Orange Belgium

IT Security Solutions

Security Assessment

Identify risks associated to your ISMS and appreciate 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.

Current organizations are exposed as never to cyber risk 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 having a proper vision over its risk exposure remain underestimated. Consequently, organizations are implementing several solutions hoping to improve their resiliency. Such approach is proven to be insufficient while it requires important investment to be equipped.

Know where you are to decide where to go

Orange approach is different than the one mentioned above. By reviewing your ISMS according to ISO27001 framework, we will provide you with a clear and pragmatic assessment of your current posture and associated risks. This assessment combined together 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 stand in terms of cyber security and deliver 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 ISO27001 framework;**
- **Actionable recommendations to improve you security posture according to low maturity domains and associated risks identified as a priority;**

ISO27001

- **International standard for data security, ISO27001 framework aims to ensure measures and processes compliancy to secure information;**
- **ISO 27001 is made of annexes defining security objectives and measures to implement to avoid risks of data leak, stealing or distortion;**

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 look for 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

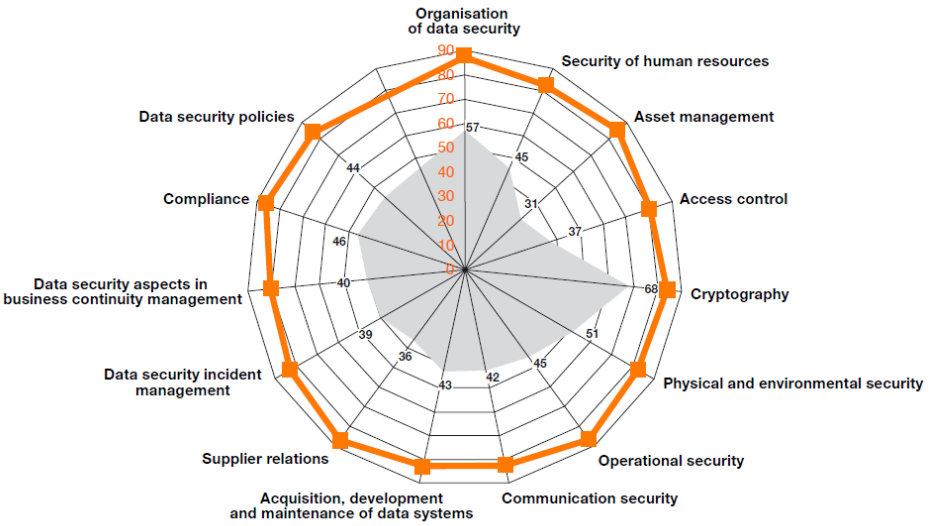
In-house methodologies to maximize efficiency

1 In collaboration with decision makers to border the mission by defining organization's challenges and ambition 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 recommendation and initiatives to undertake to mitigate potential risks associated to weaknesses identified

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 resulting from 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