A) Risk assessment

What is it and why do we do it?

A risk assessment is done with any new projects and/or when Awave takes over an existing website/system. It's also meant as a tool for the project team to keep being aware of potential risks along the road.

The purpose of doing the risk assessment is thus to be aware of critical factors, applicable internal and/or external, that could affect quality and information security. These are identified and assessed through this process.
Once the risk assessment is done, it will be easier for the team to be proactive if/when a risk occurs.

When do we do it?

After a quote has been prepared or in connection with project planning, a risk assessment is prepared, using the **Risk assessment template**.

Depending on the size of the project, not all factors in the template will be applicable. However, 3 factors are always necessary to include in the risk assessment:

- Resources/Personnel (don’t forget about Project Managers)
- If there’s any personal data involved (GDPR)
- Budget

Risk assessment shall always be performed on clients with Service Level Agreements (SLA) and/or any other kind of management agreements.

Note that it is important to update the risk assessment if the project takes a different direction than first expected.

Who’s responsible for making it happen?

The overall responsibility for scheduling a meeting for the risk assessment lies with the **Project Manager (PM)**.
It's an advantage to have as many project team members as possible participating in the risk assessment, since different team members can have different views of any probable risks.
It is, however, up to the PM in charge to decide how many of their team members should participate (depending on size of the project, budget, etc).

It is always mandatory for **Tech Leaders** to take part and evaluate any possible technical and/or development risks of a project.