



ISACA®

Malaysia Chapter

NOVEMBER 2025

Deciphering PQC: Future-Proofing Crypto Strategy Workshop



Exclusive two-day workshops for ISACA Malaysia Members

Event Details

DATE: 18 - 19 NOVEMBER 2025

TIME: 9 .00AM - 5.00PM

VENUE: TBD

ISACA Members RM 2,480

Non Members RM 3,080

Fees exclude 8% SST

ELIGIBLE FOR 14 CPE HOURS

REGISTER AT [ISACA MY CHAPTER ENGAGE](#)

About the workshop

The mantra of any good security engineer is: "Security is not a product, but a process." It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.

Bruce Schneier

Currently, the appreciation of cryptography as the last line of defense (or offense) has grown tremendously. Organisations are protecting their data by encrypting and digital signing, including among others for DLP and integrity of logs.

Cryptography is based on mathematical functions only the privilege few understand. Nonetheless the strength of cryptography is also based on the processing power to compute the mathematical functions or algorithms. From Caesar cipher, we are now in the advent of quantum computing, hence Post Quantum Cryptography (PQC).

As quantum computing advances, the cryptographic algorithms protecting our financial and government systems today will be obsolete tomorrow. Are you ready to lead the transition? Join us to gain the insight on how to prepare for PQC transition.

What you'll learn

Understand the Current Cryptography types and Use Cases

- Gain a solid insight in understanding the cryptography function in layman's terms. With the understanding, the expectation of applications in data in motion, data in use and data at rest would be set correctly.

Emphases on the needs of PQC

- History of PQC
- Current Development of PQC

Cryptography Risk Assessment

- Participants will be walked through of how to identify assess their cryptography risk in relations to use cases. The risk assessment will be an integral part of the transition planning

Transition Planning and roadmapping

- Participants will be coached on the thought process of how to plan for PQC readiness based on risk assessment.

Pitfalls, Case Studies and Enablers

- Participants will be discussing the key success factor in the transition to PQC. Regulatory enablers will be factored in.

Key Takeaways

- The background of PQC
- Current Cryptography and Future State
- Cryptography Risk Considerations.
- Designing transition roadmap for PQC
- Awareness on the key success factor of transition
- Practical thought process in implementing cryptography transition roadmap.

Who should attend

This workshop is also designed for leaders, strategists, and technical professionals responsible for

- Cybersecurity Strategy & Architecture
- IT & Network Security
- Data Protection & Privacy
- Compliance & Risk Management
- Product Development & Innovation
- Senior Management concerned with long-term organizational resilience

About the training

DAY 1

1

Module 1: Applied Cryptography Development

- a. History of Cryptography
- b. Types of Cryptography
- c. Use Cases of Cryptography

2

Module 2: The State of PQC

- a. Current Development in PQC Standards
- b. Hybrid Cryptography Model
- c. Roles of Standardisation / Certification Bodies

DAY 2

3

Module 3: Cryptography Risk and Vulnerability

- a. Cryptography assets and Protocols
- b. Identifying High Risk System

4

Module 4: Transition Planning and Enablers

- a. Association of transition program with Risk Management.
- b. Application Readiness
- c. Peer review and expert feedback.

Speaker Profile

Ami is an experienced security professional who focuses on cryptography, secure software development and IT Operations for over 25 years. He was the CTO and subsequently a CEO of Licensed Certification Authorities (CA) where he built the foundation in terms of compliance and innovation. He has also led a Public Key Infrastructure based software development organization in addition to serving a 'Big Four' firm in Cyber Risk Advisory. Ami has also presented in international conference on cryptography and PKI topic. Key PKI project initiatives experience and exposures : -

- Handling business and CA operations of three licensed CAs in Malaysia. Part of the Service include Private Cloud Certificate as a Service and Secure Signed QR code application
- Setting up the PKI based e-passport compliant to ICAO 9303 standards for Malaysia and Iraq
- Project Director (System Integrator) for Government PKI initiative
- Project Director for setting up of an internal Security Operations Centre for an aviation company
- Managed the provisional cross signing of root key between Malaysia and Thailand
- Cryptography Assessment for three financial institutions based on the requirements of RMiT by BNM
- Speaker / Trainer in PKI related conference such as Saudi PKI conference, ASEAN PKI conference, DepKomInfo Cryptography Training.



**AMI AZRUL
ABDULLAH**

Contact us for more details



ISACA®

Malaysia Chapter

W: [HTTPS://ENGAGE.ISACA.ORG/MALAYSIACHAPTER/EVENTS/](https://engage.isaca.org/malaysiachapter/events/)

E: OFFICEADMIN@ISACA.ORG.MY

M: 6017 219 6225 (JAYASEELAN)



Important Notice

As good practice, ISACA Malaysia Chapter is informing you that your personal data will be processed, retained and used by ISACA Malaysia Chapter in relation to this training event. Your personal data may also be retained and used by ISACA Malaysia Chapter to market and promote training events conducted by ISACA Malaysia Chapter.