



# Cybersecurity Risk Assurance Services Capability Statement

NTT Audit & Assurance delivers consulting and assurance capability to clients addressing **audit, risk management, governance and compliance** requirements including within the associated domain of **information security risk management and governance**.




## Cyber Security risk management to achieve Cyber Resilience

The risks to business data and assets is becoming far more prevalent within our region. Global digitisation has brought with it a ready platform for global threat actors to launch from – at a very low price point.

NTT Audit & Assurance understand that Cyber Resilience can only be achieved through the analysis and implementation of procedural and structural/technical controls in concert.

The cost of prevention is far less than the cost of remediation. As a consequence, the Executive understand the need for Cyber Safety within their organisations. This is the first step towards a Cyber maturity that will protect against the significant risks associated with the cost of remediation, loss of productivity, and reputational damage.

Some of the key Cyber Security program drivers for the Executive are:

-  Avoiding Data Breaches, Financial Loss or Business Interruption
-  Regulatory Compliance and Reputation Protection
-  Improving the overall organisation risk posture and resilience in the connected world

At NTT Audit & Assurance, our Security Practice and experienced team are geared to address these drivers with you to ensure that your risk profile is minimised and your business protected.



## Our capabilities

NTT Audit & Assurance conducts the following activities to enhance Cyber Security Resilience for our clients:



### Cyber Governance Health Check

Our Cyber Governance Health Checks are light touch, involving desktop review, appraisal of main documents, interview of key staff and utilisation of surveys.

A Governance Health Check is typically of low resource intensity and impact upon client staff and management.

Deliverables include gap analysis comparison to relevant standards, guidance and best practices and roadmap for enhancement, recommendations and maturity assessment.

A final Health Check Report for management is prepared.

### Case Study






A NSW Government statutory agency required a light touch governance review to determine the adequacy of the cyber security posture of the organisation.

A health check was proposed by conducting a gap analysis comparing the agency approach to the Australian Cyber Security Centre guidance and the NSW Cyber Security Policy requirements, overlayed with best practice in governance.

A Roadmap for enhancements was developed and an Essential Eight Maturity Assessment provided.



### Cyber Information Security Audit

-  Audit approach with defined scope and objectives tailored to organisation's requirements
-  Usually aligned to better practice standards – ISO 27001, ISMS
-  Detailed procedures to achieve scope and objectives including review of risk management, compliance and governance; policy, procedures and processes; interview of key staff; identification and testing of key controls and strategies; and other additional activities
-  Typically medium resource intensity including management and staff involvement
-  Detailed report including executive summary, commentary on objectives, detailed recommendations and support analyses



## Cyber Resilience Scenario Tests



Scenario Tests are live, virtual desktop activities that test cyber resilience and business continuity without actually impacting BAU operations.




These are run as facilitated workshop activities with key operational and managerial staff which can have multiple phases. Scenario Tests typically run for 2 - 4 hours depending upon no. of phases, participants and complexity desired

Outcomes include Scenario Test report, lessons learnt and recommendations.

Resource intensity is typically low to medium depending upon planning, number of iterations of the test and reporting.

## Cyber Advisory, Training & Awareness

NTT Audit & Assurance also tailors solutions for clients in the following areas, based on specific needs:




-  Integration of Cyber / Info Security Risk Assessment and Threat Assessment with organisational Risk Management Frameworks including Business Continuity
-  Development of client specific training and awareness activities including information assets, training packages, workshops and surveys
-  Governance, compliance and risk management assurance advisory consulting on implementing frameworks including for information security including cyber



We also have access to technical and technology security specialists in the broader NTT Security Solutions and Cybersecurity teams.

## Staff Qualifications and Experience

NTT Audit & Assurance personnel have the following attributes:

-  Specialist expertise and deep experience in conducting risk management, governance and information security reviews including current work reviewing and advising on cybersecurity governance and risk management frameworks
-  Relevant qualifications in audit, risk and information security including Certified Internal Auditors, CA/CPA, CISA, CRMA
-  Specific cybersecurity training including NTT best practices

## NTT's Cyber Security Governance Model






At NTT Audit & Assurance, we recognise that the risks associated with Cyber Security do not solely reside in the IT infrastructure domain. Cyber Security risks are also treated by business governance and policy control implementation. Consequently, we approach Cyber Security as a holistic enterprise-wide risk management issue.

We have experienced consultants who can recognise and analyse the technical risks to ensure that best-practice business governance and policy controls are implemented to minimise your overall enterprise risk profile.













## Better Practice

NTT Audit & Assurance utilises best practices and global standards to deliver optimal outcomes for clients. Our method for cybersecurity and resilience incorporates:

-  Australian and international best practices and compliance standards – Australian Cyber Security Centre, NIST, ISMS (ISO 21001, 27002)
-  Compliance requirements for specific jurisdictions eg NSW Cybersecurity Policy, VPDSS
-  Accepted standards and guidance in associated governance – eg risk management (ISO 31000) and business continuity management
-  Guidance from relevant professional bodies (ISACA and IIA)
-  Specific cybersecurity risk and threat awareness from relevant sources including NTT internal sources



## Questions to assess your Cyber Security posture:

-  How is the Executive informed about the level and business impact of Cyber Security risks?
-  What business or information assets are critical to your organisation?
-  Are Cyber risks well integrated in your risk management practice?
-  What opportunity costs do you have with regards to theft of information or intellectual property?
-  How Cyber Safe are your employees?
-  What measures are in place to protect you against spear phishing and other Social Engineering attacks?
-  What measures are in place to protect your business against abuse or misuse of systems by employees?
-  What is your Incident Management framework?
-  What is the cyber resilience of your clients or third-party providers?
-  Is your organisation aware of the Top 8 strategies that mitigate 85% of unwanted and costly Cyber intrusions?

## For further information please contact:



Rohit Gadgil – Principal Consultant (Victoria)



[rohit.gadgil@global.ntt](mailto:rohit.gadgil@global.ntt)



0414 025 307



Ben Owens – Principal Consultant (ACT & NSW)



[ben.owens@global.ntt](mailto:ben.owens@global.ntt)



0400 477 687





## We are NTT

Together we help people, clients and communities move confidently into the digital future.



Everything we do is driven by our purpose, vision and shared values.

### Our purpose

Contributing to society by resolving social issues through our business operations.

### Our vision

Your valued partner that can be trusted and is committed to long term relationships.

### Our shared values

**Connect, Trust and Integrity** inform all our decision making.

We believe that the best of human traits are brought to life by our company: authenticity, quality, commitment, trust and integrity.

We have a global, forward-looking view that is agile, dynamic, competitive and innovative. **We are NTT.**

