

Here are the most important elements to include in your risk register template

- **Risk Trigger**

It's also important to indicate the triggers that would signal that you need to start implementing your contingency plans. This makes it easier for you to know exactly when you must deal with the risk.

Here are the most important elements to include in your risk register template

- **Prevention Plan**

This refers to an action plan as part of your risk tracker that you create in order to prevent the occurrence of risks. It's always better to prevent issues from arising rather than having to deal with them.

▪ **Contingency Plan**

Even despite all your prevention efforts, some risks might still occur. In such cases, you must have a different action plan which you would use to address these risks when they occur. That way, your project won't have to get delayed because you don't have a plan.

▪ Risk Owner

This refers to the person you assign to manage the risk when it occurs. Make sure that each risk owner knows about the contingency plans you've created so they know exactly what to do.

▪ **Residual Risk**

This refers to the risk which remains even after you've dealt with it. In such a case, you can assign the level of risk as "Low."

What is a risk register?

A risk register is a document that is used as a risk management tool to identify potential setbacks within a project. This process aims to collectively identify, analyze, and solve risks before they become problems. While usually centered around projects, other circumstances where risk management is helpful include product launches and manufacturing.



When should you use a risk register?

There are many instances when a risk register comes in handy. Ideally, it should be used—or available for use when needed—for every project. It can be used for both small and large projects, though your risk log may look different depending on the scope and complexity of your initiative.



When should you use a risk register?

While a small project may only include basic information about the risk such as likelihood, priority, and solutions, a more complicated project may require around 10 different document fields.



When should you use a risk register?

Some risk scenarios ranked by priority could include:

- Low priority: Risks such as lack of communication and scheduling errors can leave projects open to scope creep and missed deliverables.
- Medium priority: Risks such as unplanned or additional work can cause teams to struggle with productivity and create unclear objectives.
- High priority: Risks such as data security and theft can leave your company open to revenue loss and should be prioritized.



Common risk scenarios

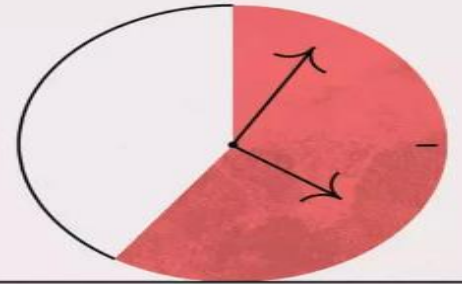
Common risk scenarios



Data security



Communication issues



Scheduling delays



Unplanned work



Theft of materials

Common risk scenarios

Multiple risks could arise during a new project. Anything from data security to unplanned work can risk projects going over budget and scope. Nobody wants to imagine the consequences of missed due dates, which is why it's important to identify potential risks before they happen.



It's a good idea to include common risk categories in your risk register log so you're prepared when they occur.

Common risk scenarios

Data security

If you're working on projects that could affect data security, it's extremely important to track and mitigate potential risks. Unmanaged risks could result in:

Data security is a top risk and should be prioritized accordingly in order to prevent long-term security issues.

- Information being stolen: Without proper mitigation, your business could become vulnerable to private information being stolen. This is especially harmful if it's customer information being stolen.
- Credit card fraud: This is dangerous for a number of reasons, but could result in a loss of revenue and potentially require legal action.



Communication issues

Communication issues can arise no matter the size of your project and team. While a risk register can help identify where communication areas live, it can be helpful to also implement work management software to streamline communication at work.



Here are some risks that could arise from lack of communication:

Common risk scenarios

Here are some risks that could arise from lack of communication:

- Project inconsistencies: Without proper communication, inconsistencies in deliverables can cause confusion.
- Missed deadlines: No one wants to miss a deadline but without clear communication, your team may not be aware of due dates for deliverables.



Creating a proper communication plan can also help prevent risks from surfacing in the first place

If scheduling errors and delays go unnoticed, they can become a big problem when deadlines are missed. Tools such as timelines and team calendar software can help prevent scheduling errors in the first place.

Project scheduling delays could result in:

- Rushed deliverables: There's nothing worse than a project that hasn't been properly executed, which can cause goals to be missed and work to appear sloppy.
- Confusion: Teams can become overwhelmed and confused without a proper schedule in place.



Implementing a schedule can help keep deliverables on track for both daily tasks and one-off projects

Unplanned work

We've all been in a situation where a project goes over scope. It's a common risk that can be fairly easy to mitigate if tracked properly. Catching unplanned work early on allows you to properly delegate it to the project lead.



Common risk scenarios

Without a proper risk register, you could experience:

- **Missed deliverables:** If work slips through the cracks, you may be at risk of missing a deadline altogether.
- **Employee burnout:** Overscheduling your team members with unplanned work can create tension and even cause overwork and burnout. That's why it's important to scope projects correctly.



If you do run into issues with unplanned work, implementing a change control process can help communicate additional work to your team members.

Theft of materials

While hopefully uncommon, businesses that have a large inventory of products could run the risk of theft or reporting errors. By tracking inventory consistently and frequently, you can catch risks early on to determine the cause.



Theft can leave your business open to:

- **Loss of revenue:** Whether products are being stolen or there are errors in reporting, theft will have a negative impact on revenue.
- **Uncertainty:** When theft happens, employee and business uncertainty can cause internal stress.
- **Misuse of time:** Along with theft of tangible goods, there's a risk of time theft. In a remote working environment, it can be more difficult to track where your team is spending their time.

