**Risk Assessment memo for:**

**Project name/system**

**Contents:**

[1. Basic information: 2](#_Toc132196218)

[2. Introduction 2](#_Toc132196219)

[3. System/project description 3](#_Toc132196220)

[4. Overall assessment, conclusion and recommendation 3](#_Toc132196221)

[5. Analysis 3](#_Toc132196222)

[6. Financial, regulatory and technical considerations 4](#_Toc132196223)

[7. AU's risk landscape when implementing a new system, as well as assessing and calculating risk scores and mitigating measures 6](#_Toc132196224)

[8. Overall risk landscape: 12](#_Toc132196225)

[9. Signature and confirmation 12](#_Toc132196226)

## Basic information:

|  |  |
| --- | --- |
| System/project name: |   |
| Date of risk assessment: |  |
| Participants: |  |
| System/data classification: | *A, B or C* |
| Type:physical / digital / mixed |  |
|  System owner: | *Name* |
| Operations/systems manager: | *AU IT/own operation/outsourced/mixed* |
| Project manager: | *Name* |
| Users: | *Who is the user group?* |
| Data owner: | *Which named person with associated function decides who is allowed to access data?* |
| Written procedures: | *Are written procedures required to ensure and control that the system and its assets are used correctly and lawfully?* |

## Introduction

Before implementing a newly developed or newly procured system, a risk assessment must be carried out of the information security consequences of the project/system. It is important to have a risk-based approach when assessing new systems and projects that are going to be operationalised, or when assessing existing systems and projects.

The risk assessment must be completed to ensure that management is aware of the risks associated with conducting the project and the subsequent use of the system. It is possible to approve the solution with reservations, meaning that parts of the system/solution may not be taken into use.

If, for some reason, a system has been implemented without a risk assessment, a risk assessment must be completed as soon as possible in order to be able to adjust the system for any risks.

*Red italics* in the document mark sections that must be filled in with information for use as the basis of the risk assessment.

Remember to use a risk-based approach to identify the most important risks that could create the biggest problems for AU if something goes wrong and could have major consequences for research, education or people. These risks must be assessed with regard to consequence and probability.

## System/project description

*Brief description of what the system/product is to be used for at AU – what is the purpose of using the system/project?*

## Overall assessment, conclusion and recommendation

*Here, those responsible for the project should briefly summarise the overall assessment, conclusion and recommendation so that the relevant management team can see it before they review the analysis and confirm in writing that they approve the information and risk assessment presented.*

## Analysis

*The analysis is divided into different areas for consideration:*

* *Whether sensitive personal data is to be used*
* *Acceptable downtime*
* *Financial considerations*
* *Regulatory considerations*
* *Technical considerations*

*Check the sub-sections for detailed guidelines.*

**Information about personal data in the system/project:**

1. Is personal data to be processed? (Yes/No)
2. Can we, and do we want to, avoid processing personal data? (Yes/No)
3. Does the whole system process personal data? (Yes/No)
4. Can sub-systems that process personal data be cut off from the rest? (Yes/No)
5. Is personal data anonymised/pseudonymised in part of the system? (Yes/No)

If data and personal data is collected and stored, consider preparing an impact assessment for the data subject’s rights when the risk assessment is prepared.

Visit the Data Protection Unit's website: [Risk assessment and impact assessment (au.dk)](https://medarbejdere.au.dk/informationssikkerhed/databeskyttelse/saerligt-om-forskning/risikovurdering-og-konsekvensanalyse/)

1. Describe in general what data is to be collected:

|  |
| --- |
| *Fill out* |

2. Describe in general why the data is to be collected (purpose):

|  |
| --- |
| *Fill out* |

3. Describe in general who can access the data:

|  |
| --- |
| *Fill out* |

4. Describe in general how collecting personal data adds value to AU:

|  |
| --- |
| *Fill out* |

**What type of data/personal data is to be used in the system/project?**

Describe and assess briefly on the basis of the four categories in the AU data classification model. [Classification of data (au.dk)](https://medarbejdere.au.dk/informationssikkerhed/klassifikation-af-data)

|  |  |  |
| --- | --- | --- |
| No. | Short description of the data | Classification categories: (Public, Internal, Confidential, Sensitive)  |
| *x* | *Fill out* | *Fill out* |
|  |  |  |
|  |  |  |

 **How long is acceptable for the system/project to be down and inaccessible?**

 Select an assessment in the table below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Down < 4 hours**Lack of accessibility will be time-critical almost immediately. | **Down 4-8 hours**Lack of accessibility should preferably not last more than one working day. | **Down 2 days**A couple of days without accessibility is the maximum permissible. | **Down < 1 week**Lack of accessibility may last more than a couple of days, but preferably no more than one working week. | **Down > 1 week**Lack of accessibility may last more than a week. |
| *X* | *X* | *X* | *X* | *X* |
| **Reason/comment for selected assessment of downtime:***Fill out* |

The choice of acceptable downtime will affect the emergency response (technical and operational[[1]](#footnote-1)) required for the system/project as well as the risk accepted during the downtime.

## Financial, regulatory and technical considerations

**Financial**

* *Will AU incur costs to procure and/or operate licences/staffing/other?*
* *Are there any financial benefits?*

**Regulatory**

The regulatory consideration is divided into three areas:

1. Legislation
2. Organisational responsibility of the user
3. Other legal ties

Re. a) Legislation.

* *Which legislation and rules apply for the data and the system you want to use? This often involves the Danish Act on Processing of Personal Data (Persondataloven) and the associated Security Ministerial Order – but also other regulations and agreements, such as EU legislation. In this context, consider that, in legal terms, when data moves across the internet it also moves across national borders, unless the data transport and storage are very tightly controlled.*

*For example, refer to the Danish Act on Processing of Personal Data (Persondataloven) and GDPR (EU legislation)*

Re. b) Organisational responsibility of the user

* *It may be necessary to protect the data/information to be processed either individually or collectively. It may also be necessary to draw up guidelines or put technical limitations in place and ensure that users know what is, and what is not, correct use. Consider whether attachments, flex fields and sending cases directly from the systems may cause security breaches.*

*For example: Primary users will be..., who must.... Non-necessary user access to personal data must be avoided. Relevant instructions should be prepared for administration and management of the solution.*

*For example: Other users include..., who must.... Non-necessary user access to personal data must be avoided. Relevant instructions for the supervision and control of user access and rights should be prepared.*

Re. c) Other legal ties.

* *It is not only legislation that can impose constraints on the use and processing of data/information. Agreements concluded with collaboration partners such as data processing agreements and other rights may also determine the regulatory framework. Sometimes these agreements impose requirements that are stricter than those stipulated in legislation.*

**Technical**

* *Describe the technical security elements of the solution in general with regard to securing access to the information, security regarding storage, security regarding transport of data, known limitations, etc.*
1. Storage of data (location, technology, encryption):
2. Backup of data (location, frequency, storage):
3. Communication of data (network, technology, encryption):

## AU's risk landscape when implementing a new system, as well as assessing and calculating risk scores and mitigating measures

In the table below, list the risks identified and justifications for assessment and calculation of the risk score, and describe planned or existing mitigation measures. Focus solely on the risks incurred by AU by using information/data and processing it in connection with implementing the system. Assess the largest risks with regard to impact and probability.

The risks should be specified according to whether they are based on:

* + Confidentiality (C): Only people with a legitimate need have access to information.
	+ Integrity (I): Information must be consistent and in a form that can be trusted.
	+ Accessibility (A): Information must be available to the right people when they need it.

It must be possible to draw a risk landscape, which the organisation can consider through the steering committee/system owner. Insert the risks from the risk table in the matrix under item 8, stating a Cx, Ix or Ax number.

Consequences (C) and probability (P) are weighted from 1-4 for C, I, A, where 4 is the most critical. Assess and weigh the probability of a risk occurring and what the impact could be.

The system owner determines the consequences of these risks, if possible in dialogue with someone from management, and assesses what this will mean for the organisation. The consequences are indicated using the following scale:

1 Insignificant (unimportant)

2 Slightly serious (troublesome)
3 Very serious (critical)
4 Grave and destructive (unacceptable)

An example of an impact assessment is that disclosure of information about important research results or the research results of a large number of research projects may negatively affect turnover/reputation (High impact).

In a dialogue with other IT and operational experts, the system owner assesses the probability that the experience-based risk in question will become an actual security incident. The probability is indicated using the following scale:

1 Unlikely
2 Not very likely
3 Likely

4 Expected

When evaluating the probabilities, take into account the administrative and technical security measures that have already been implemented and which can help reduce the experience-based probabilities. For example, training employees in the correct use of systems, tools and security in general can reduce the probability of information about research projects being disclosed. The same applies if you restrict the access of employees with just an operational need.

**NB!**It is important to describe and note the relevant risks and reasons for both the consequences and probability in the field "Why has the consequence/probability been assessed at these specific values?" in the risk assessment sheet. This is partly so the risk assessment can be presented to management and partly so a follow-up can be conducted on any changes in the risk landscape (threats, vulnerabilities, consequences and/or new topics to be assessed).

**Table with probability scale and descriptions:[[2]](#footnote-2)**

|  |  |  |
| --- | --- | --- |
| **Value** | **Probability** | **Example description** |
| 1 | **Unlikely** | It is considered almost impossible that the incident can ever occur.* Incident has not been experienced previously
* Only known from a few other public and private organisations, but none in Denmark
 |
| 2 | **Not very likely** | The incident is not expected to occur* Incident has not been experienced previously
* Only known from a few other public and private organisations, but none in Denmark
 |
| 3 | **Likely** | It is probable that the incident will occur* There is experience with the incident, but not within the last 12 months
* Known from other public and private organisations in Denmark (referred to annually in the press)
 |
| 4 | **Expected** | It is expected that the incident will occur* There is experience with the incident within the last 12 months
* Occurs often in other public and private organisations in Denmark (often mentioned in the press)
 |

**Table with a consequence scale and examples of types of consequences:[[3]](#footnote-3)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Value** | **1** | **2** | **3** | **4** |
| **Type of consequence and description** | **Insignificant (unimportant)** | **Slightly serious (troublesome)** | **Very serious (critical)** | **Grave/destructive (unacceptable)** |
| **Strategic:**Entails limitations on the ability to act for a period of time | No particular impact | Planned activities can be carried out with minor adjustments | Entails reassessment of important activities in the short term | Important planned activities will not be carried out for a period of time |
| **Financial:**Leads to additional costs or losses | No particular impact | Additional costs and losses at a limited level, which may require minor budget changes | Major financial losses with the risk of being put under administration | Significant financial losses. Placed under administration |
| **Administrative/procedural:**Entails administrative burdens | Handled without drawing on the resources of the administrative functions | Handled by drawing on reasonable additional administrative resources | Necessary to draw on considerable new and existing administrative resources  | Requires unrealistic expansion of administrative resources |
| **Reputation:**Affects reputation negatively  | No particular impact | Passing interest from certain groups | General negative interest from the public, which may lead to a limited loss of researchers and students. | Significant damage to reputation Responsible manager must resign |
| **Political/strategic:** Entails limitations on the ability to act for a period of time | No particular impact | Planned activities can be carried out with minor adjustments | Entails reassessment of important activities in the short term | Management must resign Important planned activities will not be carried out for a period of time |
| **Relations with stakeholders:** Affects relations with stakeholders | No particular impact | Deteriorated collaboration with some stakeholders | Overall deterioration of collaboration with stakeholders | Significant breakdown in overall collaboration with stakeholders |
| **Human:** Entails consequences for the individual | No particular impact | The individual is subjected to some inconvenience but nothing serious | Serious physical or mental injury to the individual | The life, mobility or health of the individual is at risk |
| **Privacy:**Leads to a breach of privacy  | No particular impact | There are formal deficiencies in the information given to the individual but not to a serious degree | The individual is denied the rights to their own data. Non-sensitive data is transferred unlawfully. | The individual is exposed to unacceptable violations of their privacy.Burdensome decisions are made against the individual on the wrong grounds. Sensitive data is transferred unlawfully. |
| **Breach of legislation** Entails breach of legislation, e.g. of the Danish Public Administration Act and Criminal Code | No particular impact | Failure to follow administrative procedures and rules of a non-critical nature. | Breaches of law that are critical and can discredit AU. | Critical breach of legislation, e.g. the Danish Penal Code. Responsible manager must resign. |

**NB!** The risk table below must be completed and include mitigation measures. Consequence and probability should be assessed on the assumption that mitigating measures are implemented

**Risk table:**

The table below includes examples of risks (highlighted in red) within all three areas of Confidentiality, Integrity and Accessibility. Please insert any further risks that you consider relevant in relation to the system or project in this risk assessment. Some of the examples given may be relevant.

| **Confidentiality** |
| --- |
| **#**Cx | **Risk** | **Description:**  | **Mitigation measures:****(what security measures are under consideration)** | **Why has the consequence/probability been assessed at these specific values?** | **Consequence****C** | **Probability****P** | **Risk** **(C\*P)** |
| C1 | *IT burglary (hackers, etc.)* | *Fill out* | *Fill out* | *Fill out* | *C* | *P* | *C\*P* |
| C2 | *Lack of training* |  |  |  |  |  |  |
| C3 | *Application error*  |  |  |  |  |  |  |
| C4 | *System error*  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

| **Integrity** |
| --- |
| **#**Ix | **Risk** | **Description:** | **Mitigation measures:****(what security measures are under consideration)** | **Why has the consequence/probability been assessed at these specific values?** | **Consequence****C** | **Probability****P** | **Risk** **(C\*P)** |
| I1 | *Error integrating with*  | *Fill out* | *Fill out* | *Fill out* | *C* | *P* | *C\*P* |
| I2 | *Error integrating with*  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

| **Accessibility** |
| --- |
| **#**Ax | **Risk** | **Description:** | **Mitigation measures:****(what security measures are under consideration)** | **Why has the consequence/probability been assessed at these specific values?** | **Consequence****C** | **Probability****P** | **Risk** **(C\*P)** |
| A1 | *Downtime due to system error* | *Fill out* | *Fill out* | *Fill out* | *C* | *P* | *C\*P* |
| A2 | *Downtime due to fire, water damage, etc.* |  |  |  |  |  |  |
| A3 | *Downtime due to hardware error* |  |  |  |  |  |  |
| A4 | *Lack of upgrade of*  |  |  |  |  |  |  |
| A4 | *Application error*  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

## Overall risk landscape:

In the matrix below, insert the risks from the risk table under item 7, specifying the risks identified using Cx, Ix or Ax numbers.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|   Consequence | Critical4 |  |  |  |  |
| Serious3 |  |  |  |  |
| Some impact2 |  |  |  |  |
| No impact1 |  |  |  |  |
|    | Unlikely 1 |  Likely 2 | Very likely 3 | Will occur 4 |
|  P r o b a b i l i t y |

**Red:** Must be considered and acted on immediately.

**Yellow:** Must be assessed and considered.

**Green:** No immediate need for action.

## Signature and confirmation

The result of this risk assessment memo with the risks listed has been approved and considered and will be assessed for any initiatives to be implemented to minimise risks

when operating the system/project.

dd.mm.yyyy

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

System owner or manager responsible for the system/project.

1. <https://medarbejdere.au.dk/informationssikkerhed/forretningsberedskab> [↑](#footnote-ref-1)
2. Content inspired by the Danish Agency for Digitisation. Guidance for IT risk management and assessment [↑](#footnote-ref-2)
3. Content inspired by the Danish Agency for Digitisation. Guidance for IT risk management and assessment [↑](#footnote-ref-3)