



Cybersecurity Advisory

Application Security Module

This outcome-driven engagement focuses on security gaps in your software development practices that pose a risk to your organization's security and provide recommendations and a prioritized roadmap to embed security policies, standards, processes and technologies.

Security boundaries have moved; no longer can you rely solely on traditional network security controls to provide adequate protection for your most valuable business assets. Threats continue to evolve rapidly, and your IT landscape changes, driven by new business demands that include more mobile access, more web-based applications, and hybrid IT environments. You need to think strategically about planning, designing and operating your enterprise security.

A review of the current state of your security posture is required as part of your ongoing security improvement initiatives. A robust security roadmap includes the unified and integrated design, implementation and operation of security practices across your organization. This will enable you to formulate a plan to manage risks, maintain compliance with external regulations and contractual mandates and align to industry best practice.

Our Cybersecurity Advisory service is a business-outcome-driven consulting engagement with a flexible, modular framework that spans the entire lifecycle of security, from developing a strategy and plan aligned to your business needs, optimizing existing security controls, to designing your next-generation enterprise security architecture, policies and framework. Insight gained from optional assessments allow you to apply your resources and controls in the most effective way to protect key assets.

'The current explosion in the number of vulnerabilities has **only served to increase complexity** as organizations strive to keep up with patches and migrating controls on a weekly and daily basis.'

Executive Summary -

2019 Global Threat Intelligence Report

Business outcomes

Business outcome	Solution/services benefit
Identification of gaps in your application security policies, standards, processes and technologies.	Improve security within your software development practices ensuring that you achieve your governance, risk and regulatory compliance requirements.
Prioritized roadmap to embed more mature security practices within your applications environment.	Establish confidence that your security requirements are in place within your application development practices and procedures.

How we deliver

Our Application Security Module uses workshops and interviews to undertake a detailed review of your current policies, standards, processes and tools required to develop and implement a strategy for software security that is tailored to the specific risks facing the organization.

Our consultants work with your stakeholders to determine the gaps between your security posture today, where you want to be in the future and how your organization bridges the gap to meet those future requirements. We then benchmark you against other clients in your industry and region and develop a highly-tailored recommended roadmap to integrate security practices within the application security process.

The recommended roadmap can be used to build a budget and resource plan, or simply aligned to an existing strategy for confirmation and reassurance.

Key service features:

- Globally consistent methodology, reporting and benchmarking.
- Provides a comprehensive review of your policies, standards, processes and technologies used for secure software development and identifies any gaps.
- Provides a prioritized, actionable security roadmap to integrate security good practices into your application security process that is business aligned.

Additional Cybersecurity modules for consideration

- **MS365** for application protection, data protection, device protection, and the identities across your Microsoft 365 landscape to protect and secure applications and underlying systems based on sensitivity and criticality.
- **SAP Applications** for application protection, data protection, device protection and the identities across your SAP landscape to ensure that your SAP environment is secure.
- **Reputation, Compliance & Customer** for the protection of data, visibility into where data is stored, who has access to the data, and what the end users do with it to mitigate risk to data compromise or loss and to protect your reputation.
- **Managed Security Services** for the ability to identify, contain, investigate and resolve security incidents. We identify areas for improvement during the transition phase when moving to our Managed Security Services.
- **GDPR** for compliance with the General Data Privacy Regulation (GDPR) to improve the efficacy of your current governance and compliance posture.

Why NTT?



Global experience

More than 15,000 security engagements with clients spanning 49 countries across multiple industries.



Track record

Decades of experience in providing professional, support, managed and fully-outsourced security services to over 6,000 clients.



Expert skills

Highly certified security consultants with expertise across various infrastructures, systems and application technologies.



Proven approach

Client-centric, pragmatic approach using proven assessments, methodologies, frameworks and best practices to deliver consistent, high-quality engagements.