



gaskita
Juaranya Gas Ngalir Terus

by **PGN**



PLN

Konferensi Auditor Internal **GOVERNANCE 5.0** Redefining Board Oversight and Internal Audit in a Digital-First Era



www.ypia.id

kai@ypia.id

[d](#) [@](#) [f](#) [in](#) [ciar.ypia](#)

[ciar-tv](#)

Strengthening Internal Audit Capability in Enhancing Cyber Resilience of the Banking Sector

Yulianto Setiawan

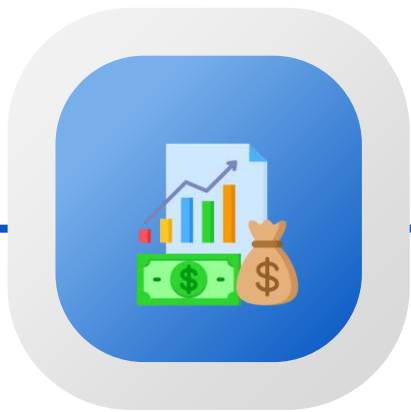
SEVP Satuan Kerja Audit Intern
PT Bank Rakyat Indonesia (Persero) Tbk.

Yogyakarta | 9 Juli 2026

This document and the information contained herein for Konferensi Auditor Internal on July 9, 2026, are proprietary to PT Bank Rakyat Indonesia (Persero) Tbk. and shall not be published or disclosed to any third party without the express written consent of an authorized representative of PT Bank Rakyat Indonesia (Persero) Tbk.



Strengthening Internal Audit Capability in Enhancing Cyber Resilience of the Banking Sector



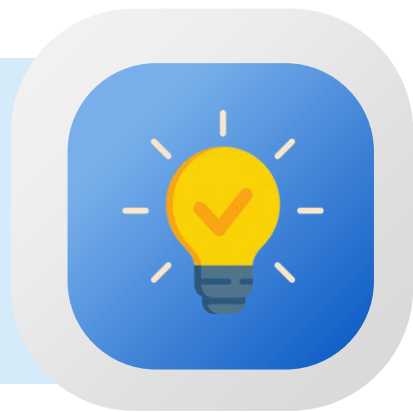
**Banking
Transformation**



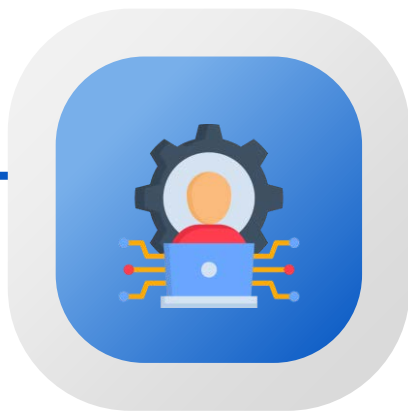
**Cyber Risk
Exposure**



**Cyber
Resilience**



**Key
Takeaways**



**Internal Audit
Role**

Established in 1895, BRI has been serving the community with the widest reach across Nusantara

With a large customer base and extensive digital channels, cyber resilience becomes a strategic necessity to protect service continuity, customer data, and public trust.



10

Perusahaan
Anak



>7.300

Jaringan Unit
Kerja



6 Titik

Kantor Luar
Negeri



>167 Jt

Nasabah



>4,6 Jt

Titik QRIS



>1,18 Jt

BRILink Agent



>47 Jt

User yang
terdaftar di BRImo



>637 rb

Titik e-channel



2.250 T

Aset



1.555 T

Dana Pihak
Ketiga



1.562 T

Total Kredit



15,5 Tn

Laba bersih





Bank is a technology company with a banking license

Brett King - Author

Bank 1.0	Bank 2.0	Bank 3.0	Bank 4.0	Bank 5.0
Branch Banking (Pre – 1960s)	Multi-channel Banking (1960s – 1980s)	Digital Banking (1990s – 2010s)	Embedded Banking (2010 – present)	Intelligent Banking
Banking was centered on physical branches and personal relationships between customers and bank managers.	Banks began using automation and offering services beyond office hours.	Customers began using online banking and mobile banking.	Banks became part of an open ecosystem with fintech and third-party providers.	Banking becomes more intelligent, personalized, integrated, and less visible as a traditional banking service.
Face-to-face Service	ATM	Internet Banking	Open Banking	AI Banking Assistant
Manual Records	Credit & Debit Card	Mobile Banking	API	Biometrics Authentication
Physical Transactions	Computerized Transactions	Digital Payments	Fintech Collaboration	Voice Banking
Cyber/Fraud exposure: ☐ Cheque forgery ☐ embezzlement ☐ human error ☐ Etc.	Cyber/Fraud exposure: ☐ Card Skimming ☐ Counterfeit Cards ☐ IT Vulnerabilities ☐ Etc.	Cyber/Fraud exposure: ☐ Data Breach ☐ Phishing ☐ Malware ☐ Etc.	Cyber/Fraud exposure: ☐ API Risk ☐ Third-party Risk ☐ Cloud/Data Leakage ☐ Etc.	Cyber/Fraud exposure: ☐ AI Risk ☐ Deepfake ☐ Biometric Risk ☐ Etc.

The expansion of digital services, open ecosystems, and interconnected technologies has significantly increased cyber risk exposure globally.

2026 Technology Risk Focus

KPMG positions technology risk as one of the key risk in the 2026 risk landscape

79%

Cybercrime &
Cyber Insecurity

69%

Regulatory
Demands

57%

Geopolitical
Conflicts

Top 3 Technology Risk 2026 (KPMG)



1 Data & Information Governance



2 AI Technology



3 Cybersecurity

Technology risks shaping both boardroom investment decisions and internal audit plans worldwide

Source: KPMG, 2025 CEO Outlook

GLOBAL TREND

42%

Cyber risk remains the #1 business risk globally

5 years

Consistently ranked as the top concern by executives

36%

Cyber risk ranked #1 across Asia Pacific

Source: Allianz Risk Barometer 2026

INDONESIA TREND

5.5 Billion

Cyberattacks recorded in Indonesia throughout 2025 and 714% jump from the 2020–2024 average

Source: BSSN (June 2026)

Rp700 M

Total Losses Caused by AI-Enabled Fraud Schemes

Source: BSSN (July 2025)

52%

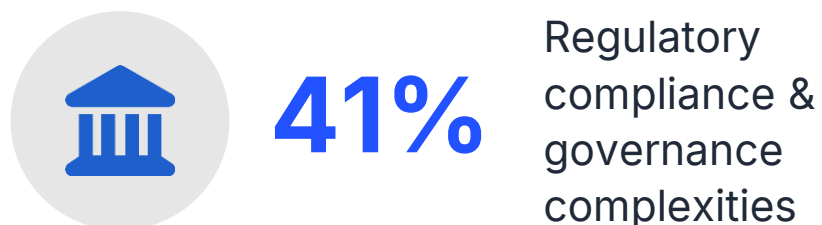
of DDoS attacks on banking websites and apps worldwide were aimed at banks in the APAC region

Source: Liputan6 (6 Jun 2026)



Cyber risk is no longer an IT issue, it is a strategic business risk that can disrupt operations, erode customer trust, and threaten financial stability.

Challenge Snapshot

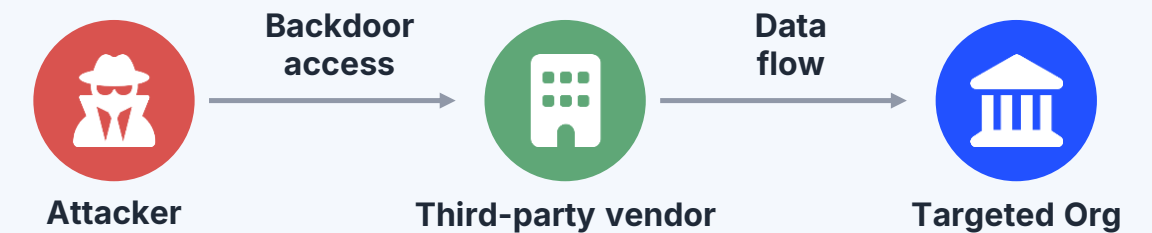


Typical gaps in less resilient organizations

- Lack of funds **63%**
- Cybersecurity skills shortage **56%**
- Limited visibility across IT/OT/IoT **56%**

Why Supply Chain Risk Matters

“Over the past five years, major supply chain third-party breaches increased sharply, with incidents quadrupling”



Threat Priority Perspective



What More Resilient Organizations Do



Cyber resilience is no longer only an internal technology issue. It increasingly depends on how effectively the organization governs third-party ecosystems, embeds security in procurement, and tests joint response readiness.

1 Human Error Remains a Key Weakness in Cyber Resilience

People-related vulnerabilities continue to enable cyberattacks and amplify operational disruption.

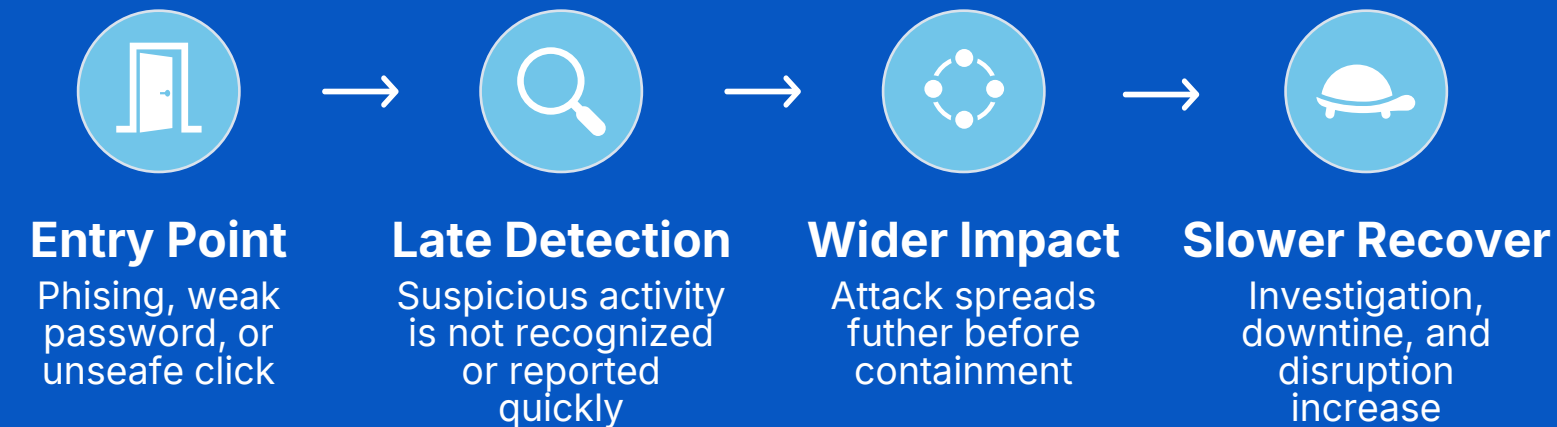
60%
of breaches involved the human element (2025)

62%
of breaches involved the human element (2026)

16%
of breaches involved social engineering (2026)

54% vs 12%
AI-automated phishing click-through rate vs standard phishing (2025)

How Human Error Weakens Cyber Resilience

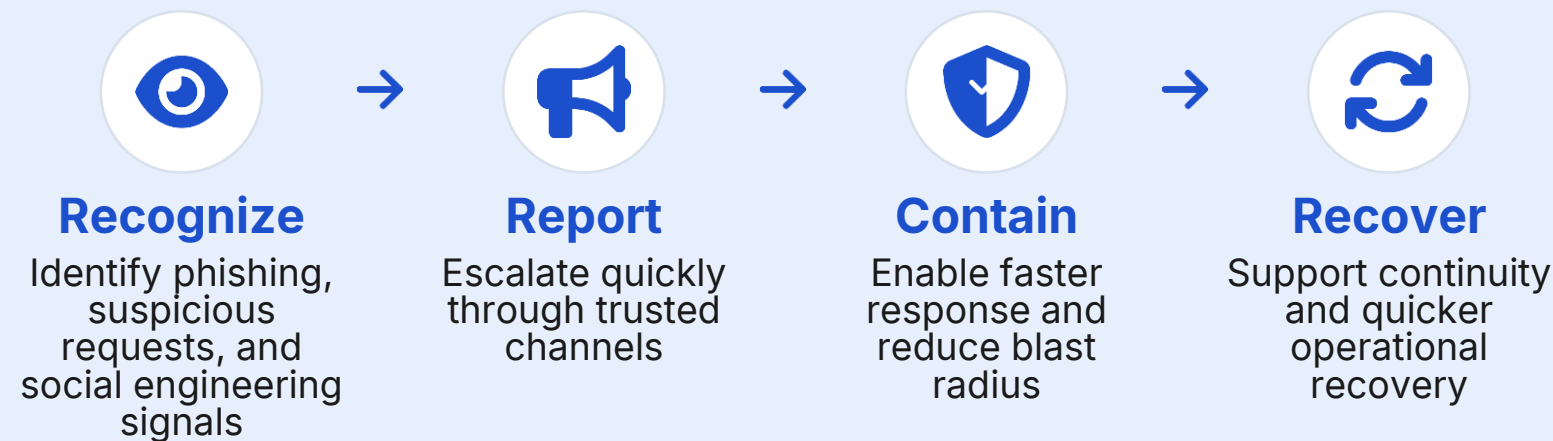


✗ Human risk not only drives initial compromise, but also increases investigation burden, slows response, and prolongs recovery.

2 Human Firewall Strengthens Cyber Resilience

A human firewall is a trained, aware, and motivated workforce that acts as the first line of defense when technical controls are bypassed.

A. Mechanism: From Awareness to Action



B. Impact & Evidence

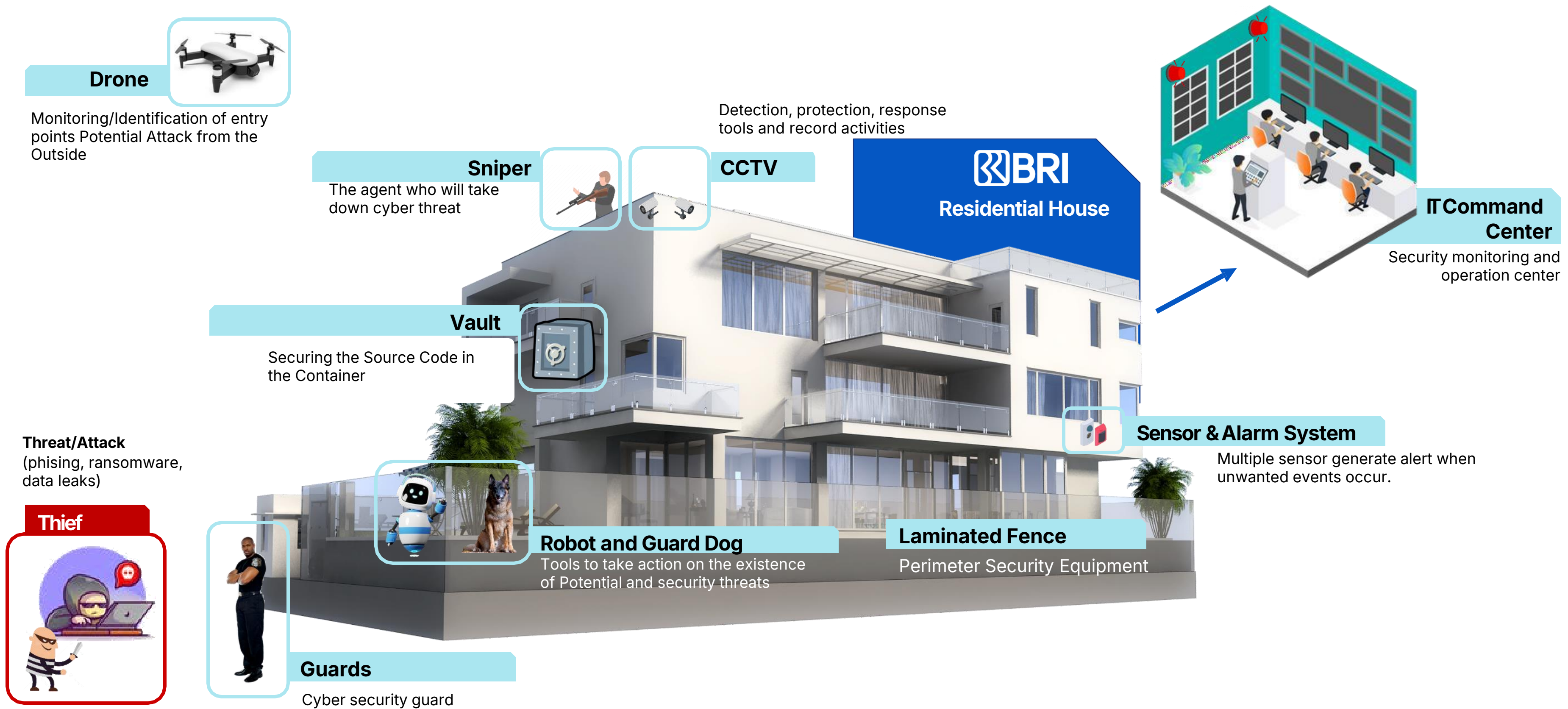
57,9%
Security awareness is the strongest predictor of phishing mitigation behavior

48,9%
Security awareness strongly predicts reporting behavior

76%
High-resilience organizations provide training and awareness programs

🎯 **Training is most effective when it builds lasting awareness and everyday habits — not when it is compliance-only.**

An analogy illustrating how securing BRI's operational systems is similar to securing our homes



Why Internal Audit Matters in Cyber Resilience?

Cyber resilience is not only an IT responsibility, but a strategic business priority.

While NIST CSF provides the structure for managing cyber risk, **internal audit provides independent assurance to ensure that the framework is effectively implemented across governance, risk management, and control processes.**



Cybersecurity is a top CAE concern, but audit plan allocation remains disproportionately low.



Priority and plan allocation are not yet fully aligned.

RISK PERCEPTION

86%

North American **CAEs** identify **cybersecurity** as a Top 5 organizational risk.



73%
Global average



83%
highest audit priority
in North America

Source: IIA, Cybersecurity Topical Requirement (2025)

AUDIT COVERAGE

9% of total **audit plan** allocation is devoted to cybersecurity.

Audit plan allocation comparison (North America)



Source: IIA, 2026 North American Pulse of Internal Audit

The core issue is not awareness, but the gap between perceived cyber risk and actual audit coverage

STRATEGIC IMPLICATIONS FOR INTERNAL AUDIT

1

Building specialized cybersecurity audit skills and tools

2

Rebalance audit coverage toward cyber risk

3

Expand scope to governance, incident response, recovery, and third-party resilience

Ability to Communicate Cyber Risks to Management and the Board

Auditors must be able to translate technical cyber risks into clear business impacts, so management and the board can make informed decisions on risk mitigation, resources, and strategic priorities.

Data Analytics and Continuous Auditing & Monitoring Capability

Auditors should be able to use data analytics and continuous monitoring tools to detect anomalies, identify control weaknesses, and provide more timely assurance over cybersecurity risks.

Incident Response and Recovery Audit Capability

Auditors need the capability to review whether the organization has effective procedures to detect, contain, respond to, recover from, and learn from cybersecurity incidents.

Cybersecurity Risk Assessment Capability

Internal auditors need the ability to identify, assess, prioritize, and monitor cyber risks that may affect business objectives, operations, customer data, and regulatory compliance

IT General Control and Application Control Knowledge

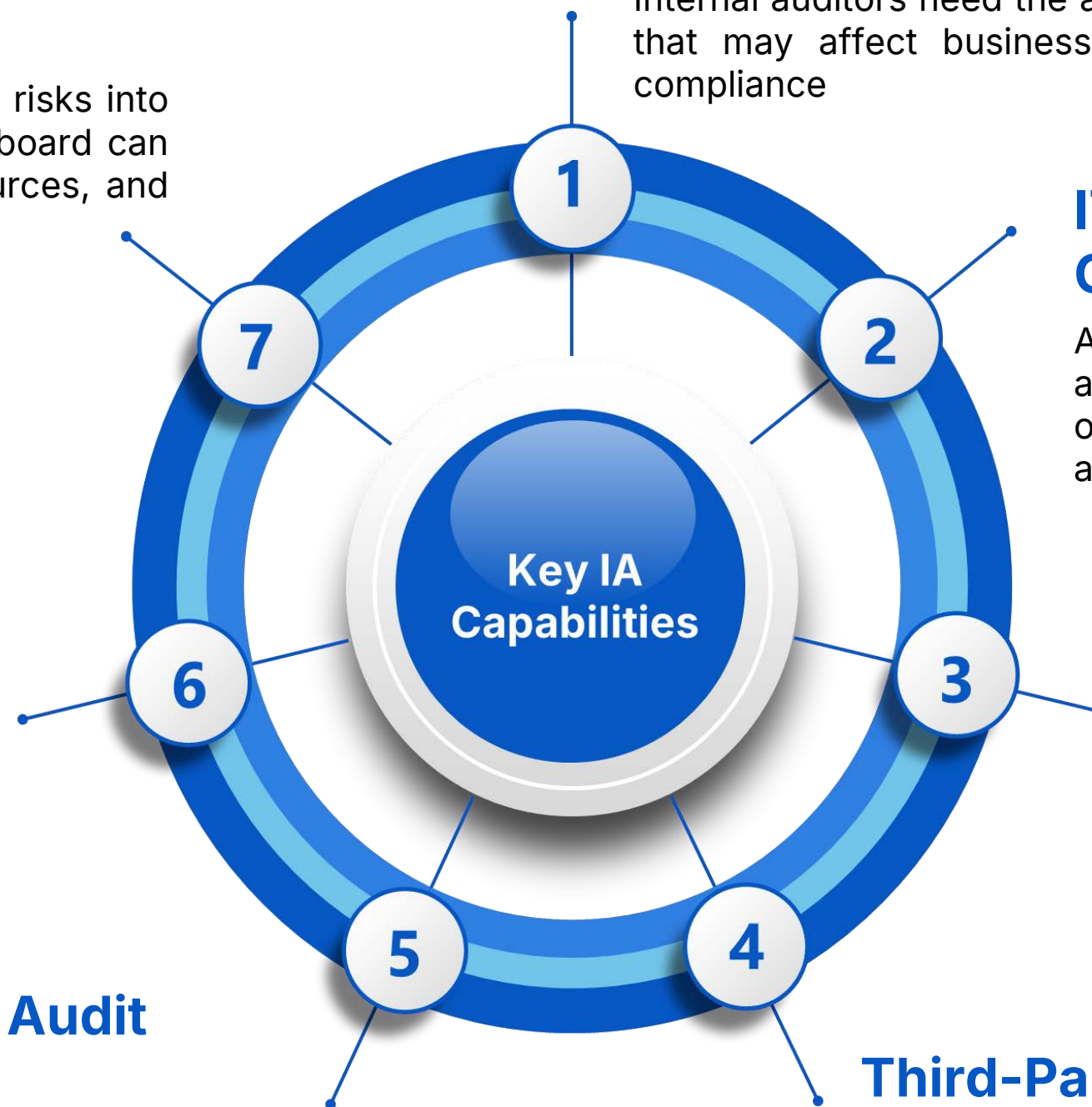
Auditors should understand key IT controls, including access management, change management, backup, system operations, and application-level controls to ensure data accuracy, security, and reliability.

Understanding of NIST CSF and Cybersecurity Standards

Auditors need knowledge of cybersecurity frameworks and standards, such as NIST CSF, to assess whether the organization has effective processes to govern, identify, protect, detect, respond to, and recover from cyber threats.

Third-Party/Vendor Risk Audit Capability

Auditors should be able to assess cybersecurity risks from vendors, cloud providers, fintech partners, API connections, and other third parties that may affect the organization's security posture.

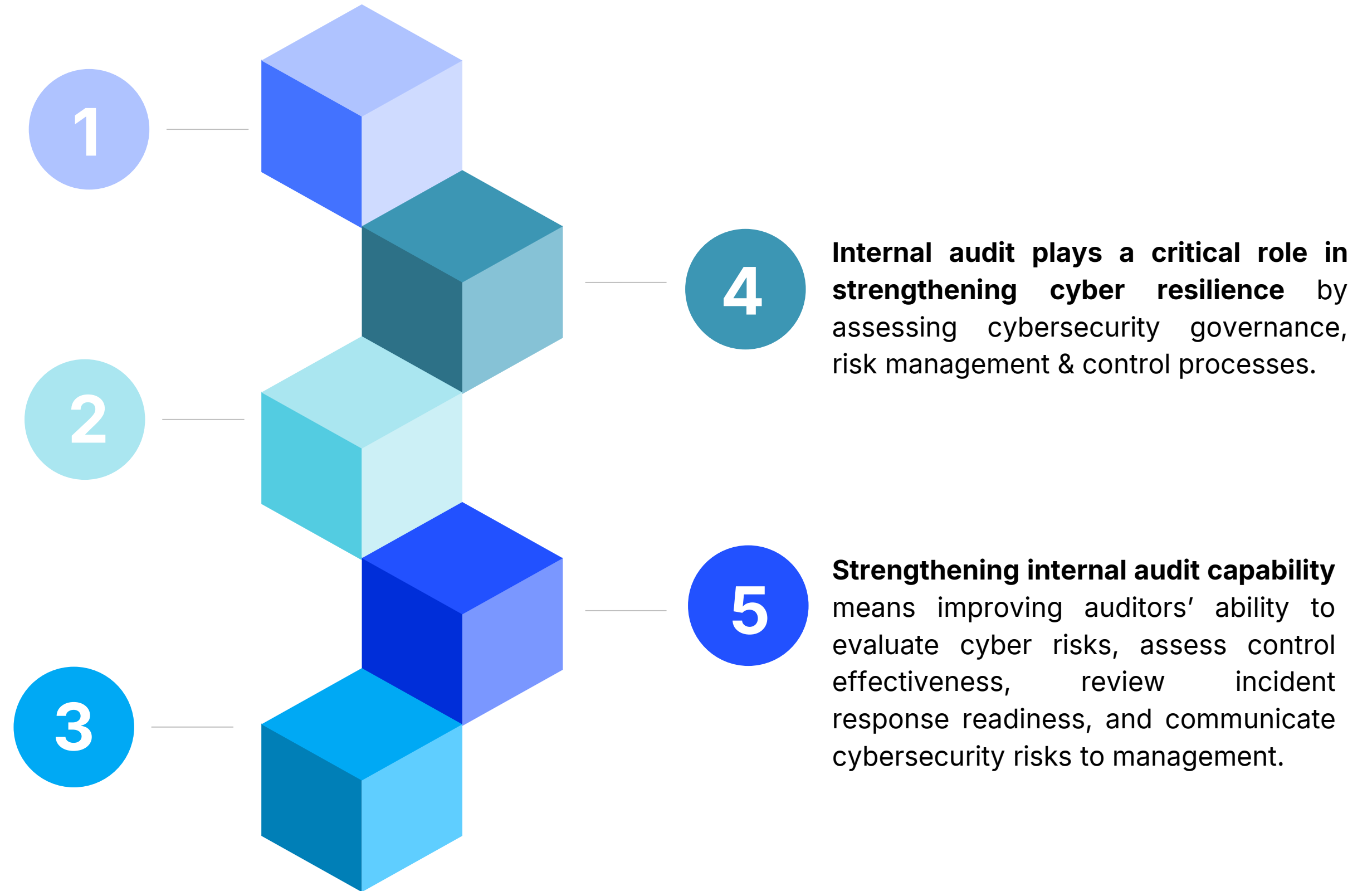


Key Takeaways

Cyber risk in the banking sector is no longer only a technical issue, but a **strategic business risk** that can disrupt operations, expose customer data, damage reputation, and create regulatory consequences.

As banking continues to evolve toward digital, embedded, and intelligent banking, cyber exposure also increases through mobile banking, internet banking, APIs, cloud, third-party services, and AI-enabled fraud.

Cyber resilience is essential for banks to anticipate threats, adapt to evolving attack methods, respond quickly to incidents, recover critical services, and maintain business continuity.





**The strongest security system
is not the one installed in the
data center, but the one built in
the minds of every employee.**

Yulianto Setiawan - Chief Audit Executive PT Bank Rakyat Indonesia (Persero) Tbk.

Thank You

This document and the information contained herein for Konferensi Auditor Internal on July 9, 2026, are proprietary to PT Bank Rakyat Indonesia (Persero) Tbk. and shall not be published or disclosed to any third party without the express written consent of an authorized representative of PT Bank Rakyat Indonesia (Persero) Tbk.

