NTT Security

Cybersecurity Maturity Assessment

For a business to become resilient to cyber attacks it needs to embed security into the fabric of the organization. As the threat landscape evolves, it becomes increasingly challenging to remain in a state of continuous risk management and it's difficult to assess the maturity of your organization's security program without expert advice.

Many businesses embark on cyber risk assessment programs, but these may only cover a specific security framework or small area of the business in limited depth. They rarely take a comprehensive look at the information security status of the entire organization, or provide a reliable security roadmap for the enterprise.

The Cybersecurity Maturity Assessment (CMA) looks across your entire business to determine the maturity of your practices, processes and cyber response capabilities and to understand if you have reached a level of maturity to support your cybersecurity readiness. We have developed our assessment to provide:

- A comprehensive maturity assessment in terms of breadth and depth
- Evaluation of your complete security architecture, infrastructure and technology
- An established roadmap supported by Enterprise Architecture discipline

Unified Cybersecurity Maturity Assessment framework

Our Cybersecurity Maturity Assessment is based on our security assessment framework. This incorporates two leading industry frameworks, NIST and SABSA, and controls from both frameworks are mapped and consolidated to create our unified approach.

Our framework is tailored to align with the cybersecurity framework of NIST, which supports the five core functions of identify, protect, detect, respond and recover; and the four core functions within the SABSA Architecture framework: security vision and strategy, information security framework, risk management, and logical security architecture. Our evaluation covers more than 180 NIST and SABSA control requirements, ensuring that organizations gain a comprehensive understanding of their cybersecurity posture from a security controls and architecture point of view.

Deliverables

Our team of experts work with you through all stages of the project, from initiation through to assessment, analysis, and reporting. You will receive a comprehensive Maturity Assessment report and Cybersecurity and Security Architecture Roadmap, providing:
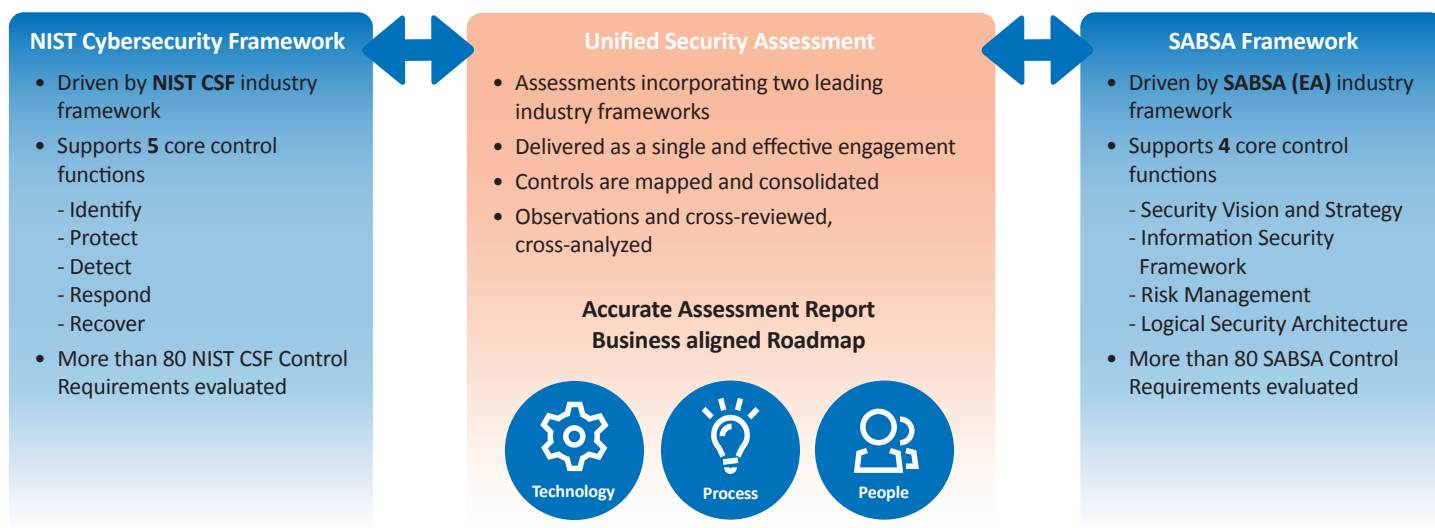
- A detailed executive summary comprising a high-level overview of the gaps
- A clear description of the control areas that require improvement, based on our work program mapped with the NIST Cybersecurity and SABSA Framework
- A detailed view of current security best practice and your organization's assessment outcome
- An in-depth roadmap detailing key improvement areas and a recommended remediation approach

Our methodology

The Cybersecurity Maturity Assessment is a consultative process that will help you understand the gaps that exist between your present and your ideal future state. Once we have identified these gaps, you are better placed to create specific action plans to close the gaps and move your organization towards its security goals. Some of the key steps in our gap analysis process are:

- **Establish scope** – we define the scope of the work and all infrastructure components within it including hardware, software, and locations
- **Identify and collect** – we gather all current documentation including policies, procedures, standards and guidelines
- **Review** – we review all information gathered and evaluate it based on industry best practice
- **Collaboration** – we interview, discuss, and engage with relevant stakeholders to understand and document how your business and IT processes are aligned
- **Designate gaps** – we provide an expert view on the gaps identified and make comparisons between your current security practices and the goals identified by the CMA
- **Present gaps** – we walk your stakeholders through the list of gaps identified during the assessment. We then advise on the steps required to attain the optimum level of security

Figure 1: Our Cybersecurity Maturity Assessment is based on our security assessment framework, which incorporates two leading industry frameworks, NIST and SABSA

NIST Cybersecurity Framework

- Driven by **NIST CSF** industry framework
- Supports **5** core control functions
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- More than 80 NIST CSF Control Requirements evaluated

Unified Security Assessment

- Assessments incorporating two leading industry frameworks
- Delivered as a single and effective engagement
- Controls are mapped and consolidated
- Observations and cross-reviewed, cross-analyzed

Accurate Assessment Report
Business aligned Roadmap

Technology   Process   People

SABSA Framework

- Driven by **SABSA (EA)** industry framework
- Supports **4** core control functions
  - Security Vision and Strategy
  - Information Security Framework
  - Risk Management
  - Logical Security Architecture
- More than 80 SABSA Control Requirements evaluated

Maturity Assessment Metrics

Each framework control requirement will be evaluated and a maturity assessment metric (aligned to the CMMI) used to indicate the level of maturity of each control. We use our own assessment tool kit for the delivery of the maturity assessment, comprising a set of questions which will provide a structured evaluation of the organization's cybersecurity maturity.

Level	Name	Description
5	Optimized	Security architecture is fully aligned to business-driven objectives
4	Managed	Constant monitoring and measuring of policies, procedures, and technology is in place
3	Defined	Complete set of policies and procedures are documented to support the security architecture
2	Repeatable	Technology and/or procedures are developed to a point where they result in the same outcome when repeated
1	Initial	Some ad-hoc approaches may exist
0	Non-existent	Controls are absent which may include policies, procedures, and/or training

We understand that one size does not fit all

We understand that our customers' cyber risks and security needs vary, and that you may not need all the elements of our service. Please contact us to outline your specific challenges and requirements and we'll work with you to tailor a service for the unique needs of your business. Our consultative approach will help you make informed decisions around your overall risk and security strategy.

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **www.ntt.co.jp/index_e.html** to learn more about NTT Group.