



REGIONAL CYBER RESILIENCE & MATURITY STUDY

2026

Published by:



Release date: October 2026

Disclaimer

This publication contains findings based on a survey conducted by ASOCIO. All information furnished in this publication is provided strictly on an 'as is' and 'as available' basis and is so provided for your information and reference only. With this caution, kindly be informed that this release is not presented to address the circumstances of any particular individual or entity. As such, ASOCIO including their sponsors, partners and associates, whether named or unnamed, do not warrant the accuracy or adequacy of the data and findings. Moreover, all parties concerned explicitly disclaim any liability for errors or omissions or inaccuracies pertaining to the contents of this publication. Therefore, the use of data and findings presented in this publication is solely at the user's risk. ASOCIO shall in no event be liable for damages, loss or expense including without limitation, direct, incidental, special, or consequential damage or economic loss arising from or in connection with the data and / or findings published in this series. However, professional advice can be sought from the producers of this publication.

Copyright

Copyright © 2026. All rights reserved. No part of this publication may be produced or transmitted in any form or any means, electronic, mechanical, photocopying or otherwise, including recording or the use of any information storage and retrieval system without prior written permission from ASOCIO.

ASOCIO contact for inquiry: info@asocio.org

<https://www.asocio.org/>

RESEARCH COMMITTEE



Junya Kawamoto
ASOCIO Policy Task Force Committee



Woon Tai Hai
Research Lead
PIKOM Research & Publication Committee
Chair



Rodney Lee
Advisor
PIKOM Advisor for Cybersecurity Chapter



Desmond Teo
Advisor
PIKOM Cybersecurity Chapter Chair



Nurul Asyiqin Nasir
Research Consultant
PIKOM Head of Strategic Relations &
Communications



Chong Bing Zhao
ASOCIO Secretariat Manager



TABLE OF CONTENTS

Foreword by ASOCIO Chairman	4
Message by Chair of ASOCIO Policy Task Force.....	5
1. Executive Summary	7
How to Read This Report	10
2. Methodology and Evidence Architecture	11
2.1 About this report.....	11
2.2 Three evidence layers	11
2.3 Five Maturity Pillars and One Regional Enabler	11
2.4 Respondent survey base and interpretation.....	12
2.5 Limitations and publication controls.....	12
3. Regional Comparative Maturity Overview.....	13
3A. Regional Maturity Matrix — Five Pillars and One Regional Enabler.....	13
3B. Regional Maturity Ranking.....	15
3C. Detailed Maturity Scores.....	16
4. Economy-Level Maturity Tiers.....	18
5. Cross-Cutting Regional Themes	19
5.1 Regional Threat Landscape	19
5.2 Regulatory & Compliance Mapping.....	20
5.3 Architecture & Innovation	20
5.4 Talent & Economic Gap	21
5.5 Future Frontiers: AI and Post-Quantum Cryptography	21
5.6 Regional Collaboration.....	22
6. Respondent Survey Findings	23
6.1 Survey base and respondent profile	23
6.2 Threat outlook, governance and incidents	23
6.3 Regulation and compliance.....	24
6.4 Architecture, innovation and assurance	24
6.5 Investment and talent	24
6.6 Supply-chain and third-party risk	24
6.7 Advanced AI and quantum readiness	24
6.8 Regional collaboration priorities	25
6.9 How the survey changes the interpretation of the desk research	25
7. Strategic Recommendations for ASOCIO	26
8. Economy Profiles	28
Oceania — Australia, New Zealand	28
Northeast Asia — Japan, South Korea, Taiwan, Hong Kong, Macau, Mongolia	29
Southeast Asia — Singapore, Malaysia, Thailand, Philippines, Indonesia, Vietnam, Brunei, Cambodia, Laos, Myanmar	32
South Asia — India, Pakistan, Bangladesh, Sri Lanka, Nepal, Bhutan	38
Central Asia — Uzbekistan	41
9. ASEAN-Japan Cybersecurity Community Alliance (AJCCA) — Expert Perspectives	42
10. Appendix A: Source References by Economy.....	45
11. Appendix B: Survey Methodology and Interpretation Notes	52

FOREWORD



STAN SINGH-JIT Chairman of ASOCIO

In today's rapidly evolving digital landscape, cybersecurity has become a cornerstone of economic resilience, digital trust, and sustainable innovation. As organisations and governments across the Asia-Oceania region embrace emerging technologies such as Artificial Intelligence (AI), cloud computing,

and connected digital ecosystems, strengthening cybersecurity capabilities has never been more critical.

The **ASOCIO Cyber Resilience & Maturity Study 2026** presents valuable insights into the region's cybersecurity maturity, emerging challenges, and strategic priorities. Drawing on perspectives from industry leaders, policymakers, and cybersecurity professionals across our member economies, this report provides evidence-based findings and practical recommendations to support informed decision-making and strengthen cyber resilience.

Cybersecurity is a shared responsibility that demands close collaboration between governments, industry, academia, and the broader digital community. By fostering trusted partnerships, investing in cybersecurity talent, and advancing forward-looking policies, we can build a more secure, resilient, and inclusive digital future for our region.

On behalf of ASOCIO, I extend my sincere appreciation to the Policy Task Force Committee, the research team, our member economies, and all contributors whose dedication and expertise made this report possible. I hope this publication will serve as a valuable reference for policymakers, business leaders, and technology professionals as we work together to strengthen cybersecurity and advance a trusted digital economy across the Asia-Oceania region.

Warm regards,

A handwritten signature in black ink that reads "Stan Singh - Jit". The signature is stylized with a large, sweeping initial 'S'.

MESSAGE



JUNYA KAWAMOTO Chair of ASOCIO Policy Task Force

As digital transformation continues to reshape economies and societies, cybersecurity has become a fundamental pillar of digital trust and sustainable growth. The increasing complexity of cyber threats highlights the need for stronger collaboration, informed policymaking, and a shared commitment to building cyber resilience across the Asia-Oceania region.

On behalf of the ASOCIO Policy Task Force Committee, I am pleased to present the **ASOCIO Cyber Resilience & Maturity Study 2026**. Drawing on insights from cybersecurity leaders and industry stakeholders across ASOCIO member economies, this report provides an evidence-based assessment of the region's cybersecurity landscape, organisational maturity, emerging challenges, and key priorities.

Beyond identifying current trends, this report offers practical recommendations to support policymakers, business leaders, and organisations in strengthening cybersecurity governance, enhancing resilience, and fostering greater regional cooperation. We hope these findings will contribute to more informed decisions and meaningful collaboration as we navigate an increasingly interconnected digital future.

I extend my sincere appreciation to all member economies, survey participants, researchers, and contributors for their valuable support and commitment in making this report possible. Together, we can continue to strengthen digital trust and build a safer, more resilient, and inclusive digital ecosystem for Asia and Oceania.

Warm regards,

川本 淳也



1 EXECUTIVE SUMMARY

This report consolidates desk research covering all 25 ASOCIO member economies into a single, comparable regional assessment, now integrated with the 2026 organisational respondent survey and a survey-to-report validation review. The three evidence layers are kept intentionally distinct: the underlying desk research and evidence originate from the ASOCIO Regional Cyber Resilience & Maturity Survey 2026 economy studies; this document organises that material into a consistent framework, adds a region-wide comparative maturity view, and layers in the respondent survey as validating and enriching evidence rather than a substitute for the desk-research maturity scores.

The headline finding is a wide and structurally consistent maturity spread across the region.

A leading and advanced group led by Singapore, followed by South Korea, Japan, New Zealand, Hong Kong, Australia and Taiwan, demonstrates comparatively mature regulatory, institutional and architectural capabilities, although important gaps remain in areas such as

talent depth, third-party assurance and demonstrated recovery capability.

A second group of Established economies, including India, Malaysia, Thailand, the Philippines and Macau, has built substantial regulatory and technical foundations, but implementation remains uneven, particularly beyond banking, telecommunications, government and large enterprises.

A larger Developing group, including Indonesia, Vietnam, Uzbekistan, Mongolia, Pakistan, Sri Lanka, Nepal, Brunei, Bhutan, Bangladesh and Cambodia, is strengthening foundational law, institutions and technical capability, but faces continuing challenges in converting policy intent into consistent operational resilience.

Laos and Myanmar remain in the Nascent tier, where structural capacity constraints make regional cooperation, capability development and practical implementation support particularly important. (This grouping mirrors the formal five-tier ranking in Sections 3C and 4 exactly.)

Patterns recur across most of the 25 ASOCIO member economies, regardless of maturity tier:

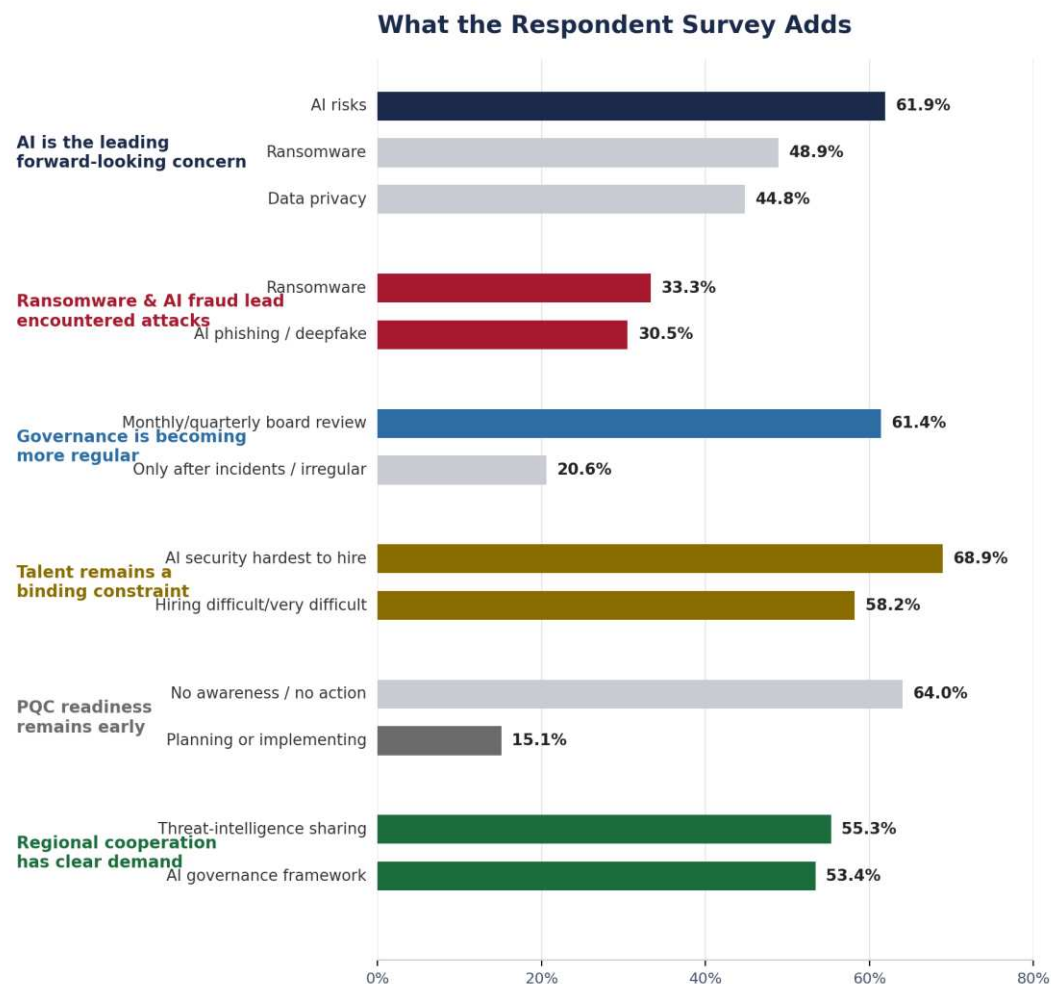
- Phishing, social engineering and AI-enabled fraud are among the most widespread threat categories, from Singapore's AI-generated BEC to Cambodia's romance-scam networks and Myanmar's cross-border scam compounds and the 2026 respondent survey independently confirms AI-enabled phishing/deepfake impersonation as a leading encountered attack type.
- Ransomware remains the most disruptive threat class, with the clearest large-scale case study being Indonesia's June 2024 national data-centre attack, which affected over 230 government agencies.
- Regulatory activity is accelerating almost everywhere in 2025–2026 (Australia's Cyber Security Act 2024, Taiwan's amended CSMA and AI Basic Act, Vietnam's new cybersecurity law, Laos's first cybersecurity law, Hong Kong's critical-infrastructure ordinance), but implementation maturity consistently lags legislative ambition.
- Talent scarcity is a region-wide constraint, from Taiwan and Japan's advanced-economy skills shortages to Vietnam's projected 700,000-professional shortfall and Laos/Bhutan's structural capacity limits.
- PQC readiness remains early across most member economies reviewed. The study found limited evidence of funded, economy-wide migration programmes, while organisational awareness and board-level prioritisation remain uneven; a region-wide "harvest now, decrypt later" exposure worth monitoring.

The board-level implication for the region is consistent: cyber resilience has moved from an IT cost centre to an enterprise governance and public-policy issue. Boards and regulators across the region should expect closer scrutiny of demonstrated recovery capability, not just policy existence, as the defining maturity signal through 2026 and beyond.

Evidence updates: The 2026 respondent survey adds organisational responses from 21 ASOCIO member economies. It validates several regional themes but does not generate or independently validate the 25-member economies maturity scores.

What the respondent survey adds

Organisational responses across 21 ASOCIO economies



- AI is now the leading forward-looking concern: 61.9% selected AI risks, ahead of ransomware (48.9%) and data privacy (44.8%).
- Ransomware remains the leading reported attack category among organisations identifying an encountered attack (33.3%), closely followed by AI-generated phishing or deepfake impersonation (30.5%).
- Cyber governance is becoming more regular: 61.4% reported monthly or quarterly board/executive discussion, but 20.6% discussed cybersecurity only after incidents or not regularly.
- Talent remains a binding constraint: 58.2% described recruitment and retention as difficult or very difficult; AI security was the hardest-to-hire skill at 68.9%.
- PQC readiness remains early: 64.0% reported no awareness or awareness without strategic action; only 15.2% were planning a transition or implementing quantum-safe cryptography.
- Regional cooperation has clear demand: threat-intelligence sharing (55.3%) and an AI governance framework (53.4%) were the two most-selected regional initiatives.

How to Read This Report

This report combines two different kinds of evidence, and distinguishing between them is essential to reading it correctly.

- Reported score (quantitative) – for 13 member economies, a numeric 1–5 figure was calculated directly from that economy's own five-pillar assessment in the underlying study. These are labelled "Reported score" throughout.
- Working estimate / indicative (qualitative) – for the remaining 12 member economies, the underlying study described maturity in narrative terms only, without a numeric score. The curation team derived an indicative 1–5 figure from that economy's own qualitative posture, regulatory timeline and evidence, cross-checked against comparable economies. These are labelled "Working estimate" or "Indicative" throughout and should be read as directional rather than precise.
- Respondent survey findings (Section 6) – a third, separate evidence layer drawn from organisational responses across 21 member economies. This validates or challenges regional themes but does not itself generate or independently confirm the 1–5 maturity scores.

Wherever a figure in this report carries decimal precision (for example, 3.9), that precision reflects the underlying calculation method, not a claim of statistical certainty. Twelve of the twenty-five headline figures are indicative estimates rather than measured scores, and are marked as such at every appearance, in the matrix, the ranking chart, the detailed score table and the economy profiles.



2 METHODOLOGY AND EVIDENCE ARCHITECTURE

2.1 About this report

This final report integrates three complementary evidence layers: the original 25-economy desk-research assessment, the 2026 organisational respondent survey, and a validation review comparing the survey results with the desk-research narrative. The layers are intentionally kept distinct so that respondent evidence is not used to imply a maturity score that the survey instrument was not designed to calculate.

2.2 Three evidence layers

Evidence layer	Coverage	Purpose	How used
25-member economies desk research	All 25 ASOCIO member economies	Policy, threat, architecture, talent, future-readiness and collaboration baseline	Primary basis for economy profiles, five-pillar maturity scoring and regional comparison
Organisational respondent survey	Responses from 21 member economies	Practitioner experience, adoption, incidents, budgets, skills and priorities	Regional validation and organisational-level findings; not a population estimate
Survey-to-report validation review	Comparison of survey dataset and draft report	Identify supported themes, unsupported claims and methodology gaps	Used to qualify wording, correct inconsistencies and strengthen publication controls

2.3 Five Maturity Pillars and One Regional Enabler

Each economy's numerical maturity score is calculated from five maturity pillars: (1) Threat Resilience, (2) Regulation & Governance, (3) Architecture & Technology, (4) Talent & Capability, and (5) Future Readiness (including post-quantum cryptography and advanced AI threats). A sixth dimension, Regional Collaboration, is assessed separately as a cross-cutting regional enabler rather than a maturity pillar; it describes an economy's orientation toward regional cooperation, not its internal cybersecurity maturity, and is therefore not included in the numerical score. Section 6 applies a parallel lens where organisational experience rather than economy-level policy posture is drawn from the respondent survey.

2.4 Respondent survey base and interpretation

The respondent dataset spans 21 ASOCIO member economies. Question-level denominators vary because some respondents did not complete later sections and because some incident questions applied only to organisations providing incident details. Economy-level comparisons should therefore be treated as indicative and reported with the corresponding share of sample. The survey should be interpreted primarily as a practitioner-perspective dataset rather than a representative sample of the ASOCIO organisational population.

2.5 Limitations and publication controls

- The 25 member economies maturity ranking is a desk-research assessment, not a respondent-derived index.
- Thirteen member economies have reported numeric scores from underlying studies; the other twelve use clearly labelled working estimates, calibrated from qualitative posture, regulatory timelines, and available evidence. Some figures may shift over time, please verify with authoritative sources before relying on them.
- The maturity score should therefore be interpreted as an analytical comparative indicator rather than a statistically derived national index.
- The respondent survey is not population-representative across all ASOCIO member economies because the sample is uneven and four member economies are absent.
- Economy-level survey percentages should be used only where the sample is adequate; regional percentages should be read as describing participating organisations, not the whole region.
- This report uses two distinct sets of tier language, deliberately kept separate:
 - Economy-level maturity tiers (Leading → Advanced → Established → Developing → Nascent, Sections 3C–4) describe an economy's overall standing;
 - Pillar-level posture (Established → Advancing → Developing, Section 3A) describes standing on an individual pillar.
 - The two scales are not interchangeable.



3 REGIONAL COMPARATIVE MATURITY OVERVIEW

3A. Regional Maturity Matrix – Five Pillars and One Regional Enabler

Each economy is rated across the five maturity pillars used throughout this study, plus Regional Collaboration, using three qualitative posture terms: Established, Advancing, or Developing. This is a categorical, at-a-glance view; the numeric scores in Section 3C provide the underlying detail. Note these are pillar-level posture terms, distinct from the economy-level maturity tiers (Leading/Advanced/Established/Developing/Nascent) used in Sections 3C–4.

Economy	Threat Resilience	Regulation & Governance	Architecture & Technology	Talent & Capability	Future Readiness	Regional Collaboration †
Singapore	Established	Established	Established	Established	Established	Established
South Korea	Established	Established	Established	Established	Established	Established
Japan	Established	Established	Established	Established	Established	Established
New Zealand	Established	Established	Established	Established	Advancing	Established
Hong Kong	Established	Established	Established	Advancing	Advancing	Established
Australia	Established	Established	Established	Established	Advancing	Established
Taiwan	Established	Established	Established	Established	Established	Established
India	Advancing	Established	Advancing	Established	Advancing	Established
Malaysia	Advancing	Established	Advancing	Advancing	Advancing	Established
Thailand	Advancing	Advancing	Advancing	Advancing	Advancing	Established
Philippines	Advancing	Advancing	Advancing	Advancing	Developing	Established
Macau	Advancing	Advancing	Advancing	Developing	Developing	Advancing
Indonesia	Advancing	Advancing	Advancing	Advancing	Developing	Established

Economy	Threat Resilience	Regulation & Governance	Architecture & Technology	Talent & Capability	Future Readiness	Regional Collaboration †
Vietnam	Advancing	Established	Advancing	Advancing	Advancing	Established
Uzbekistan *	Developing	Developing	Developing	Developing	Developing	Advancing
Mongolia	Developing	Developing	Developing	Developing	Developing	Advancing
Pakistan	Developing	Advancing	Developing	Developing	Developing	Advancing
Sri Lanka	Advancing	Advancing	Developing	Developing	Developing	Advancing
Nepal	Developing	Developing	Developing	Developing	Developing	Developing
Brunei	Advancing	Advancing	Advancing	Developing	Developing	Advancing
Bhutan	Developing	Developing	Developing	Developing	Developing	Advancing
Bangladesh	Developing	Advancing	Developing	Developing	Developing	Advancing
Cambodia	Developing	Developing	Developing	Developing	Developing	Developing
Laos	Developing	Developing	Developing	Developing	Developing	Developing
Myanmar	Developing	Developing	Developing	Developing	Developing	Developing

■ Established ■ Advancing ■ Developing

† Regional Collaboration is assessed as a cross-cutting regional enabler, not a maturity pillar, and is not included in the numerical maturity score in Sections 3B–3C (see Section 2.3).

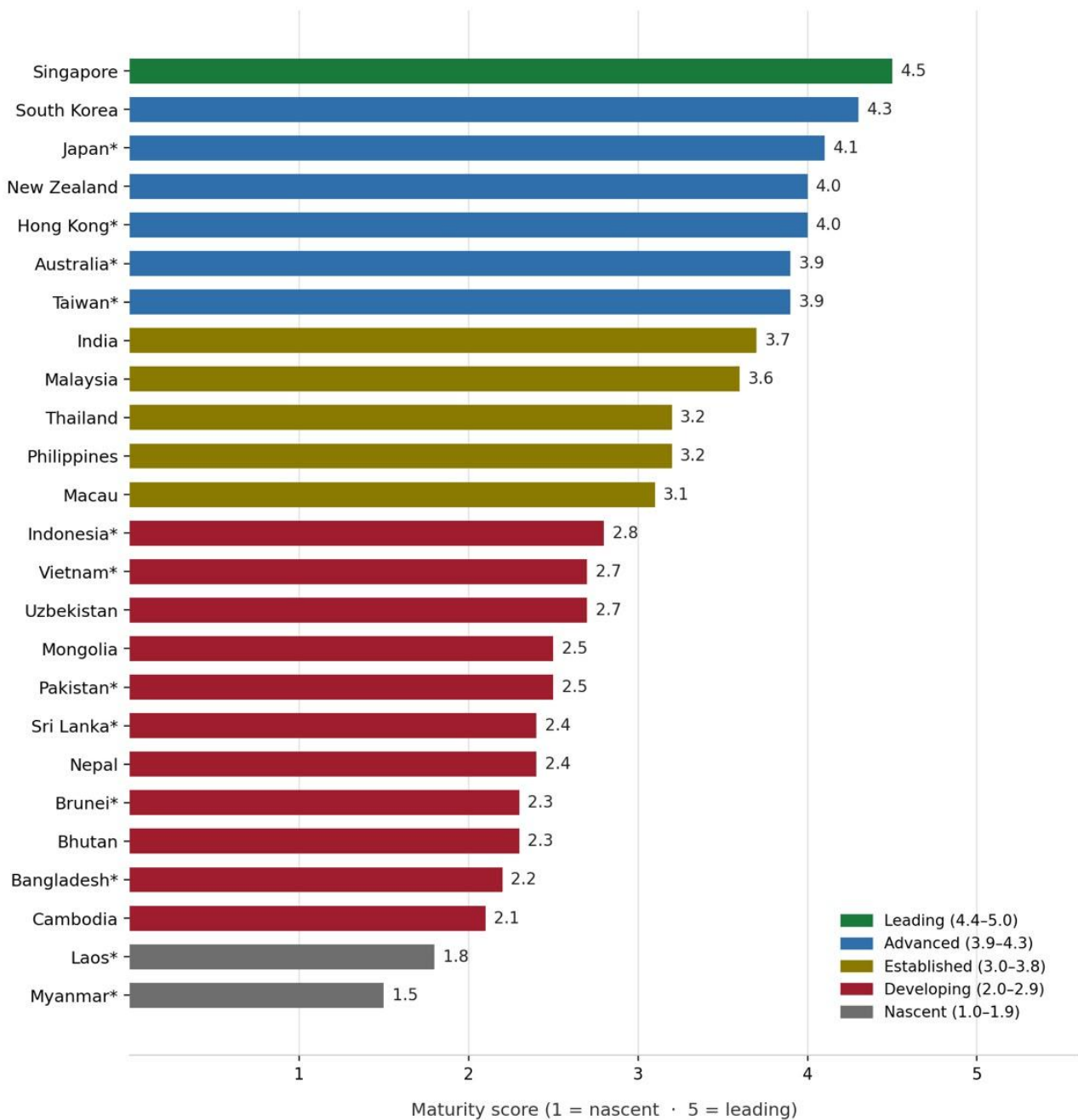
* Uzbekistan was not part of the original team-assessed matrix and is shown here as a working estimate, calibrated against economies with a similar numeric maturity profile (see Section 2.2). All other ratings reflect the research team's direct assessment.

3B. Regional Maturity Ranking

The chart below ranks all 25 ASOCIO member economies by overall numeric maturity score (1–5 scale), coloured by tier. Economies marked with an asterisk (*) carry a working estimate rather than a reported score; see "How to Read This Report" and Section 2.2.

** Working estimate (indicative) — not a measured score*

Regional Maturity Ranking — ASOCIO Member Economies



3C. Detailed Maturity Scores

The table below ranks all 25 ASOCIO member economies on a common 1–5 maturity scale, providing the numeric detail behind the matrix and chart in Section 3A–3B. Thirteen scores are drawn directly from the underlying economy studies ("Reported score"); twelve are working estimates, marked with an asterisk (*), derived from the qualitative posture, regulatory timeline and threat evidence already present in the respective economy study, applied to enable region-wide comparison.

Interpretation:

1 = nascent, 2 = developing, 3 = established but uneven, 4 = advanced, 5 = leading and broadly institutionalised.

Rank	Economy	Sub-region	Score /5 *	Tier	Basis
1	Singapore	Southeast Asia	4.5	Leading	Reported score
2	South Korea	Northeast Asia	4.3	Advanced	Reported score
3	Japan	Northeast Asia	4.1*	Advanced	Working estimate
4	New Zealand	Oceania	4.0	Advanced	Reported score
5	Hong Kong	Northeast Asia	4.0*	Advanced	Working estimate
6	Australia	Oceania	3.9*	Advanced	Working estimate
7	Taiwan	Northeast Asia	3.9*	Advanced	Working estimate
8	India	South Asia	3.7	Established	Reported score
9	Malaysia	Southeast Asia	3.6	Established	Reported score
10	Thailand	Southeast Asia	3.2	Established	Reported score
11	Philippines	Southeast Asia	3.2	Established	Reported score
12	Macau	Northeast Asia	3.1	Established	Reported score
13	Indonesia	Southeast Asia	2.8*	Developing	Working estimate
14	Vietnam	Southeast Asia	2.7*	Developing	Working estimate
15	Uzbekistan	Central Asia	2.7	Developing	Reported score
16	Mongolia	Northeast Asia	2.5	Developing	Reported score
17	Pakistan	South Asia	2.5*	Developing	Working estimate
18	Sri Lanka	South Asia	2.4*	Developing	Working estimate
19	Nepal	South Asia	2.4	Developing	Reported score

Rank	Economy	Sub-region	Score /5 *	Tier	Basis
20	Brunei	Southeast Asia	2.3*	Developing	Working estimate
21	Bhutan	South Asia	2.3	Developing	Reported score
22	Bangladesh	South Asia	2.2*	Developing	Working estimate
23	Cambodia	Southeast Asia	2.1	Developing	Reported score
24	Laos	Southeast Asia	1.8*	Nascent	Working estimate
25	Myanmar	Southeast Asia	1.5*	Nascent	Working estimate

* Working estimate (indicative) is not a measured score. See Section 2.2 and "How to Read This Report".

Indicative regional average: 3.03 / 5.0 (established but uneven). Labelled "indicative" because 12 of the 25 inputs are working estimates, not measured scores.

How the "Basis" column is determined

Reported score – taken directly from that member economy's underlying study, which scored each of five pillars on a 1–5 scale and averaged them into the overall figure shown here. 13 of the 25 member economies were assessed this way.

Working estimate – the remaining 12 member economies' studies described maturity in qualitative terms only, without a numeric score. For these, the curation team derived a working figure on the same 1–5 scale directly from that economy's own qualitative posture, regulatory timeline and threat evidence, cross-checked against economies with a comparable profile. These are estimates for comparability, not official scores, and should be validated with the respective national ICT association before external use. Full methodology: Section 2.2.



4 ECONOMY - LEVEL MATURITY TIERS

These five tiers describe an economy's overall standing (Leading → Advanced → Established → Developing → Nascent) and are distinct from the pillar-level posture terms used in the Section 3A matrix (Established → Advancing → Developing), which describe standing on an individual pillar rather than overall maturity. **The two scales should not be read interchangeably.**

Five Maturity Tiers Across 25 Economies

Leading 1 economy	Broadly institutionalised resilience; a regional reference point across governance, architecture and talent. Singapore 4.5
Advanced 6 economies	Mature governance and architecture under real threat pressure; the residual gap is usually execution depth (talent, third-party assurance) rather than policy intent. South Korea 4.5 Japan 4.1 New Zealand 4.0 Hong Kong 4.0 Australia 3.9 Taiwan 3.9
Established 5 economies	Strong regulatory and architectural momentum, but maturity is concentrated in banking, telecom, government and large enterprise, with a real gap to SMEs and the broader market. India 3.7 Malaysia 3.6 Thailand 3.2 Philippines 3.2 Macau 3.1
Developing 11 economies	Foundational law and institutions are forming or newly in force; the core challenge is converting legal text into operating standards, technical baselines and trained capacity. Indonesia 2.8 Vietnam 2.7 Uzbekistan 2.7 Mongolia 2.5 Pakistan 2.5 Sri Lanka 2.4 Nepal 2.4 Brunei 2.3 Bhutan 2.3 Bangladesh 2.2 Cambodia 2.1
Nascent 2 economies	Structural capacity constraints dominate; regional collaboration and capacity-building have more near-term value than benchmarking against advanced-economy frameworks. Laos 1.8 Myanmar 1.5



5 CROSS-CUTTING REGIONAL THEMES

5.1 Regional Threat Landscape

Two threat categories dominate across most of the 25 member economies, regardless of maturity tier: **phishing/social-engineering-driven fraud, and ransomware**. What differs is the local expression. In advanced economies (Japan, Taiwan, Hong Kong, South Korea), threats increasingly carry a geopolitical or supply-chain dimension – Taiwan's 2.63 million daily intrusion attempts against critical infrastructure in 2025, some synchronised with military activity, is the clearest regional example. In the established-tier group (India, Malaysia, Thailand, Philippines, Macau), threat volume is scaling with digital adoption, while fast-growing Developing-tier economies such as Vietnam and Indonesia show the same pattern even earlier in their

maturity curve, e.g. Vietnam logged 165 breaches and 473 million+ leaked records in Q1 2026 alone, while Indonesia's 2024 national data-centre ransomware attack disrupted over 230 government agencies. In the remaining Developing- and Nascent-tier economies (Cambodia, Myanmar, Laos, Bhutan, Nepal, Mongolia), fraud and scam activity, including transnational scam-compound operations in Cambodia and Myanmar is now as significant a resilience issue as conventional intrusion. The 2026 respondent survey independently corroborates this pattern: among organisations reporting an encountered attack, ransomware led at 33.3% and AI-generated phishing or deepfake impersonation followed closely at 30.5% (see Section 6.2).



Two threat categories dominating across the 25 economies, regardless of maturity tier

5.2 Regulatory & Compliance Mapping

2025–2026 has been an unusually active regulatory period across ASOCIO. New or amended cybersecurity statutes have taken effect or been announced in Australia (Cyber Security Act 2024), Taiwan (amended CSMA, Dec 2025), Hong Kong (Cap. 653, effective 1 Jan 2026), Vietnam (new Law on Cybersecurity, effective 1 Jul 2026), Laos (first cybersecurity law, 2026), Malaysia (Cyber Security Act 2024 / Act 854) and Bangladesh (Cyber Security Act 2023).

Taiwan's AI Basic Act (Jan 2026) is the region's most developed dedicated AI

statute to date. The consistent regional pattern is that legislative ambition is running ahead of implementation: technical benchmarks, sanctions detail and enforcement capacity are frequently still pending even where the statute itself is in force. The respondent survey adds a practitioner view: 44.6% of organisations reported that domestic laws and regional standards had shifted them from basic compliance toward proactive cyber resilience, though 24.9% reported no noticeable strategic impact yet (see Section 6.3).



Across the region, cybersecurity legislation is advancing rapidly—but implementation, enforcement capacity and measurable organisational impact are still struggling to keep pace.

5.3 Architecture & Innovation

Cloud and hybrid adoption varies enormously by economy but follows a consistent internal pattern: banking, telecom, government and multinational operations lead, while SMEs and the broader private sector lag, often relying on ungoverned SaaS rather than architected hybrid environments.

Singapore (indicative estimate: 80–90% large-enterprise cloud adoption), India and New Zealand (indicative estimate: 70–85%) sit at the top; Cambodia, Bhutan, Nepal and Mongolia (indicative estimate: 35–55%) sit at the bottom; these adoption

figures are analytical estimates, not measured statistics, and should be treated accordingly.

Zero Trust and defensive-AI adoption follow the same pattern, i.e. concentrated in regulated, well-resourced sectors. The respondent survey suggests the desk-research estimates, if anything, understate how early most organisations still are: only 14.5% of respondents reported Zero Trust fully implemented, and 51.9% reported 40% or less of IT/OT infrastructure in cloud or hybrid form (see Section 6.4).

5.4 Talent & Economic Gap

Cyber talent shortages emerge as a recurring constraint across the economies reviewed, although the nature and severity of the gap differ substantially by maturity tier. In advanced economies it is more often a depth and specialisation problem (Taiwan and Japan both report structural shortages despite active retraining programmes). In the established tier it is more often a distribution problem for e.g. capability concentrated in a handful of large institutions while the broader market is under-protected (Philippines, Thailand); in Developing-tier economies such as Pakistan the same distribution pattern appears even earlier, concentrated in a

handful of sectors such as banking. In the developing and nascent tiers it is more often a foundational pipeline problem, meanwhile Vietnam's projected shortfall exceeds 700,000 professionals, and Laos and Bhutan report human-capital indices below regional averages with limited structured ICT career pathways. The respondent survey confirms this is not just a desk-research inference: 58.2% of organisations described sourcing, hiring and retaining cyber professionals as difficult or very difficult, and AI security was the single hardest skill to hire, cited by 68.9% (see Section 6.5

5.5 Future Frontiers: AI and Post-Quantum Cryptography

AI is a genuinely double-edged theme across most of the 25 economies: it is simultaneously improving detection and response in the more advanced markets, and lowering the cost of deepfake fraud, voice-cloning extortion and automated phishing more broadly. Taiwan and Singapore have the region's most developed AI-governance instruments; most other economies are still at the awareness stage. Post-quantum cryptography (PQC) readiness is the most consistently under-addressed pillar in the entire dataset. The review found limited evidence of funded, economy-wide PQC migration programmes outside the more

advanced national initiatives identified in Singapore, South Korea and India, despite NIST's guidance that migration planning should begin now given the long lifespan of government, financial and identity data. The respondent survey strongly corroborates this: AI risk was the top forward-looking concern at 61.9%, Shadow AI and malicious agentic AI were joint-leading AI-specific concerns at 55.2% each, and PQC readiness remains predominantly an awareness-stage issue, with 64.0% reporting no awareness or awareness without strategic action (see Section 6.7).

5.6 Regional Collaboration

Collaboration emerges as a recurring priority across the economies reviewed, although the specific needs differ significantly by maturity tier. Advanced economies (Japan, Taiwan, Singapore, South Korea) are best positioned to contribute threat intelligence, OT resilience practice and AI-governance models. Established-tier economies want harmonised incident-reporting templates and sector-specific playbooks. Developing- and Nascent-tier economies (Laos, Cambodia, Myanmar, Bhutan) most need implementation packages — model regulations, CNII playbooks, and cross-border anti-fraud and anti-scam

cooperation, particularly given the transnational nature of scam-network activity affecting Cambodia and Myanmar. The respondent survey gives this direct, quantified support: threat-intelligence sharing (55.3%) and an AI governance framework (53.4%) were the two most-selected regional initiatives among participating organisations (see Section 6.8). Regional Collaboration is treated in this report as a cross-cutting enabler of resilience rather than a maturity pillar in its own right (see Section 2.3), which is why it does not feed into the numerical maturity score in Sections 3B–3C.



AI is accelerating both cyber defence and cyber threats, yet post-quantum readiness remains critically under-addressed—with 64% of respondents reporting no awareness or no strategic action on PQC.



6 RESPONDENT SURVEY FINDINGS

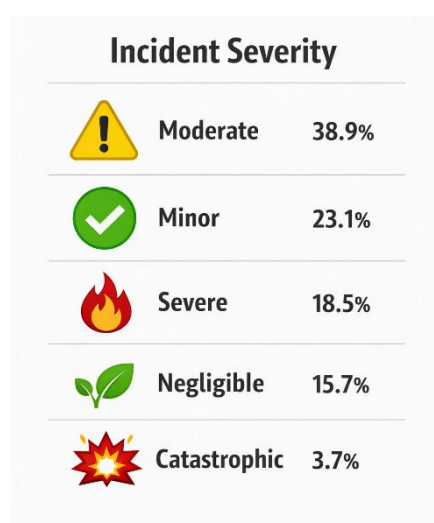
Scope: Organisational responses from 21 ASOCIO member economies. These findings describe participating organisations and should not be treated as population estimates or as the basis for the 25 member economies maturity scores.

6.1 Survey base and respondent profile

Responses were received from organisations across every ASOCIO sub-region, with the widest participation from Southeast Asia and South Asia, including strong representation from Thailand, Malaysia and Vietnam alongside contributions from other member economies. Technology providers formed the largest sector group, giving the survey a strong supplier-side perspective, and the sample skewed toward medium and large organisations, with the majority employing at least 250 people and roughly one in three employing 1,000 or more. Given this shape, the survey is best read as a practitioner-perspective dataset reflecting the experience of participating organisations, rather than a statistically representative sample of the ASOCIO organisational population.

6.2 Threat outlook, governance and incidents

AI risks were selected by 61.9% of all respondents, ahead of ransomware (48.9%) and data privacy (44.8%). Monthly or quarterly board/executive discussion was reported by 61.4%, although 20.6% discussed cybersecurity only after incidents or not regularly. Among respondents identifying an encountered attack, ransomware led at 33.3%, followed by AI-generated phishing/deepfake impersonation at 30.5%.



6.3 Regulation and compliance

The strongest reported effect of domestic laws and regional standards was a shift from basic compliance toward proactive cyber resilience (44.6%). Formal incident-reporting obligations were reported by 35.0%, and 31.6% said regulation had mandated an increase in annual cybersecurity budget. However, 24.9% reported no noticeable strategic impact. Qualitative responses pointed to stronger governance and reporting, additional investment in controls and certification, and greater administrative complexity from overlapping or cross-border requirements.

6.4 Architecture, innovation and assurance

Indicator	Finding
Cloud / hybrid depth	51.9% reported 40% or less of IT/OT infrastructure in cloud or hybrid; 23.5% reported more than 60%.
Zero Trust	14.5% fully implemented; 39.1% partially implemented; 25.1% planning; 16.2% not started.
AI for cyber defence	30.7% actively deployed and 24.6% pilot testing; another 30.2% planning implementation.
Proactive assessment	65.9% vulnerability assessment; 55.9% penetration testing; 36.9% compromise assessment; 20.7% red teaming.

6.5 Investment and talent

More than half of respondents allocated 10% or less of IT budget to cybersecurity, while 26.0% allocated more than 15%. The funding outlook is positive: 66.7% expected a moderate or significant cybersecurity budget increase in 2027. Talent remains a binding constraint: 58.2% described sourcing, hiring and retaining cyber professionals as difficult or very difficult.

6.6 Supply-chain and third-party risk

Vendor questionnaires (46.9%) and mandatory compliance certifications such as ISO 27001 or SOC 2 (42.9%) were the most common controls. More rigorous measures were less prevalent: 29.9% reported independent security audits before onboarding and 28.2% continuous real-time vendor monitoring. Almost one in five respondents (19.2%) reported no formal third-party cyber-risk process.

6.7 Advanced AI and quantum readiness

Shadow AI and malicious agentic AI were the joint-leading AI-specific concerns, each selected by 55.2% of respondents to that question. Yet only 18.6% reported partially or fully

implemented advanced-AI defences. PQC remains predominantly an awareness-stage issue: 41.3% reported awareness without strategic action and 22.7% reported no awareness. Only 10.5% were planning structural transition and 4.7% were already implementing quantum-safe cryptography.

6.8 Regional collaboration priorities

Threat-intelligence sharing (55.3%) and an AI governance framework (53.4%) were the two most-selected regional initiatives. This gives direct respondent support to the report's recommendation that ASOCIO focus on practical, interoperable regional mechanisms rather than only high-level policy alignment.

6.9 How the survey changes the interpretation of the desk research

Desk-research theme	Survey evidence	Final interpretation
AI-related threats are rising	61.9% selected AI risks as a top 24-month concern	Strongly supported; elevate AI to the leading forward-looking concern
Ransomware remains a major threat	48.9% concern; 33.3% of encountered attacks	Strongly supported
Phishing / AI-enabled fraud is widespread	30.5% AI phishing/deepfake among encountered attacks	Supported as among the most widespread, not necessarily the single most universal threat
Talent shortages constrain resilience	58.2% difficult/very difficult hiring	Supported regionally
AI security skills are scarce	68.9% selected AI security as hard to hire	Strongly supported and should be highlighted
Zero Trust implementation is uneven	Only 14.5% fully implemented	Supported
PQC preparedness is immature	64.0% no awareness or awareness without action	Strongly supported
Regional threat-intelligence sharing is valuable	55.3% selected it as a priority	Strongly supported
AI governance should be a regional priority	53.4% selected it	Strongly supported



7 STRATEGIC RECOMMENDATIONS FOR ASOCIO

These seven recommendations are the single, consolidated set of ASOCIO priorities arising from this report, synthesising the region-wide themes identified across the 25 economy studies with the concrete evidence from the 2026 respondent survey. Each is sequenced by breadth of applicability, not by priority; in practice, ASOCIO member associations should weight them against their own economy's tier and stated priorities in Sections 4 and 8.

Recommendation	Evidence	ASOCIO action	12–24-month deliverable
1. Threat Intelligence Exchange	Highest-demand regional initiative in the respondent survey (55.3%); phishing, ransomware, scam and supply-chain indicators recur across nearly all 25 economy studies.	Establish a trusted, member-led threat-intelligence exchange across member associations, CERTs and sector communities.	Pilot exchange live with at least 5 founding member economies; first quarterly threat digest published.
2. AI Security & Governance Framework	AI risk is the leading forward-looking concern (61.9%); AI governance was the second-highest regional initiative (53.4%); Taiwan's AI Basic Act is the region's most developed model to date.	Develop practical regional guidance for Shadow AI, agentic AI, deepfakes, RAG/code-generation exposure, procurement and defensive AI, building on Taiwan's and Singapore's frameworks.	Published ASOCIO AI security and governance playbook, piloted with at least 3 member economies.
3. Regional Cyber Exercise Programme	Indonesia's PDNS incident and Taiwan's sustained CI pressure illustrate the value of tested recovery capability, consistent with the report's central resilience thesis.	Run recurring cross-border exercises on ransomware, public-service continuity, identity compromise and supply-chain disruption, with recovery objectives and decision logs rather than purely technical playbooks.	First regional exercise conducted with economies from at least 3 maturity tiers; after-action report published.
4. Talent Mobility & Skills Accelerator	58.2% of surveyed organisations describe hiring as difficult or very difficult; AI security is the hardest skill to hire (68.9%);	Coordinate training pathways and cross-border mobility for AI security, cloud security, governance/risk,	Regional skills framework published; first cross-border training/mobility cohort completed.

Recommendation	Evidence	ASOCIO action	12–24-month deliverable
	talent constraints recur across most economies reviewed, from advanced-economy depth gaps to Vietnam's projected 700,000-professional shortfall.	architecture and security leadership.	
5. PQC Readiness Programme	64.0% report no awareness or awareness without strategic action; only 15.2% are planning or implementing quantum-safe cryptography; PQC is the most consistently under-addressed pillar in the desk research.	Start with awareness, cryptographic inventory, data-longevity classification and migration sequencing rather than waiting for universal deployment standards.	Regional PQC awareness toolkit issued; cryptographic-inventory pilot completed in at least 3 member economies.
6. Third-Party Assurance Baseline	19.2% of surveyed organisations report no formal third-party cyber-risk process; vendor questionnaires (46.9%) remain the dominant control, well ahead of continuous monitoring (28.2%).	Move member organisations beyond questionnaires toward proportionate pre-onboarding assurance, continuous monitoring and incident-notification requirements.	Model assurance baseline published; piloted by at least 5 member economies' anchor institutions.
7. Maturity-Tier Collaboration Model	Collaboration needs differ significantly by maturity tier. Advanced economies can contribute frameworks and threat intelligence; developing and nascent economies need implementation packages and capacity-building.	Match support to tier: reference-economy framework sharing for advanced members; implementation toolkits for established/developing members; capacity building for nascent environments.	Tiered support model formally adopted by ASOCIO; first matched partnership launched.



8 ECONOMY PROFILES

Each profile below shows pillar-level posture across the five maturity pillars, plus Regional Collaboration (marked †) shown as a cross-cutting enabler rather than a maturity pillar — consistent with Sections 2.3 and 3A, Regional Collaboration does not feed into the numerical maturity score.

OCEANIA

Australia and New Zealand anchor the region's advanced tier, with mature privacy and cyber-incident regulation and high observed board-level cyber literacy — though both reports flag a gap between stated confidence and demonstrated recovery capability.

Australia • 3.9/5 (Advanced, working estimate)

High-maturity, high-expectation environment where confidence must now be matched by proof

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Established	Established	Established	Established	Advancing	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● Ransomware and cyber extortion ● Data breaches remain material ● AI-enabled phishing and fraud ● Confidence exceeds proven capability	● Cyber Security Act 2024 in force ● 72-hour ransomware payment reporting ● SOCI Act 2.0 reforms proposed ● Critical-infrastructure rules tightening	● Recovery-proof exercises ● Cross-functional incident drills ● AI-threat benchmarking ● Board assurance frameworks

Interpretation: Australia's challenge is proving that controls work under real incident conditions, not building more of them.

New Zealand · 4.0/5 (Advanced)

Mature governance and high cloud adoption, with PQC and crypto-inventory work still early

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Established	Established	Established	Established	Advancing	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● Phishing and BEC scams ● Credential theft widespread ● Ransomware and data extortion ● Compromised edge devices	● Privacy Act 2020 core instrument ● NCSC threat reporting active ● GCSB national oversight ● Sector overlays developing	● Sovereignty and resilience assurance ● PQC crypto-inventory kick-off ● Government cloud guidance extension ● Cross-border exercise participation

Interpretation: New Zealand's mature government cloud guidance should now extend into sovereignty and resilience assurance for critical systems.

NORTHEAST ASIA

Japan, South Korea, Taiwan and Hong Kong form the region's most advanced governance and architecture cluster, operating under some of the highest sustained threat pressure in the study (Taiwan's daily intrusion volume, Hong Kong's phishing scale). Macau and Mongolia sit further down the maturity curve, with resilience concentrated in finance, gaming and government-linked sectors respectively.

Japan · 4.1/5 (Advanced, working estimate)

Established cyber capability with accelerating national security posture

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Established	Established	Established	Established	Established	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● Ransomware remains major ● Phishing against finance/e-commerce ● Espionage pressure on tech sector ● Supply-chain and OT exposure	● NCO established in 2025 ● Active cyber defence direction ● APPI privacy obligations ● Critical-infrastructure reporting rising	● Share advanced practices ● OT and supply-chain resilience ● PQC planning ● Cyber exercises around espionage

Interpretation: Japan is a regional source of advanced practice, but legacy systems, industrial base and geopolitical exposure make resilience and supplier assurance critical.

South Korea · 4.3/5 (Advanced)

Advanced governance with high cloud maturity; PQC awareness strong but not yet universal

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Established	Established	Established	Established	Established	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● Credential theft and smishing ● Ransomware and data extortion ● Telecom/software supply-chain compromise ● Citizen-scale phishing volume	● PIPA is central instrument ● KISA active incident coordination ● SK Telecom breach response tightened ● Cloud-first public policy	● Extend PQC research to migration ● Telecom supply-chain assurance ● National quantum programme scale-up ● Cross-sector threat sharing

Interpretation: Korea's advanced national quantum and cryptographic research should now translate into economy-wide PQC migration roadmaps.

Taiwan · 3.9/5 (Advanced, working estimate)

Mature policy environment operating under unusually intense, geopolitically-linked threat pressure

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Established	Established	Established	Established	Established	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● 2.63M intrusion attempts/day (2025) ● Energy, health, comms targeted ● State-linked, military-synchronised activity ● Vulnerability exploitation, DDoS, social engineering	● Amended CSMA, authority to MODA ● 1-hour incident reporting mandate ● AI Basic Act (Jan 2026) ● FSC financial resilience blueprint	● Recovery targets, not just policy ● Vendor-exit options ● OT and CI resilience exercises ● PQC migration (financial sector-led)

Interpretation: Taiwan's cyber risk is increasingly strategic in character, with direct operational implications for critical services — boards should test whether services can continue under multi-vector, geopolitically-timed pressure.

Hong Kong · 4.0/5 (Advanced, working estimate)

Advanced financial-sector resilience with new critical-infrastructure regime

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Established	Established	Established	Advancing	Advancing	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● HKCERT: phishing dominant in 2024 ● Financial and e-payment exposure ● Third-party and cloud concentration ● Ransomware remains continuity risk	● Cap. 653 effective 1 Jan 2026 ● OCCICS Code of Practice ● HKMA CFI / C-RAF ● PDPO breach guidance	● Financial cyber exercises ● AI fraud intelligence ● Common incident reporting ● Supplier and cloud risk playbooks

Interpretation: Hong Kong's financial-sector maturity and new CII regime make it a strong reference case for governance, reporting and sector cyber resilience.

Macau · 3.1/5 (Established)

Governed finance and gaming sectors; SME governance and PQC readiness still shallow

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Advancing	Advancing	Advancing	Developing	Developing	Advancing

Key threat pattern	Regulatory direction	ASOCIO priorities
● Phishing, impersonation, fraud apps ● Ransomware and malware ● Account compromise, data exposure ● SME provider-dependence	● Cybersecurity Law No. 13/2019 ● CARIC incident coordination ● AMCM cyber risk guideline ● AMCM cloud outsourcing guideline	● Crypto inventory: finance, identity ● SME governance baseline ● Cloud outsourcing assurance ● Payments-sector PQC planning

Interpretation: Macau's finance and gaming sectors operate in highly governed environments, but resilience thins quickly once outside those two industries.

Mongolia · 2.5/5 (Developing)

Developing regulatory base; resilience concentrated in banks, telecoms, mining and government

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Developing	Developing	Developing	Developing	Developing	Advancing

Key threat pattern	Regulatory direction	ASOCIO priorities
● Online fraud and phishing ● Identity theft, BEC ● Malware and ransomware ● Account compromise, data breaches	● Law on Cybersecurity (2021/2022) ● Cyber Security Council active ● National Anti-Fraud System ● Data protection law developing	● Crypto inventory: ID, finance, mining ● SME cyber baseline ● Regional capacity-building ● Shared SOC/CERT training

Interpretation: Mongolia's cybersecurity institutions are forming faster than broad-market implementation — regional capacity-building has high near-term value.

SOUTHEAST ASIA

The region's largest and most heterogeneous cluster, spanning Singapore — the regional benchmark — through established economies with strong regulatory momentum (Malaysia, Thailand, Philippines) and fast-scaling Developing-tier economies still consolidating toward established status (Indonesia, Vietnam), to economies still building foundational law and institutions (Brunei, Cambodia, Laos, Myanmar). Cyber-enabled fraud and transnational scam-network activity are a defining regional theme, especially in Cambodia and Myanmar.

Singapore · 4.5/5 (Leading)

Regional benchmark: broadly institutionalised resilience across all five pillars, plus strong regional collaboration

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Established	Established	Established	Established	Established	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● AI-generated phishing/BEC ● Ransomware and data extortion ● Botnet/infrastructure exploitation ● Highest regional cloud exposure	● Cybersecurity Act 2018 + 2024 amendments ● CSA active oversight ● MAS Technology Risk Guidelines ● PDPC enforcement mature	● Export maturity frameworks regionally ● PQC and AI-governance modelling ● Regional threat-intel leadership ● Financial-sector exercise design

Interpretation: Singapore provides a strong regional reference model, with opportunities to share proven frameworks and practices across ASOCIO member economies while continuing to strengthen its own resilience.

Malaysia • 3.6/5 (Established)

Strong regulatory momentum; PQC and crypto discovery not yet on most board registers

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Advancing	Established	Advancing	Advancing	Advancing	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● AI-assisted phishing, scams, BEC ● Malware, ransomware, data extortion ● Government-facing service compromise ● Rising OT/cloud convergence risk	● Cyber Security Act 2024 (Act 854) ● NACSA legal instruments and baselines ● MyCERT quarterly incident reporting ● 2024 implementing regulations	● Push PQC into risk registers ● Cryptographic discovery mandate ● OT/manufacturing convergence controls ● SME baseline extension

Interpretation: PQC and 'harvest now, decrypt later' risk do not yet appear to be prominent board-level priorities in Malaysia, making cryptographic discovery and migration planning an important near-term gap.

Thailand • 3.2/5 (Established)

Advancing broadly across pillars; OT/cloud integration remains uneven outside leading sectors

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Advancing	Advancing	Advancing	Advancing	Advancing	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● Phishing, call-centre scams ● Credential theft, BEC ● Ransomware and malware ● Unauthorised database access	● Cybersecurity Act B.E. 2562 (2019) ● NCSA active coordination ● PDPA breach-notification clarified ● Google Cloud AI-defence collaboration	● Extend banking/telecom practice to OT ● Mid-market cyber uplift ● AI-powered defence scale-up ● Manufacturing resilience programme

Interpretation: Thailand's banking, telecom, retail and manufacturing leaders are ahead of the wider OT-heavy market — the gap is extension, not invention.

Philippines · 3.2/5 (Established)

BPO- and fintech-led maturity; government and OT modernisation still uneven

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Advancing	Advancing	Advancing	Advancing	Developing	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● Phishing, social engineering ● Mobile/SIM-enabled scams ● Ransomware and malware ● Public/private platform breaches	● Data Privacy Act 2012 ● NPC circulars active ● National Cybersecurity Plan 2023–2028 ● Breach-notification timelines defined	● Standardise crypto/cloud baselines ● Extend BPO practice to government ● OT modernisation security-by-design ● SME cyber uplift programme

Interpretation: The Philippines' BPO and fintech sectors are comparatively advanced — the opportunity is transferring that discipline into government and OT.

Indonesia · 2.8/5 (Developing, working estimate)

Large, fast-scaling digital economy where governance ambition is outrunning operational resilience

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Advancing	Advancing	Advancing	Advancing	Developing	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● 2024 PDNS ransomware — 230+ agencies ● 98% of one data centre unbacked-up ● Phishing, web defacement ● Supply-chain compromise	● National Cybersecurity Strategy (Perpres 47/2023) ● PDP Law 27/2022 (72-hr notice) ● BSSN Reg 1/2024 (CIRT structure) ● Sectoral CIRTs forming	● Mandate resilient public-service backups ● Operationalise CIRT reporting/exercises ● Data-centre outage response drills ● SME cyber baseline

Interpretation: Indonesia is the clearest regional case for translating a major ransomware incident into a national resilience improvement agenda.

Vietnam · 2.7/5 (Developing, working estimate)

Fast digital growth outpacing organisational readiness ahead of a major new cybersecurity law

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Advancing	Established	Advancing	Advancing	Advancing	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● 165 breaches, 473M+ records (IPSIP, Q1 2026) ● Ransomware, phishing, APT, DDoS ● AI-assisted attack techniques rising ● E-commerce and fintech exposure	● New Law on Cybersecurity (eff. 1 Jul 2026) ● National CIRT Response Alliance ● Centralised state coordination ● Hanoi Convention provisions integrated	● Resilience-by-design before law takes effect ● Workforce pipeline (700k+ shortfall) ● Cross-functional incident testing ● Legal/evidence-handling readiness

Interpretation: Vietnam's board-level test is whether the organisation can detect, contain and recover under the new legal regime — not just track compliance status.

Brunei · 2.3/5 (Developing, working estimate)

Innovation-friendly digital ambition running ahead of enforceable technical baselines

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Advancing	Advancing	Advancing	Developing	Developing	Advancing

Key threat pattern	Regulatory direction	ASOCIO priorities
● Ransomware, phishing ● CII targeting ● Cloud/supply-chain vulnerabilities ● Expanding attack surface via Digital Brunei 2030	● Cyber Security Order 2023 ● National Cyber Security Framework ● Digital Brunei 2030 (sovereign cloud, AI DCs) ● Guideline-based AI governance	● Convert ambition into governed architecture ● Workforce capability build-out ● Regional partnership for capacity ● CII baseline enforcement

Interpretation: Brunei's digital ambition is ahead of its governed architecture — regional partnership is the fastest path to close that gap.

Cambodia · 2.1/5 (Developing)

Enterprise vulnerability intersecting with transnational scam-compound risk

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Developing	Developing	Developing	Developing	Developing	Developing

Key threat pattern	Regulatory direction	ASOCIO priorities
● Investment/romance scams ● Account takeover, payment fraud ● Malware/ransomware, site compromise ● Transnational scam-network data abuse	● E-Commerce Law 2019 ● 2026 landmark cybercrime/scam law ● Comprehensive data law still developing ● Board escalation limited outside majors	● Minimum viable cyber/data law ● Board escalation beyond banks/telcos ● Cross-border anti-scam cooperation ● SME compliance capacity

Interpretation: Cambodia needs both a stronger domestic compliance baseline and regional anti-scam cooperation — neither alone is sufficient.

Laos · 1.8/5 (Nascent, working estimate)

Legal foundation newly in place; implementation and technical standards still pending

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Developing	Developing	Developing	Developing	Developing	Developing

Key threat pattern	Regulatory direction	ASOCIO priorities
● Phishing, fraud, impersonation (rising) ● Basic controls still the priority ● CNII sectors newly identified ● Cross-border service exposure	● First cybersecurity law (2026) ● CNII sectors identified by MTC ● Annual reporting mandate (January) ● LaoCERT interoperability pending	● Phased implementing regulations ● Minimum technical compliance baselines ● LaoCERT-national system integration ● CNII sector playbooks

Interpretation: Laos has the legal foundation for cyber resilience; the priority now is converting 'law on the books' into 'law in operation.'

Myanmar · 1.5/5 (Nascent, working estimate)

Foundational and constrained environment with high regional cybercrime complexity

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Developing	Developing	Developing	Developing	Developing	Developing

Key threat pattern	Regulatory direction	ASOCIO priorities
● Cyber-enabled fraud, scam compounds ● Phishing, crypto, romance scams ● Limited enterprise incident visibility ● High cross-border impact	● Cybersecurity Law No. 1/2025 ● VPN and platform regulation ● Data retention concerns ● Trust and rights issues	● Cross-border anti-scam cooperation ● Victim-protection intelligence ● Safe capacity building ● AI-enabled fraud tracking

Interpretation: Myanmar should be treated as a regional cybercrime and collaboration challenge, not simply a conventional enterprise cyber maturity comparison. The maturity score should be interpreted cautiously here, since institutional, regulatory and operating conditions materially constrain the availability of comparable cybersecurity evidence.

SOUTH ASIA

India leads the sub-region with established, high-momentum architecture and regulation, while Pakistan, Bangladesh, Sri Lanka, Nepal and Bhutan are at earlier, foundational stages — each showing genuine regulatory or strategic progress in 2025–2026 but facing capacity and implementation gaps.

India · 3.7/5 (Established)

Established, high-momentum architecture and regulation with uneven SME governance

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Advancing	Established	Advancing	Established	Advancing	Established

Key threat pattern	Regulatory direction	ASOCIO priorities
● Phishing, OTP/social-engineering fraud ● BEC and deepfakes ● Ransomware and malware ● API/cloud misconfiguration exploitation	● IT Act 2000 and rules ● CERT-In Directions (2022) ● Digital Personal Data Protection Act ● Sector overlays (banking, telecom)	● Extend Quantum Mission to broader PQC ● SME governance uplift ● Cryptographic-inventory governance ● API/cloud misconfiguration controls

Interpretation: India's National Quantum Mission's early PQC experimentation should extend from banks and government into broader cryptographic-inventory governance.

Pakistan • 2.5/5 (Developing, working estimate)

Governance gap between policy approval and implementation across incident response and recovery

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Developing	Advancing	Developing	Developing	Developing	Advancing

Key threat pattern	Regulatory direction	ASOCIO priorities
● Ransomware, banking disruption risk ● Fraud, credential theft ● AI-assisted deception (deepfakes, voice fraud) ● Digital banking channel risk	● SBP Cyber Shield (roadmap to 2030) ● Proposed national Cyber Security Act ● Pakistan Information Security Framework (draft) ● Dedicated cyber authority proposed	● Separate FI/govt/telecom/SME benchmarks ● AI-fraud preparedness as distinct pillar ● Incident-reporting implementation ● Recovery-testing discipline

Interpretation: Pakistan's biggest governance gap sits between policy approval and actual implementation — incident reporting and recovery testing are the leading indicators to watch.

Bangladesh • 2.2/5 (Developing, working estimate)

Rapid digital growth with foundational legal reforms and capacity-building needs

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Developing	Advancing	Developing	Developing	Developing	Advancing

Key threat pattern	Regulatory direction	ASOCIO priorities
● Malware alerts, critical-service advisories ● Fraud, phishing, credential theft ● Financial cyber risk ● Limited national incident statistics	● Cyber Security Act 2023 ● Data protection reform evolving ● CII concepts exist ● Implementation details need validation	● Capacity building ● Incident data collection ● SME baseline controls ● Financial fraud response

Interpretation: Bangladesh's main opportunity is to translate legal reform and CIRT activity into stronger incident visibility, sector playbooks and workforce capability.

Sri Lanka · 2.4/5 (Developing, working estimate)

Strengthening national resilience with strategy and data-protection framework

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Advancing	Advancing	Developing	Developing	Developing	Advancing

Key threat pattern	Regulatory direction	ASOCIO priorities
● 4,347 incidents (Nat'l Strategy 2025–29) ● Financial scams dominate ● Phishing, ransomware, data breaches ● Public-sector resilience needs	● National Cyber Security Strategy 2025–2029 ● PDPA 2022 and DPA ● No comprehensive Cybersecurity Act yet ● Data-breach notification developing	● Fraud intelligence sharing ● CII resilience guidance ● Cyber workforce programmes ● Government ransomware exercises

Interpretation: Sri Lanka has a clear national strategy and PDPA foundation; execution, sector resilience and workforce depth are the next priorities.

Nepal · 2.4/5 (Developing)

Early-stage architecture constrained by power/connectivity resilience and data-location concerns

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Developing	Developing	Developing	Developing	Developing	Developing

Key threat pattern	Regulatory direction	ASOCIO priorities
● Phishing, social engineering ● Online banking/payment fraud ● Account takeover ● Website defacement, app compromise	● Electronic Transactions Act 2063 (2006/07) ● NRB Cyber Resilience Guidelines ● National Cyber Security Policy context ● Data protection law developing	● Extend governed architecture beyond FIs ● National crypto-inventory baseline ● Power/connectivity resilience planning ● Financial-sector workforce roadmap

Interpretation: Nepal's governed hybrid architecture is concentrated in banks and telecoms — extending that discipline economy-wide is the core resilience task.

Bhutan · 2.3/5 (Developing)

Coherent government-led model constrained by small-market capacity and limited specialist talent

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Developing	Developing	Developing	Developing	Developing	Advancing

Key threat pattern	Regulatory direction	ASOCIO priorities
● Software vulnerabilities, app compromise ● Phishing, online scams ● Ransomware/malware ● Privileged-account compromise, data loss	● Information, Communications and Media Act 2018 ● 13th Five-Year Plan cyber programme ● GovTech / BtCIRT coordination ● Sector overlays developing	● Crypto inventory: ID, gov platforms ● Focused public investment ● Regional partnership for capacity ● SME managed-service pathways

Interpretation: Bhutan's resilience is dependent on focused public investment and regional partnerships, given genuine small-market capacity constraints.

CENTRAL ASIA

Uzbekistan is ASOCIO's Central Asian member economy, with a 2022 cybersecurity law and expanding SaaS adoption running ahead of mature cloud governance.

Uzbekistan · 2.7/5 (Developing)

Rapid regulatory start; SaaS adoption expanding faster than cloud governance

Threat	Reg. & Gov.	Arch. & Tech.	Talent	Future	Regional Collab. †
Developing	Developing	Developing	Developing	Developing	Advancing

Key threat pattern	Regulatory direction	ASOCIO priorities
● Phishing, deepfake-enabled fraud ● Malware, ransomware ● Web-app compromise, known-vuln exploitation ● Localisation shapes public-sector architecture	● Law on Cybersecurity (2022) ● UZCERT active advisory/forecast function ● Data-localisation rules for public sector ● Data protection law developing	● Crypto inventory: ID, payments, telecom ● SaaS governance uplift ● Regional-event convening role (GBSF, ICTWEEK) ● SME cyber baseline

Interpretation: Uzbekistan's fast-growing SaaS adoption needs governance to catch up — and its role hosting regional ICT events is a genuine collaboration asset.

BUILDING TRUST. SHARING INTELLIGENCE. STRENGTHENING REGIONAL CYBER RESILIENCE.

A stronger, more secure digital future for ASEAN and Japan—together.

The cybersecurity landscape is entering a new era.
AI is transforming both attack and defense.
Critical infrastructure is becoming more interconnected.
Cyber threats cross borders in seconds.

**No organization—and no country—can address
these challenges alone.**

AJCCA brings together cybersecurity communities and
strategic partners across ASEAN and Japan to strengthen
cooperation, exchange knowledge, build capabilities, and
create a more resilient regional cybersecurity ecosystem.



OUR PERSPECTIVES



TRUSTED AI ADOPTION

AI should not only be
powerful—it must be
secure, accountable and
trustworthy.

As organizations move toward generative
and agentic AI, security and governance
must evolve at the same speed as
adoption.



RESILIENT CRITICAL INFRASTRUCTURE

A cyber incident can
quickly become an
operational, economic
or public-safety crisis.

Protecting critical infrastructure requires
stronger IT/OT security, shared situational
awareness and collaboration across
sectors and borders.



FROM INFORMATION SHARING TO OPERATIONAL COLLABORATION

Regional cooperation must
evolve beyond meetings
and information exchange.

We move toward actionable threat
intelligence, joint exercises, coordinated
capacity building and trusted incident
collaboration.

THE AJCCA VISION

GOVERNMENT • INDUSTRY • ACADEMIA • CYBERSECURITY COMMUNITIES

WORKING TOGETHER ACROSS ASEAN AND JAPAN TO ADVANCE



CYBER THREAT
INTELLIGENCE



AI & EMERGING
TECHNOLOGY SECURITY



CRITICAL INFRASTRUCTURE
PROTECTION



CYBERSECURITY
CAPACITY BUILDING



PUBLIC-PRIVATE-ACADEMIC
COLLABORATION



REGIONAL KNOWLEDGE &
BEST-PRACTICE EXCHANGE

“Attackers already operate
globally, use AI and share
capabilities very quickly.
Defenders cannot afford
to remain isolated.
The future of cybersecurity
in ASEAN and Japan must be
trusted, interconnected and
collaborative.

— AJCCA

FROM PARTNERSHIP TO COLLECTIVE RESILIENCE

AJCCA believes that cybersecurity resilience cannot be built
by one company, one sector or one country.

Our mission is to help transform regional relationships into
practical cybersecurity collaboration—connecting people,
knowledge and capabilities across ASEAN and Japan.

**TOGETHER, WE BUILD A SAFER
AND MORE RESILIENT DIGITAL REGION.**



CONNECTING COMMUNITIES.



STRENGTHENING TRUST.



BUILDING REGIONAL
CYBER RESILIENCE.



Join AJCCA and be part of a trusted network
building digital resilience across
ASEAN and Japan.



<https://ajcca.net>



info@ajcca.net



[linkedin.com/company/ajcca](https://www.linkedin.com/company/ajcca)

9 ASEAN-JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA) – EXPERT PERSPECTIVES

As part of the **ASOCIO** Regional Cybersecurity Resilience and Maturity Landscape 2026 study, expert views and perspectives were gathered to outline a comprehensive picture of the region's current cyber posture and future trajectory. Rather than focusing solely on static data points or incident metrics, this chapter highlights candid opinions, forward-looking outlooks, and thought leadership from regional partners, including the ASEAN Japan Cybersecurity Community Alliance (AJCCA) comments.

These expert perspectives are qualitative and complementary to, rather than part of, the quantitative respondent survey and maturity scoring.

Transcript

Q1. Regional Threat Forecast

ASOCIO: Looking ahead, what do you see as the most significant emerging cyber threats and attack trends likely to impact organisations across the region over the next 12–24 months?

AJCCA: The next wave of cyber threats will be defined not only by more attacks, but by faster and more intelligent attacks. AI will dramatically lower the barrier for sophisticated phishing, social engineering, malware development and vulnerability exploitation. At the same time, ransomware, supply-chain compromise and attacks against critical infrastructure will remain major regional concerns. ASEAN's growing digital interconnection also means that an incident in one country can quickly become a regional problem.

Q2. Advanced AI / LLM Threats

ASOCIO: Emerging threat vectors targeting commercial LLM providers, such as the so-called Claude Mythos, have raised concern. In your view, how exposed is the region to this kind of AI-specific threat, and how seriously is it being taken?

AJCCA: The region is becoming highly exposed because organisations are adopting AI faster than they are learning how to secure it. Prompt injection, data poisoning, model manipulation, sensitive-data leakage, and attacks against AI agents introduce an entirely new attack surface. The biggest concern is that many organisations still treat AI security as an extension of traditional cybersecurity, when it requires new controls, new skills and new threat models.

Q3. Architecture & Adoption Maturity

ASOCIO: In your view, is the region's pace of adopting cloud, Zero Trust and AI-driven defense keeping pace with the threat landscape or falling behind?

AJCCA: Adoption is moving quickly, but maturity is uneven. Leading organisations are implementing cloud security, Zero Trust and AI-driven defense, while many others are still strengthening basic cyber hygiene and legacy infrastructure. Our challenge is therefore not simply adopting advanced technology but preventing the cybersecurity maturity gap within the region from becoming wider.

Q4. Talent & Skills Gap

ASOCIO: What is your perspective on the region's cybersecurity talent shortage; which skills are becoming hardest to find, and what is the broader business impact of that gap?

AJCCA: The shortage is shifting from simply needing more cybersecurity people to needing people with deeper and more specialized capabilities. Skills in cloud security, OT/ICS security, threat intelligence, incident response, AI security and security architecture are increasingly difficult to find. This is why AJCCA strongly believes that cybersecurity communities must complement universities and industry by accelerating practical learning, mentorship and cross-border knowledge sharing.

Q5. AI Governance Risk

ASOCIO: Which AI-related risks do you believe organisations in the region are most underestimating or least prepared to govern?

AJCCA: One of the most underestimated risks is uncontrolled AI adoption inside organisations. Employees are already putting corporate information into public AI systems, while organisations are deploying AI agents that may access data, applications and business processes. AI governance therefore cannot be only about ethics or compliance; it must also address security, identity, data access, accountability and continuous monitoring.

Q6. Post-Quantum Readiness

ASOCIO: Realistically, how prepared do you think the region is for the shift to post-quantum cryptography and is it receiving enough attention yet?

AJCCA: Post-quantum readiness is still at an early stage across much of the region. Quantum computers may not break today's cryptography tomorrow, but migration itself can take many years. Organisations should start now by identifying where cryptography is used, understanding their long-lived sensitive data, assessing 'harvest now, decrypt later' exposure, and developing a crypto-agility roadmap. Waiting for quantum computing to become an immediate threat will already be too late.

Q7. ASOCIO Collaboration Opportunity

ASOCIO: Where could ASOCIO create the most value for global partners such as your organisation? What kind of regional initiative or collaboration would matter most to you?

AJCCA: ASOCIO can create enormous value by connecting technology industry leadership with operational cybersecurity communities across the region. AJCCA would particularly welcome stronger collaboration in cross-border threat intelligence, AI security, critical infrastructure protection, capacity building and joint exercises. Cyber threats already operate without borders; our defense ecosystem must become equally connected.

Q8. Strategic Priorities for the Region

ASOCIO: Over the next 24 months, where should ASOCIO and the broader regional ecosystem focus their efforts to strengthen digital resilience?

AJCCA: I would prioritize three things: trusted AI adoption, stronger protection of critical infrastructure, and deeper regional cybersecurity collaboration.

Trusted AI Adoption: We should not slow down AI adoption; we should make AI adoption trustworthy. Every organisation needs to know what AI it is using, what data the AI can access, what actions it can perform, and who remains accountable when something goes wrong.

Protection of Critical Infrastructure: Critical infrastructure cybersecurity is no longer only about protecting computers. A successful cyberattack can become an operational, economic and even public-safety crisis. We therefore need to protect critical infrastructure as an interconnected regional ecosystem, not as isolated organisations.

Operational Collaboration: The region already has many cybersecurity partnerships. The next step is to make those partnerships operational, moving from information sharing to operational collaboration by sharing actionable threat intelligence, conducting joint exercises, developing regional capabilities and responding collectively to cross-border incidents. Regional resilience will ultimately depend not only on technology, but on how effectively we can trust and work with one another.

ASOCIO would like to express its sincere appreciation to **AJCCA** for these valuable views and perspectives, which have contributed significantly to this study.



10. APPENDIX A: SOURCE REFERENCES BY ECONOMY

The economy studies underlying this consolidated report drew on national CERT/CIRT advisories, government and regulator publications, and reputable industry and news reporting. The references below are organised by economy for traceability; a small number of regional cross-cutting references appear at the end.

Source hierarchy: Primary government, regulatory, CERT/CIRT and legislative sources were prioritised where available. Secondary legal, industry and media sources were used to supplement areas where primary evidence was unavailable or insufficient.

OCEANIA

Australia

- RSM Australia, Cyber Security Report 2026 – rsm.global/australia/reports/cyber-security-report/2026
- Australian Cyber Security Centre, Ransomware payment and cyber extortion payment reporting – cyber.gov.au
- Allens, SOCI Act 2.0: sweeping reforms proposed to Australia's critical infrastructure framework (Jul 2026) – allens.com.au
- SecurityBrief Australia, Australia critical infrastructure rules tighten risk – securitybrief.com.au
- Australian Government Dept. of Home Affairs, Cyber Security Strategy – Horizon 2 – homeaffairs.gov.au
- Clyde & Co, Introduction of the mandatory ransomware and cyber extortion payment reporting (2025) – clydeco.com
- Dept. of Home Affairs, Ransomware Payment Reporting factsheet – homeaffairs.gov.au
- Cyber and Infrastructure Security Centre, Cyber security ransomware reporting rules – cisc.gov.au
- Landers, Enhanced Critical Infrastructure Risk Management Program Rules 2026 – landers.com.au
- Australian Computer Society, Australia's first Cyber Security Act becomes law – ia.acs.org.au

New Zealand

- New Zealand NCSC, Cyber Threat Report 2025 — ncsc.govt.nz
- Office of the Privacy Commissioner NZ — privacy.org.nz
- Privacy Commissioner, speech to the 2026 National Cyber Security Summit — privacy.org.nz
- GCSB, Annual Report 2025 — gcsb.govt.nz
- CERT NZ / NCSC, Report a cyber issue — ncsc.govt.nz

NORTHEAST ASIA

Japan

- Japan National Cybersecurity Office (NCO) — cyber.go.jp/eng
- Personal Information Protection Commission / Japanese Law Translation, APPI — japaneselawtranslation.go.jp
- JPCERT/CC, Incident Handling Report Q4 2024 (Jun 2025) — jpcert.or.jp
- AP News, Japan links MirrorFace to cyberattacks targeting security and technology data (Jan 2025) — apnews.com

South Korea

- Personal Information Protection Commission (PIPC) Korea — pipc.go.kr/eng
- Korea Internet & Security Agency (KISA) — kisa.or.kr/EN
- Chambers, South Korea Cybersecurity 2026 guide — practiceguides.chambers.com
- DLA Piper, PIPA legal update — dlapiperdataprotection.com
- Reuters, South Korea orders SK Telecom to strengthen data security after leak (Jul 2025) — reuters.com
- Inter-American Development Bank, National Cybersecurity Law, Governance and Infrastructure in the Republic of Korea — publications.iadb.org

Taiwan

- Reuters, Chinese cyberattacks on Taiwan infrastructure averaged 2.6 million/day in 2025 (Jan 2026) — reuters.com
- Foundation for Defense of Democracies, China wants to switch off Taiwan's critical infrastructure (Jan 2026) — fdd.org
- Chambers, Cybersecurity 2026: Taiwan trends and developments — practiceguides.chambers.com
- Chambers, Artificial Intelligence 2026: Taiwan trends and developments — practiceguides.chambers.com
- Taipei Times, National Security Bureau report (5 Jan 2026) — taipeitimes.com
- CyberScoop, Taiwan-China cyberattacks 2025: energy, hospitals, NSB report — cyberscoop.com
- CSO Online, Taiwan subjected to 2.6 million Chinese cyberattacks a day in 2025 — csoonline.com
- MODA (Taiwan), press report on CSMA amendments — moda.gov.tw
- Laws & Regulations Database of the Republic of China, AI Basic Act — law.nstc.gov.tw

Hong Kong

- HKCERT, Hong Kong Cyber Security Outlook 2025 (Jan 2025) — [hkcert.org](https://www.hkcert.org)
- Hong Kong e-Legislation, Cap. 653 Protection of Critical Infrastructures (Computer Systems) Ordinance — [elegislation.gov.hk](https://www.elegislation.gov.hk)
- Office of the Commissioner of Critical Infrastructure (Computer-system Security), Code of Practice v1.0 — [occics.gov.hk](https://www.occics.gov.hk)
- HKMA, Cybersecurity Fortification Initiative and C-RAF — [hkma.gov.hk](https://www.hkma.gov.hk)
- PCPD Hong Kong, Data Breach Notification guidance — [pcpd.org.hk](https://www.pcpd.org.hk)

Macau

- Polícia Judiciária de Macau, Cybersecurity Law information — [pj.gov.mo](https://www.pj.gov.mo)
- Polícia Judiciária de Macau, CARIC commencement and mandate — [pj.gov.mo](https://www.pj.gov.mo)
- AMCM, Technology and Cyber Risk Management Guideline (2023) — [amcm.gov.mo](https://www.amcm.gov.mo)
- AMCM, Cloud Outsourcing Guideline (2025) — [amcm.gov.mo](https://www.amcm.gov.mo)
- Macau SAR Government, 2025 Policy Address — [gov.mo](https://www.gov.mo)

Mongolia

- Global Cyber Security Capacity Centre (Oxford), Mongolia Cybersecurity Capacity Review 2024 — [gcsc.ox.ac.uk](https://www.gcsc.ox.ac.uk)
- Institute for Strategic Studies Mongolia, cybersecurity impact assessment — [en.iss.gov.mn](https://www.en.iss.gov.mn)
- Cyber Security Council of Mongolia — [cscouncil.gov.mn](https://www.cscouncil.gov.mn)
- DLA Piper, Mongolia data protection law overview — [dlapiperdataprotection.com](https://www.dlapiperdataprotection.com)
- Communications Regulatory Commission of Mongolia, National Anti-Fraud System — [crc.gov.mn](https://www.crc.gov.mn)

SOUTHEAST ASIA

Singapore

- Cyber Security Agency of Singapore, Cybersecurity Act — [csa.gov.sg](https://www.csa.gov.sg)
- CSA, Singapore Cyber Landscape 2024/2025 — [isomer-user-content.by.gov.sg](https://www.isomer-user-content.by.gov.sg)
- Personal Data Protection Commission Singapore — [pdpc.gov.sg](https://www.pdpc.gov.sg)
- MAS, Technology Risk Management Guidelines — [mas.gov.sg](https://www.mas.gov.sg)

Malaysia

- NACSA, Cyber Security Act 2024 (Act 854) — [nacsa.gov.my](https://www.nacsa.gov.my)
- NACSA, legal instruments and baselines — [nacsa.gov.my](https://www.nacsa.gov.my)
- MyCERT, Q1 2025 incident summary — [mycert.org.my](https://www.mycert.org.my)
- MyCERT, Q4 2025 incident summary — [mycert.org.my](https://www.mycert.org.my)
- Cyfirma, Malaysia Threat Landscape Report — [cyfirma.com](https://www.cyfirma.com)
- PwC Malaysia, AI, quantum and trust: the new shape of cyber risk — [pwc.com](https://www.pwc.com)

Thailand

- Thailand National Cyber Security Agency (NCSA) — nrsa.or.th
- DLA Piper, Thailand PDPC clarification on personal data breach notification (2025) — privacymatters.dlapiper.com
- Legal 500, Thailand Data Protection & Cybersecurity guide — legal500.com
- Google Cloud, NCSA and Google Cloud to bolster AI-powered cyber defence (Apr 2025) — googlecloudpresscorner.com

Philippines

- DICT, National Cybersecurity Plan 2023–2028 — cms-cdn.e.gov.ph
- National Privacy Commission Philippines — privacy.gov.ph
- DLA Piper, Philippines data-breach timelines — dlapiperdataprotection.com
- Cyberint, Philippine Threat Landscape Report 2024–25 — cyberint.com
- Cyfirma, Philippines Evolving Cyber Threat Landscape 2025–2026 — cyfirma.com

Indonesia

- GovInsider, Collaboration is the key to Indonesia cyber resilience — BSSN, Perpres 47/2023 — govinsider.asia
- Reuters, Indonesia president orders audit of data centres after cyberattack (Jun 2024) — reuters.com
- DLA Piper, Indonesia PDP Law overview — dlapiperdataprotection.com
- Chambers, Data Protection & Privacy 2026: Indonesia — BSSN Reg. No. 1/2024 — practiceguides.chambers.com

Vietnam

- Duane Morris, Vietnam Law on Cybersecurity 2026: what you must know (Jan 2026) — blogs.duanemorris.com
- Vietnam Briefing, Vietnam's cybersecurity and data protection rules: a compliance roadmap — vietnam-briefing.com
- VietNamNet, Digital transformation fuels demand for cybersecurity talent — vietnamnet.vn
- IPSIP, Cybersecurity Report in Vietnam Q1 2026 — ipsip.vn
- DataGuidance, Vietnam government issues implementation guidance — dataguidance.com
- Tilleke & Gibbins, Vietnam issues new Cybersecurity Law — tilleke.com
- DFDL, Vietnam's new Cybersecurity Law to take effect 1 July 2026 — dfd.com
- Ministry of Public Security (Vietnam), National Assembly passes Law on Cybersecurity — en.bocongan.gov.vn
- Xinhua, Vietnam cybersecurity law coverage (Dec 2025) — english.news.cn
- VNETWORK, Vietnam Cyber Attack Report 2026 — vnetwork.vn

Brunei

- East-West Center, Asia Pacific Bulletin — Brunei (Mar 2025) — eastwestcenter.org
- Cyber Security Brunei (CSB) — csb.gov.bn
- CSB, Stack 2026 — csb.gov.bn
- ENISA, NIS360 2026 — enisa.europa.eu
- World Economic Forum, Global Cybersecurity Outlook 2026 — Regional Analysis: Middle East and North Africa — reports.weforum.org

Cambodia

- DLA Piper, Cambodia data protection status — dlapiperdataprotection.com
- Lexology, Cambodia draft personal data law update — lexology.com
- Khmer Times, Cybersecurity preparedness critical for inclusive growth — khmertimeskh.com
- Reuters, Cambodian parliament passes landmark cybercrime law after scam-centre scrutiny (Apr 2026) — reuters.com
- FACT (Cambodia), Cybersecurity in Cambodia: new laws but a range of challenges remain — factsasia.org

Laos

- World Economic Forum, Global Cybersecurity Outlook 2026 — Regional Analysis: East Asia and Pacific — reports.weforum.org
- Xinhua, Laos cybersecurity coverage (Dec 2025) — english.news.cn
- Security Studies Info, Laos country report (Feb 2026) — securitystudies.info
- Asia IP Law, Laos publishes new Law on Cybersecurity — asiaiplaw.com
- UNDP, Lao PDR Digital Maturity Assessment 2022 — undp.org
- Internet Laos, Building digital trust: understanding the 2026 Laos Law on Cybersecurity — internetlaos.com

Myanmar

- Myanmar Cybersecurity Law No. 1/2025 (English translation) — lincolnmyanmar.com
- Tilleke & Gibbins, Myanmar Cybersecurity Law takes effect (Aug 2025) — tilleke.com
- AP News, Myanmar military rulers enact cybersecurity law with censorship provisions (Jan 2025) — apnews.com
- AP News, Myanmar military shuts down major cybercrime centre, detains 2,000+ (2025) — apnews.com

SOUTH ASIA

India

- CERT-In — cert-in.org.in
- CERT-In, Directions under Section 70B (2022) — cert-in.org.in
- Ministry of Electronics & IT, Digital Personal Data Protection Act framework — meity.gov.in
- Economic Times, Only 7% of organisations in India ready for cyber threats — Cisco report (2025) — economictimes.indiatimes.com
- Times of India, PwC flags \$1M hit for Indian firms; AI/cloud security budgets set to rise — timesofindia.indiatimes.com

Pakistan

- Arab News, Pakistan cybersecurity coverage — arabnews.com
- ProPakistani, Govt prepares new security system to hunt hackers (Jul 2026) — propakistani.pk
- The Nation, Pakistan's AI trust challenge — can it be fixed (Jun 2026) — nation.com.pk
- LetsDataScience, Pakistan strengthens banking cybersecurity with Cyber Shield — letsdatascience.com
- State Bank of Pakistan, Cyber Shield circular CL01/2026 — sbp.org.pk
- Pakistan Telecommunication Authority, Cyber Security Annual Report 2024-25 — pta.gov.pk
- National Assembly of Pakistan, proposed Cyber Security Act draft — na.gov.pk
- Senate of Pakistan, related legislative documents — senate.gov.pk
- ProPakistani, Pakistan to get first dedicated cybersecurity authority (Nov 2025) — propakistani.pk
- Ministry of IT & Telecom Pakistan, Digital Pakistan Monitor (May 2026) — moitt.gov.pk / fnpk.org

Bangladesh

- BGD e-GOV CIRT portal and alerts — cirt.gov.bd
- ICNL, Bangladesh Cyber Security Act 2023 Handbook (Nov 2024) — icnl.org
- DataGuidance, Bangladesh Personal Data Protection Ordinance 2025/2026 summaries — dataguidance.com

Sri Lanka

- Sri Lanka CERT, National Cyber Security Strategy 2025–2029 — cert.gov.lk
- Sri Lanka Data Protection Authority — dpa.gov.lk
- Parliament of Sri Lanka, Personal Data Protection Act No. 9 of 2022 — parliament.lk
- LIRNEasia, Cybersecurity policy considerations for Sri Lanka (Jan 2026) — lirneasia.net

Nepal

- Office of the Attorney General Nepal, National Cyber Security Policy context — ag.gov.np
- Government of Nepal, A Study on Cyber Crime Cases in Nepal 2022 — giwmscdnone.gov.np
- Nepal Rastra Bank, Cyber Resilience Guidelines — nrb.org.np
- DLA Piper, Nepal data protection law overview — dlapiperdataprotection.com
- Nepalnews, Cybersecurity roadmap for BFIs handed to governor — english.nepalnews.com

Bhutan

- Bhutan National Data Governance Baseline Report 2024 — tech.gov.bt
- Royal Government of Bhutan, 13th Five-Year Plan — trashiyangtse.gov.bt
- GovTech Agency, 13th FYP cybersecurity programme — tech.gov.bt
- GovTech / BtCIRT services — tech.gov.bt

CENTRAL ASIA

Uzbekistan

- UZCERT, Forecast of major cyber threats in Uzbekistan for 2025 — uzcert.uz
- UZCERT, statistics and services — uzcert.uz
- Lex.uz, Law of the Republic of Uzbekistan on Cybersecurity — lex.uz
- DLA Piper, Uzbekistan data protection law overview — dlapiperdataprotection.com
- AI Committee Uzbekistan, public-sector AI use guide — ai.gov.uz

Regional and cross-cutting references

- INTERPOL, Asia and South Pacific Cyber Threat Assessment Report 2025/2026 — interpol.int
- World Economic Forum, Global Cybersecurity Outlook 2026 — weforum.org
- NIST, Post-Quantum Cryptography project and migration guidance — nist.gov/pqc
- ASOCIO, Member Economies & Representatives — asocio.org
- ASOCIO, Mongolian Software Industry Association (MOSA) officially rejoins ASOCIO (26 May 2026) — asocio.org

11. Appendix B: Survey Methodology and Interpretation Notes

This appendix records the controls applied when integrating the organisational survey with the 25-economy desk-research report.

- Base dataset: organisational responses from 21 economies.
- Question-level denominators vary because of partial completion and conditional incident questions.
- Multiple-response questions can sum to more than 100%.
- The survey instrument does not contain a numeric maturity scoring formula aligned to the five maturity pillars used in this report, pillar-level scores, or a mapping from answers to the 1–5 maturity scale.
- Accordingly, the 25-economy maturity ranking is retained as a separate desk-research assessment and is not described as a survey-derived index.
- Future survey waves should consider stratified economy targets, minimum response thresholds for economy-level reporting, and an explicit reproducible maturity instrument if ASOCIO wishes to publish respondent-derived maturity scores.

Final editorial conclusion

Taken together, the evidence points to a region in which cyber resilience is moving from policy and compliance toward demonstrated operational capability. The desk research shows a wide maturity spread across 25 economies; the respondent survey shows that organisations across that spread are converging on the same pressure points — AI risk, ransomware, talent scarcity, uneven Zero Trust, weak PQC readiness and the need for stronger regional cooperation. The practical opportunity for ASOCIO is therefore not to make every economy look the same, but to create shared visibility, interoperable response mechanisms and faster transfer of proven practice across the region.

This report should be treated as a final report issued for stakeholder validation prior to publication. Maturity scores marked "Working estimate" (indicative), all cloud/architecture adoption percentages, and all recently enacted legislative provisions should be validated with the respective national ICT associations, CERTs and legal counsel before any external or public release.

Use of Artificial Intelligence

Artificial intelligence tools were used selectively in the preparation of this report to support activities such as research synthesis, language refinement, consistency checking, data presentation and editorial review. The underlying survey data, research inputs, analysis, validation and substantive conclusions were developed from the work of the ASOCIO Cybersecurity Survey 2026 research team and participating respondents. AI-generated or AI-assisted content was reviewed, verified and refined by the research team before inclusion. Responsibility for the interpretation, accuracy and final content of this report remains with the authors and the research team

ACKNOWLEDGEMENT

ASOCIO extends its deepest appreciation to the ASOCIO Policy Task Force Committee for its exemplary leadership and unwavering commitment in guiding the development of this landmark study. We also convey our sincere gratitude to the many distinguished experts, institutions, Member Economies, and Global Partners across the Asia–Oceania region whose insights and support have been invaluable throughout this process.

This report draws upon research, data, and guidance from leading global agencies, including the OECD, UNESCO, the European Commission, the U.S. National Institute of Standards and Technology (NIST), and the World Economic Forum, together with regional initiatives across Asia. Their collective contributions have been instrumental in shaping a balanced, comprehensive, and evidence-based perspective on cyber resilience, digital trust, and future readiness within the region.

ASOCIO also acknowledges the participation of organisations across 21 economies in the ASOCIO Cybersecurity Survey 2026, whose practitioner insights enriched and validated the findings of this study. Their engagement ensures that the report reflects both policy frameworks and lived operational realities, strengthening its relevance for governments, industry, and society.

Together, these contributions have enabled ASOCIO to deliver a consolidated, comparative, and forward-looking assessment that will serve as a foundation for advancing cyber resilience and regional collaboration across Asia–Oceania.

Stronger Together
for a Digital Future



ASOCIO

Mapping ASOCIO Digital Economy

MAPPING ASOCIO DIGITAL ECONOMY (M.A.D.E.)



CONNECTING
ECOSYSTEMS



DRIVING
INNOVATION



ACCELERATING
DIGITAL ECONOMY



EMPOWERING
MEMBER ECONOMIES



BUILDING A
SUSTAINABLE FUTURE



Asian-Oceanian Computing Industry Organization
(ASOCIO)

 www.asocio.org



ASOCIO

Mapping ASOCIO Digital Economy

www.asocio.org