

Security Assessment Service

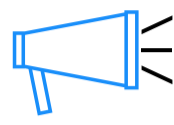
A security assessment is an exercise that tests your organization's security posture by identifying potential risks, evaluating the existing controls, and suggesting new controls.

Benefits for Business



Avoid Negative Impact to the End Customer

Ensure that customers personal data is secured. After data loss customers may receive not only negative emotions but suffer financial loss as well.



Avoid Negative Impact to Company's Reputation and Brand

Save customer's trust, ensure that company's reputation and brand image will be secured. Recovery after security breach demands a lot of time and finances.

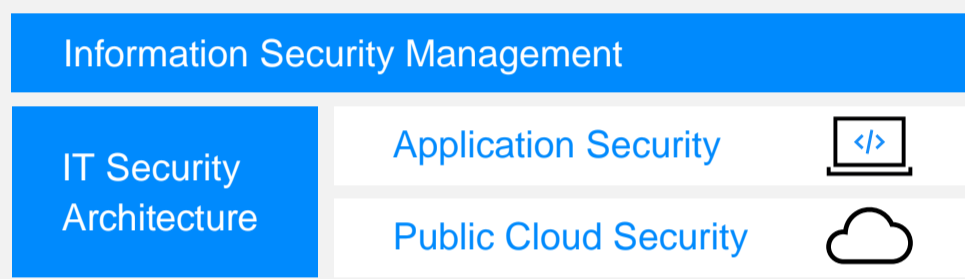


Avoid Financial Impact After GDPR Breach

Costs after GDPR breach can include compensating affected customers, legal fees, and penalties. Penalties may be up to €10-€20 million or 2%-4% of the firm's worldwide annual revenue from the preceding financial year.



What to assess?



Information Security Management	IT Security Architecture	Public Cloud Security	Applications Security
Assess Information Security Management procedures and practices in organization (compliance with ISO/IEC 27002 Standard)	Assess Design & Implementation of Security Controls of IT System	Assess Security Risks related to consumption of Public Cloud and its Services	Assess Application Security posture by vulnerability analysis & penetration testing

When to assess?

<ol style="list-style-type: none"> 1. If never assessed 2. During IT due diligence 3. After organizational changes 	<ol style="list-style-type: none"> 1. If never assessed 2. During IT due diligence 3. After organizational changes 4. When buying/releasing new application 5. When changing IT landscape 	<ol style="list-style-type: none"> 1. If never assessed 2. During IT due diligence 3. After organizational changes 4. When establishing Cloud environment 5. When changing Cloud configuration 	<ol style="list-style-type: none"> 1. Periodically every year 2. If never assessed 3. During IT due diligence 4. After organizational changes 5. When buying/releasing new application 6. When releasing changes to the application
---	--	---	---

Why us?

At **Baltic Amadeus**, we believe in the **power of business digitalization**. We are a reliable technology partner for clients and **our goal is to simplify the complex digital world** by creating valuable experiences for our clients, users, and employees.

With cutting-edge technologies, the latest delivery models, and a 96% recommendation rate among clients **we are a one-stop-shop provider of a full spectrum of IT services and strategic consulting**.



Founded in 1988 in Lithuania, and since then **Baltic Amadeus is a technology partner for many clients** : Luminor Bank, Euro Apothea, Telia, Wallenius Wilhelmsen, Moog, StormGeo.

Experience of Baltic Amadeus consultants **is recognized by industry well-known certificates** like Certified Information Systems Security Professional (**CISSP**), Certified Data Privacy Solutions Engineer (**CDPSI**) and Certified Information Security Auditor (**CISA**).

Let's discuss it further

Andrius Martinonis
 Business Development Manager
 +370 676 64080
 a.martinonis@ba.lt