



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Everyone's Smart University

Project (Spring 2021)

Student Name	Aseel Salih Al Salamah	اسم الطالب
Students I. D.	2021200182	الرقم الجامعي

Section	Date	Course Code
Master	Thursday 18 / 03 / 2021.	(PMG510)

Project Risk Management

Instructions:

- اخر موعد للتسليم هو يوم السبت 08-05-2021 في تمام الساعة 9 مساءً.
- الإجابة متاحة باللغة الإنجليزية أو اللغة العربية مع مراعاة أن تكون المصطلحات العلمية باللغة الانجليزية.
- يتم تسليم المشروع في صيغة ملف pdf مع الالتزام نموذج الجامعة ولن تقبل أي مستندات أخرى.
- يجب مراعاة أقسام البحث الرئيسية (مقدمة Introduction، دراسات علمية سابقة Literature Review، طريقة البحث Methodology، النتائج والمناقشة Results and Discussion، وأخيراً المراجع References .
- وأن كان هناك ملحقات Appendices يتم إضافتها)
- يجب الالتزام بـ Theme موحد كما يلي:
- حجم الخط ١٢.
- نوع الخط Arial.
- لون الخط أسود.
- المسافة بين الأسطر line spacing 1.5
- عدد صفحات البحث (لا يقل عن ثلاث صفحات ولا يزيد عن ست صفحات).

Instructor's Name: Eng. Mosaab M. Hamed

Project:

Risk Identification and Analysis (Based on the project you chose in APM)

The objective of this report is to identify project risks, prepare a risk probability matrix, and carry out an analysis of selected risks. Referring to the project you select in **Advanced projects management APM course**, your task is to prepare a risk management plan that identifies potential risks in **the selected stage of the project** and identify risk management strategies.

From the course content and readings, you know that the overall purpose of risk planning is to anticipate possible risk events and be ready to take appropriate action when risk events occur—to eliminate or reduce negative impacts on the project.

You may wish to begin this exercise with a brainstorming about potential risks to get candidate risks “on the table” for consideration. And then identify and refine that wording for risks that have some realistic chance of occurring in this stage. For example, potential weather problems present a real obstacle to completing field data collection by the planned completion date. It is also an issue that the project manager will ultimately have to plan for, as opposed to other issues such as a major disaster (e.g., your office burning down), is not a high-enough probability event that requires much time in planning. As described below, you will select several of the identified risks and carry out a risk analysis.

You will use the distilled list of risks to make a risk probability/impact matrix. The matrix will have at least three categories (high/medium/low) for probability and impact.

Remember that it is important to name risks effectively—use words that describe the risk event and point to the impact on the project (e.g., “injury of field technician disrupts data installation work”).

After completion of the risk matrix, document a risk analysis for the selected risks. This detailed documentation for that selected risk will include:

- a description of the risk and potential impacts (schedule, quality of work, cost, etc.) on the project.
- indicators or triggers that would be monitored to help identify the risk as early as possible.
- specific risk response strategies to take.

Using probability and impact matrix calculate the **Expected Monetary Value (EMV)** for all risks that have the impact in terms of cost \$\$.

Best of luck...

المشروع:

التعرف على المخاطر وتحليلها (بحث مبني على مشروعك الذي اخترته في مادة ادارة المشاريع المتقدمة)

الغرض من هذا التقرير هو التعرف على المخاطر المحيطة بالمرحلة التي تختارها المرحلة من مراحل مشروعك (نفس المرحلة التي اخترت التطرق لها في مشروعك لمادة إدارة المشاريع المتقدمة Advanced project management) حيث أن مهمتك هي تحضير خطة متكاملة لإدارة المخاطر تشمل التعريف بالمخاطر المحتملة التي تحيط بتلك المرحلة وتحضير مصفوفة احتمالية المخاطر ومن ثم القيام بالتحليل لهذه المخاطر المختارة وتحديد استراتيجيات إدارة المخاطر المناسبة لكل خطر على حدة.

من محتويات المقرر والمصادر الأخرى المتاحة أصبحت تعلم الآن أن الغرض العام لمرحلة التخطيط للمخاطر هي توقع أحداث المخاطر المحتملة والتجهز لاتخاذ ردة الفعل المناسبة عند وقوع الخطر – لمنع أو تقليل الآثار السلبية على المشروع.

قد تحبذ بداية هذا البحث بعصف ذهني عن ماهية المخاطر التي قد تحيط بتلك المرحلة من مراحل مشروعك، وذلك للحصول على قائمة بتلك المخاطر. ومن ثم تحديد وتصنيف هذه القائمة للوصول إلى قائمة مختصرة بالمخاطر التي لها فرصة واقعية أكبر في الحدوث. على سبيل المثال: المشاكل الجوية المتوقعة والتي تمثل عقبة حقيقية أمام اكتمال جمع البيانات من المواقع في أو قبل الوقت المحدد، هذه تعتبر مشكلة على مدير المشاريع أن يضعها في الحساب. من ناحية أخرى، فإن المخاطر غير الواقعية مثل الكوارث الطبيعية والأعاصير (تلك التي تسبب حريقاً بمكتبك وفقدان الأوراق المهمة) ليست لها احتمالية وقوع عالية وبالتالي لاتستدعي تضيق الكثير من الوقت في التخطيط لها. كما سيتبين لك، ستقوم باختيار عدة مخاطر من تلك التي قمت بالتعرف عليها لتحليلها.

ستقوم باستخدام هذه القائمة المختصرة لعمل مصفوفة المخاطر (الاحتمالية/الأثر). المصفوفة ستحتوي على الأقل على ثلاث تصنيفات (عالي/متوسط/منخفض) للاحتتمالية والأثر.

لاتنس استخدام أسماء تصف طبيعة المخاطر بصورة فعالة – قم باستخدام كلمات تصف الحادثة الخطرة وتشير الى أثرها على المشروع (مثل: إصابة أحد الفنيين في الموقع مما يؤثر على أعمال التركيب).

بعد انتهاءك من مصفوفة المخاطر، قم بتوثيق تحليلك للمخاطر المختارة. هذا التسجيل المفصل للمخاطر يجب أن يتضمن:

- وصف للخطر واثاره المحتملة (الجدولة، جودة العمل، التكلفة، الخ)
- المؤشرات والمحفزات التي يجب مراقبتها للمساعدة في التعرف على هذا الخطر قبل وقوعه
- تفصيل للاستجابة المقترحة للتصدي لهذا الخطر

باستخدام مصفوفة الاحتمالات والتأثير ، احسب **القيمة النقدية المتوقعة (EMV)** لجميع المخاطر التي لها تأثير من حيث التكلفة \$\$.

مع تمنياتي بالتوفيق..

Risk Identification and Analysis of PREMIA ASTRA System

Organizations are struggling with risks on multiple fronts, including cybersecurity, liability, investment and more. Risk analysis, or risk assessment, is the first step in the risk management process. IT risk analysis focuses on the risks that both internal and external threats pose to the availability, confidentiality, and integrity of your data. During risk analysis, a company identifies risks and the level of consequences, such as potential losses to the business, if an incident happens.

The risk analysis process involves defining the assets (IT systems and data) at risk, the threats facing each asset, how critical each threat is and how vulnerable the system is to that threat. It is wise to take a structured and project-based approach to risk analysis, such as those offered in NIST SP 800-30 or ISO/IEC 27005:2018 and 31010:2019.

Risk analysis is important for multiple reasons. IT professionals who are responsible for mitigating risks in the infrastructure often have difficulty deciding which risks need to be resolved as soon as possible and which can be addressed later; risk analysis helps them prioritize properly. In addition, many regulatory and compliance requirements include security risk assessment as a mandatory component.

Handpicked related content:

- [Gartner Report] A Data Risk Assessment Is the Foundation of Data Security Governance
In this article, we will look at a risk analysis example and describe the key components of the IT risk analysis process.

Risk Analysis Example

The following sections lay out the key components of a risk analysis document.

Introduction

This part explains why and how the assessment process has been handled. It includes a description of systems reviewed and specifies the assignment of responsibilities required for providing and gathering the information and analyzing it.

Purpose

In this section, you define the purpose of a detailed assessment of an IT system. Here's an example:

According to the annual enterprise risk assessment, *PREMIA* was identified as a potential high-risk system. The purpose of the risk assessment is to identify the threats and vulnerabilities related to < *system name* > and identify plans to mitigate those risks.

Scope

In this section, you define the scope of the IT system assessment. Describe the system components, users and other system details that are to be considered in the risk assessment.

The scope of this risk assessment is to assess the use of resources and controls (implemented or planned) to eliminate and/or manage vulnerabilities exploitable by threats internal and external to *PREMIA*.

System Description

List the systems, hardware, software, interfaces, or data that are examined and which of them are out of assessment scope. This is necessary to further analyze system boundaries, functions, system and data criticality and sensitivity. Here is an example: *PREMIA consist of components, interfaces that process sensitive / critical / regulated data. JAVA is located the system provides core functions.*

Participants

This section includes a list of participants' names and their roles. It should include the owners of assets, IT and security teams, and the risk assessment team.

Assessment Approach

This section explains all methodology and techniques used for risk assessment. For example:

Risk will be determined based on a threat event, the likelihood of that threat event occurring, known system vulnerabilities, mitigating factors, and impact to the company's mission. The data collection phase includes identifying and interviewing key personnel in the organization and conducting document reviews. Interviews will focus on the operating environment. Document reviews provide the risk assessment team with a basis for evaluating compliance with policies and procedures.

Risk Identification and Assessment

Here begins the core part of the information security risk assessment, where you compile the results of your assessment fieldwork.

Handpicked related content:

- [How to Jump-Start GDPR Risk Assessment](#)

Data Inventory

Identify and define all valuable assets in scope: servers, critical data, regulated data, or other data whose exposure would have a major impact on business operations. For example:

Type of data	Description	Level of sensitivity (High, Moderate, Low)
Personally, identifiable information	Name Address Social Security number Credit card number	High
Financial information	Credit card number Verification code Expiry date Authorization reference Transaction reference	High

System Users

Describe who is using the systems, with details on user location and level of access. You can use the example below:

System name	User Category	Access Level	Number of users	Home Organization	Geographic Location
PREMIA	Regular user	Read/Write	10	Gulf General Cooperative Insurance Company	Saudi Arabia

Threat Identification

Develop a catalogue of threat sources. Briefly describe risks that could negatively affect the organization's operations, from security breaches and technical missteps to human errors and infrastructure failures:

Threat source	Threat action
Cyber criminal	Web defacement Social engineering System intrusions (break-ins) Identity theft
Malicious insider	Browsing of personally identifiable information Unauthorized system access Accidental or ill-advised actions taken by employees that result in unintended physical damage, system disruption or exposure
Employees	Illness, death, injury, or other loss of a key individual
Reputation	Loss of confidence from employees Damage to the reputation of the company
Organizational (planning, schedule, estimation, controlling, communication, logistics, resources, and budget)	Improper worker termination and reassignment actions
Legal and administrative actions	Regulatory penalties Criminal and civil proceeding
Technical	Malicious code (e.g., virus) System bugs Failure of a computer, device, application, or protective technology or control that disrupts or harms operations or exposes the system to harm
Environmental	Natural or man-made disasters

Vulnerability Identification

Assess which vulnerabilities and weaknesses could allow threats to breach your security. Here's an example:

Vulnerability	Description
Poor password strength	Passwords used are weak. Attackers could guess the password of a user to gain access to the system.
Lack of disaster recovery	There are no procedures to ensure ongoing operation of the system in the event of a significant business interruption or disaster.

Risk Determination

Here, you assess the probability that threats, and vulnerabilities will cause damage and the extent of those consequences.

Risk Probability Determination

During this step, focus on assessing risk probability — the chance that a risk will occur.

Level	Probability Definition	Example
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.	Unauthorized malicious disclosure, modification, or destruction of information
Moderate	The threat source is motivated or capable, but controls are in place that may impede successful exercise of the vulnerability.	Unintentional errors and omissions
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.	IT disruptions due to natural or man-made disasters

Impact Analysis

Perform risk impact analysis to understand the consequences to the business if an incident happens. Risk analysis can include qualitative risk assessments to identify risks that pose the most danger, such as data loss, system downtime and legal consequences. Quantitative risk assessment is optional and is used to measure the impact in financial terms.

Incident	Consequence	Impact
Unauthorized disclosure of sensitive information	The loss of confidentiality with major damage to organizational assets. The incident may result in the costly loss of major tangible assets or resources, and may significantly violate, harm, or impede the organization's mission, reputation, or interests.	High
IT disruptions due to unauthorized changes to the system	The loss of availability with a serious adverse effect on organizational operations. The organization can perform its primary functions, but the effectiveness of the functions is significantly reduced.	Medium
Non-sensitive data is lost by unauthorized changes to the data or system	The loss of integrity with a limited effect on organizational operations assets, or individuals. The organization can perform its primary functions, but the effectiveness of the functions is noticeably reduced.	Low

Risk Level Evaluation

During this step, the results of the risk analysis are compared to the risk evaluation criteria.

The results are used to prioritize risks according to the level of risk.

Level of Impact	Risk Level Definition
High	There is a strong need for corrective measures. The system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Moderate	Corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	The system's owner must determine whether corrective actions are still required or decide to accept the risk.

Risk Assessment Results

List the risks in the Risk Assessment Results table. The report should describe the threats and vulnerabilities, measure the risk, and provide recommendations for control implementation.

Threat	Vulnerabilities	Mitigation	Likelihood	Impact	Risk
Hurricane	Power outage	Install backup generators	Moderate	Low	Low
Lack of disaster recovery plan	Disaster recovery	Develop and test a disaster recovery plan	Moderate	High	Moderate
Unauthorized users can access the server and browse sensitive company files	Open access to sensitive content	Perform system security monitoring and testing to ensure adequate security is provided for <i>server name</i>	Moderate	High	Moderate

Conclusion

Risk analysis enables you to know which risks are your top priority. By continuously reviewing the key areas, such as permissions, policy, data, and users, you can determine which threats post the highest risk to your IT ecosystem and adjust the necessary controls to improve security and compliance.