DATA SHEET

Cybersecurity Advisory

Identity and Access Management Module

This outcome-driven engagement determines the gaps between your security posture today, where you want to be and how to bridge the gaps to meet future requirements for privileged and non-privileged access.

In today's complex ICT environment, managing a user's identity and access across multiple applications and services has become critical in managing the risk to the organization. As organizations adopt cloud services, access is often not centrally controlled and is hard to manage. Users are granted access when they join an organization and when they change roles further access is granted, making it very difficult to control across systems, applications and data.

Organizations are further challenged by access granted within an application which often results in 'segregation of duties' issues which pose a potential financial and compliance risk. Often a user's access remains intact if they leave the organization and this is only detected during audits and not managed on an ongoing basis.

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 security gaps in access management processes and technologies.	Improvement of the efficacy of your identity and access management policies, processes, standards and controls reduces operating costs and enables better governance of your compliance obligations.
Prioritized roadmap and implementation recommendations.	Unified and integrated design, implementation, and operation of security practices enabled for identify and access management across your enterprise.

How we deliver

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

Our Identity and Access Management module uses workshops and interviews to analyse the maturity levels of identity and access management policies, standards, processes and controls for privileged and non-privileged access.

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 benchmark you against other clients in your industry and region and develop a highly-tailored recommended roadmap to improve the efficacy of your identity and access management policies, processes, standards and controls to enable a holistic approach to identity and access management across the enterprise.

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 identity and access management maturity through the lifecycle of an identity across applications, data, devices, networks and cloud services.
- Provides a prioritized, actionable security roadmap that is business aligned.

Additional Cybersecurity modules for consideration

- **Digital Workplaces** evaluates the data protection, identity and device protection, secure collaboration and cloud access management.
- **Threat Intelligence** evaluates your capabilities, so your organization is able to predict and prevent, protect and respond to cybersecurity attacks.
- **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.
- **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.