



# Cybersecurity Advisory

## Managed Security Service Readiness

**This outcome-driven engagement** determines the gaps in your information security posture and defines recommendations and a roadmap for improvement, in order to enhance the effectiveness of your managed security services.

**In today's complex ICT environment and threat landscape, utilizing managed security services is an increasingly attractive option. However, for managed security services to be effective and SLAs to be met, organizations need to carry out a comprehensive review of their information security. This needs to cover all aspects of people, process and technology, to identify areas of low maturity, such as incident response, that must be improved before or during a transition to a managed security service, to ensure that it is effective.**

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 information security areas at low levels of maturity that require improvement.	Improvement in your security posture enables Managed Security Services Service Level Agreements to be valid, and incident response and management to be effective.
Identification of gaps in your information security management policies, standards, processes and technology.	Improvement in information security practices reduces business risk and improves the effectiveness of your Managed Security Services.
Recommendations and a prioritized roadmap for implementation.	Increasing the maturity level of your security posture across your ICT landscape improves information security for current and future architectures.

## How we deliver

The Cybersecurity Advisory is delivered in a flexible way, allowing the engagement to be customized based upon the level of detail required.

Our **Managed Security Service Readiness** module uses workshops and interviews to analyse the maturity levels of your security policies, standards, processes and controls, as well as your ability to identify, contain, investigate and resolve security incidents.

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, actionable roadmap for areas that need to be improved during the transition phase of a move to our Managed Security Services.

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.
- Assesses all areas of information security maturity focusing on the areas that are key to utilizing a managed security service effectively.
- Provides a prioritized, actionable security improvement roadmap.

## 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.
- **Application Security** for the development and implementation of a strategy for software security that is tailored to specific risks facing the organization.
- **Reputation, Compliance & Customer Data** 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.
- **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.