Computer Security

Risk Management Framework (RMF)

Understand the Business Context

Our team has the goal to increase productivity for the company's inventory, repairs, warehouse, sales, and logistics departments. They all have something in common and that is looking up information about the company's vehicles, components and parts.

Currently, those tasks are done with manually shared spreadsheets, and consequently no unified data source, causing inconsistencies between files and frustration for the people in charge of querying data.

After analyzing the problem, along with the client, we have come up with a solution: a web application connected to a REST API, where the data is centralized, is easy to look up and accessible anywhere with an internet connection.

Identify the Business and Technical Risks

Business and Technical risks are listed below with their impact mentioned between [brackets].

Business Risks

- Items entered into the system needing constant updates (will require tools to efficiently edit and/or delete items) [increased development time]. This could happen in various scenarios:
    - Physical delivery of wrong inventory items that slip into the data sources.
    - Items that are no longer active or relevant (maybe due to low demand).
    - Changes in established provider agreements (products will be different).
- Project cancelling due to time and/or budget constraints. [financial loss, loss of reputation]
- Change of requirements in advanced stages of development. [unsatisfied stakeholders, financial loss, delays]
- Poor communication with the client / Unclear requirements [delays]

Technical Risks

- Related to the used cloud infrastructure (OCI): [increased development time and cost]
    - Change in functionality of services (database connectivity, hosting, etc.) that require reconfiguration.
    - Service failure due to external circumstances (e.g. timeouts).
- Lack of data integrity due to poorly handled user input, incorrect processing, and corruption. [loss of reputation, time needed to fix]
- Attacks: [privacy violation, financial loss, time needed to fix]

    - People trying to access unauthorised features.
    - Attackers actively trying to steal or modify information.
    - Sensitive information accidentally exposed due to programming mistakes could make vulnerabilities bigger.
- Terminated support to one or more of the technologies used for frontend or backend. [increased development time, migration required]
- Connectivity failure to external API (SAP). [loss of reputation, decreased productivity for users]
- Spreadsheet upload tool format failure [decreased productivity for users, time needed to fix]
    - Tool failing to understand a format
    - Misplacing data
- Lack of web app maintenance (database cleanup, updates, etc.). [decreased productivity, financial loss]

Synthesize and Rank the Risks

Likelihood weights:
LOW (1)
MID (2)
HIGH(3)

Impact weights:
LOW (2)
MID (4)
HIGH(8)

Risk level:
Likelihood * Impact

Rank	Risk	Likelihood	Impact	Risk Level
#1	Change of requirements in advanced stages of development	MID	HIGH	16
#2	Poor communication with the client / Unclear requirements	MID	HIGH	16
#3	Attacks	MID	HIGH	16
#4	Spreadsheet upload tool format failure	HIGH	MID	12
#5	Issues related to the used cloud infrastructure (OCI)	LOW	HIGH	8
#6	Terminated support for backend/frontend development technologies	LOW	HIGH	8

#7	Project cancelling due to time and/or budget constraints	LOW	HIGH	8
#8	Lack of web app maintenance	HIGH	LOW	6
#9	Lack of data integrity	LOW	MID	4
#10	Connectivity failure to external API (SAP)	LOW	MID	4
#11	Items entered into the system needing constant updates	LOW	LOW	2

***NOTE:** Risks with equal level where ordered based on qualitative considerations.

Talking about the Information Security module, I like the way you explained each stage and nicely connected each stage to the next. Explanations are clear and very much related to the business context. However, Synthesize and Rank the Risks could be written better by explaining the likelihood, impact, and how you categorize each risk.