Orange Belgium

IT Security Solutions

Security Assessment

Identify risks associated with your ISMS and assess your security posture to build a long-term security strategy for the future.

Performing a *Security Assessment* is the ideal starting point to define or enhance your cyber security strategy.

Organizations are being exposed to unprecedented cyber threat levels because of their IT perimeter extension as a result of cloud migration, remote working conditions or digital experience offered to internal and external stakeholders. Nevertheless, security strategies are often technology and budget-driven while the importance of having a proper vision over risk exposure remains underestimated. Consequently, organizations are implementing several solutions hoping to improve their resilience. Such an approach has proved insufficient while requiring important investments.

Know where you are to decide where to go

Orange takes a different approach than the one outlined above. By reviewing your ISMS according to the ISO27001 framework, we provide you with a clear and pragmatic assessment of your current posture and the associated risks. This assessment combined with expert recommendations will help you build an effective cyber security strategy.

Our *Security Assessment* is an affordable first step to help you understand where you are in terms of cyber security and provide you with ideal content to build a long-term strategy based on identified risks.

What to expect from our Security Assessment?

- **Short-term content delivery (weeks);**
- **Technical and organizational review of your IT systems, processes and people;**
- **Positioning of the maturity of your ISMS in every domain of the ISO27001 framework;**
- **Actionable recommendations to improve your security posture according to low maturity domains and associated risks identified as a priority;**

ISO27001

- **As an international standard for data security, the ISO27001 framework puts in place measures and process compliance to secure information;**
- **ISO27001 defines security objectives and measures that are implemented to avoid data leak, theft or distortion risks;**

When should you perform a Security Assessment?

- You don’t know where to start to define your cyber security strategy;
- You want to assess your current security measures to improve your posture;
- Clients ask you to demonstrate your security posture to limit cyber risk in their supply chain;
- You need a neutral assessment of your security strategy performed by a 3rd party;

How does Security Assessment work?

ISO27001 certified consultants

Review ISMS according to ISO27001 security controls and measures

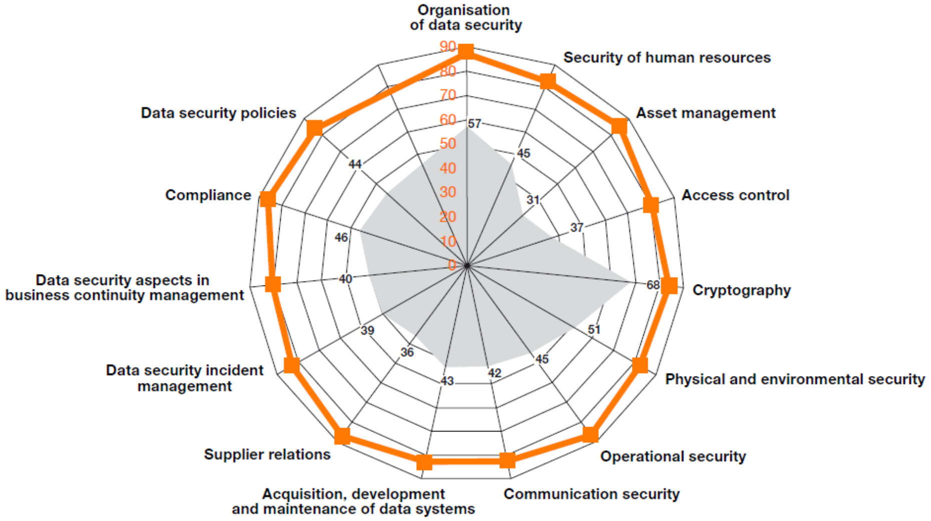
In-house methodologies to maximize efficiency

1 Border the mission in collaboration with decision makers by defining the organization’s challenges and ambitions in terms of cyber security. Translate it according to ISO27001 domains

2 Interview phase to identify measures and processes already in place and associated improvement budget as well as potentially missing elements

3 Report to summarize findings and rank your ISMS maturity level complemented by recommendations and initiatives to mitigate potential risks associated with the identified weaknesses

How to leverage on a Security Assessment?



- Perform a risk impact assessment to prioritize corrective actions according to their potential impact on your organization and business continuity
- Define a risk mitigation roadmap with clear milestones to mitigate the risks identified by the Security Assessment

More information
https://business.orange.be/en/it-solutions/security-solutions

Orange Belgium
Avenue du Bourget 3,
1140 Evere

Contact us
B2BSecurity@orange.be