ASIAN SCHOOL OF CYBER LAWS

# Cyber Security Checklist for Banks: 20 Questions to Ask

Tick each question you can answer with a confident yes. Every unticked box is a place to start.

## VISIBILITY

01 ☐ Do we know every system and person that can initiate or approve payments?

02 ☐ Do we know which suppliers can reach payment systems, customer data or admin tools?

03 ☐ Do we have a current inventory of internet-facing systems and cloud services?

## ACCESS

04 ☐ Is phishing-resistant MFA used for everyone who can approve payments or administer systems?

05 ☐ Are privileged accounts granted just in time and monitored?

06 ☐ Is support staff access to customer data limited to what they need?

## NETWORK

07 ☐ Are payment systems and signing infrastructure isolated in restricted network zones?

08 ☐ Are internet-facing systems patched quickly when vulnerabilities are exploited?

09 ☐ Are cloud configurations checked continuously?

## DETECTION

10 ☐ Would we detect an unusual payment from the bank's own accounts in real time?

11 ☐ Do we monitor for unusual access and bulk downloads by staff and suppliers?

12 ☐ Do we monitor around the clock for intruders?

## RESILIENCE

13 ☐ Are there limits on how much can be paid out, how fast and to where?

14 ☐ Are backups of core systems stored offline and tested?

15 ☐ Could we reconcile accounts and restore services after a major attack?

## RESPONSE

16 ☐ Can we halt outgoing payments within minutes if needed?

17 ☐ Do we have contacts ready at other banks, exchanges and law enforcement to freeze funds?

18 ☐ Have we run a crisis exercise on payment fraud or ransomware in the last 12 months?

## PEOPLE AND GOVERNANCE

19 ☐ Are staff trained to resist deepfakes, impersonation and bribery?

20 ☐ Does the board receive regular reporting on cyber and third-party risk?