

CYBER PROFILING

CYBER ANALYSIS SERVICE

Across Asia Pacific, cybersecurity threats are estimated to cost organisations up to US\$1.75 trillion in losses — both for direct economic loss due to cyberattacks, and loss of customers and company reputation.*

Enable a more strategic approach to implementing effective enterprise security – with the Adura Cyber Profiling service.

There's a cost to not knowing how effective your security posture is.

USD 1.745 trillion

Economic losses due to cyber security incidents in Asia Pacific*

USD 30 million

Average for a large organisation

USD 96,000

Average for a mid-sized organisation

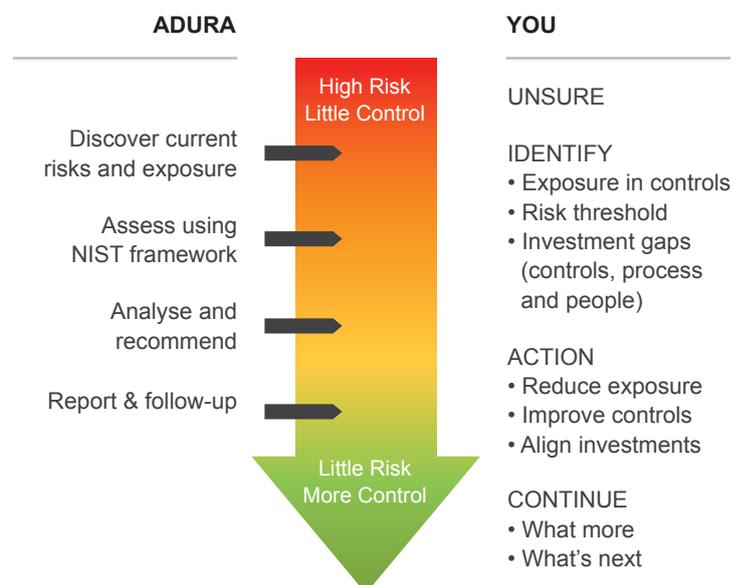
*Microsoft and Frost & Sullivan, Understanding the cybersecurity threat landscape in Asia Pacific: Securing the modern enterprise in a digital world

ENABLE THE RIGHT SECURITY MEASURES

Businesses with heavy IT service requirements and significant assets to protect must align their policy, business and technological approaches, to manage security risks better.

Get a clear measure of your company's security alignment and how effective it is for your cyber security controls. Our Cyber Profiling service will assess your organisation's existing security practices and appliances, and match them against industry benchmarks. Using the globally recognised NIST Cybersecurity Framework, we'll help you to systematically identify and prioritise actions for reducing cyber security risks.

A GUIDED JOURNEY WITH ADURA



THE CYBER PROFILING PROCESS

CHECKPOINTS

SCOPING, PLANNING AND INTELLIGENCE GATHERING

1



Passive system information gathering or documentation delivery from client

ASSESSMENT

2



Onsite NIST control assessment

REPORT AND PRESENTATION

3



NIST findings with recommendations delivered to client

OPTIONAL SERVICES

4



Post assessment monitoring and re-assessment report

ACTIONABLE INSIGHTS

We use the NIST Framework to provide a common language for both technical and management teams to better communicate and manage cyber security risk. An executive report is also included to present details in four key areas:

CYBER CONTROL SUMMARY

Our assessment takes into account the various ways to improve cyber controls; recommendations will be tailored to each functional group for action.

High-level recommendations will then be aligned to the specific tiers used in the Cyber Function assessment for clarity and continuity.

CYBER FUNCTION

Cyber function is a weighted average taken from the compliance scoring, based on 5 key cyber security domains:

- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

Better organised information improves risk management decisions – for addressing threats and learning from previous incidents.

COMPANY CYBER RISK PROFILE

Your Cyber Function score is matched to a 4-tier Company Cyber Risk Profile framework to determine the characteristics of your profile.

90%-100%
• Tier 4 Adaptive

66%-89%
• Tier 3 Repeatable

26%-65%
• Tier 2 Informed

0% -25%
• Tier 1 Partial

EXECUTIVE RECOMMENDATIONS

Recommendations are made by comparing the Current Profile and the Target Profile to prioritise a tailored action plan to address the security gaps.

This will allow you to make better-informed decisions about cybersecurity, support risk management, and perform targeted and more cost-effective improvements.

CYBER PROFILING IS THE STARTING POINT FOR ADURA CYBER SECURITY SERVICES

Journey towards stronger security posture with our Cyber Profiling service. It will deliver the clarity needed to strengthen the foundation of your enterprise security.

Get in touch: Connect with our dedicated consultants to discover how we can help secure your business outcomes on a highly disciplined, verifiable and rigorous approach.



SINGAPORE
E: sg-enquiry@aduragroup.com
T: +65 6817 9596

HONG KONG
E: hk-enquiry@aduragroup.com
T: +852 3750 7518



To learn more about Adura and our services, please visit <https://aduragroup.com/>