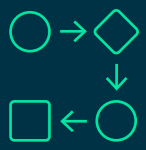
Cyberrisk assessment checklist

This framework is the fruit of 20+ years of successful cybersecurity client projects. Steal it and implement it at your own pace.

Understand and secure your business



Get prepared

- ☐ Identify the key stakeholders who are driving the business activities by means of interviews
- ☐ Identify the most relevant processes
- ☐ Prepare all processes according to relevance
- ☐ Prepare a list potential threat actors and threat scenarios

Conduct a discovery workshop

- ☐ Invite business managers, IT managers and decision makers
- ☐ Identify the business assets
- ☐ Identify the security assets
- ☐ Visualize the business processes in a high-level landscape
- ☐ Visualize threat actors in a high-level landscape

Evaluate the results

- ☐ Overview of the business processes
- ☐ List of the assets to be protected as part of the critical business processes
- ☐ Definition of threat landscape, including threat actors and threat scenarios

Understand who can attack and why

Get prepared

- ☐ Collect documentation about the data flows
- ☐ Collect documentation about the architecture
- ☐ Learn about key digital processes and data flows

Conduct a technology workshop

- ☐ Invite the head of IT, CIO and CISO
- ☐ Visualize critical business processes as a digital workflow
- ☐ Identify all digital systems (potential targets) related to the business assets
- ☐ Identify all digital systems (potential targets) related to the digital assets
- ☐ Sketch the information flows

Evaluate the results

- ☐ List of digital assets and data flows
- ☐ Transcription of assets in terms of data (in motion, at rest, in use)
- ☐ Digital system architecture, incl. the configuration of those systems
- ☐ Attack surface associated with digital assets
- ☐ List of resilience and alignment requirements
- ☐ List of threats

Understand the risks and their impact

Get prepared

- ☐ Analyze the network diagrams
- ☐ Analyze the infrastructure and the systems

Conduct a security workshop

- ☐ Invite business stakeholders, IT stakeholders, and security stakeholders
- ☐ Analyze cyber risks based on a combination of assets, the associated attack surface and threat scenarios

Evaluate the results

- ☐ Detailed overview of the security architecture and digital systems
- ☐ Risks classified according to their level and relevance
- ☐ List of prioritized risks that can be validated with business stakeholders

Create a security roadmap

Get prepared

- ☐ Analyze all identified risks in terms of probability and impact
- ☐ Define mitigation measures for the risks listed based on best practices

Conduct a planning workshop

- ☐ Invite business managers, IT managers and security stakeholders
- ☐ Define security controls for each risk and calculate the residual risk
- ☐ Define the implementation budget and timeline for each control
- ☐ Validate budget requirements with business stakeholders
- ☐ Obtain acceptance of residual risks from business stakeholders

Create your security roadmap

- ☐ Create a backlog with prioritized security controls
- ☐ Based on the backlog, establish an implementation plan

Congrats, you've now launched a high-class security initiative in your company. If you don't want to do it all on your own, we are happy to help.

Go to adnovum.com