



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

ciar.ypia

ciar-tv

EMPOWERING INTERNAL AUDITORS TO NAVIGATE EMERGING CYBER RISKS

GOVERNANCE 5.0 • RESILIENCE • ASSURANCE • TRUST

*Strengthening Governance, Building Cyber Resilience,
and Enabling Continuous Assurance
in an AI-Driven Digital World*



ASSURE TODAY
RESILIENCE TOMORROW
TRUST ALWAYS

Taufikurrahman

-  Country Ambassador, Sagana Capital
-  Member of British Chamber of Commerce in Indonesia
-  Prominent Lecturer at International Business Management (IBM) Program, Binus University
-  Lecturer at PKN STAN, BPPK, Ministry of Finance, Republic of Indonesia
-  Head of Policy Research, HIPPG, FIA, University of Indonesia (UI)



ANTICIPATE
Emerging Threats



STRENGTHEN
Governance
and Oversight



ENABLE
Continuous
Assurance



BUILD
Cyber Resilience
and Adaptability



EMPOWER
People, Skills
and Culture



CREATE
Trust and
Sustainable Value



THE CYBER RISK LANDSCAPE HAS CHANGED

From Technology Risk to Enterprise and Strategic Risk

In a digital-first world, cyber risk affects every part of the enterprise, its ecosystem, and its ability to create and protect value.

KEY DRIVERS EXPANDING CYBER RISK



Cloud Computing

Greater adoption, more misconfiguration risk



Artificial Intelligence

New capabilities, new vulnerabilities



Hyperconnectivity (IoT, APIs, Ecosystems)

Larger attack surface and interdependencies



Remote & Hybrid Work

Expanded endpoints, weaker perimeters



Digital Supply Chains & Third Parties

Risk moves across organizational boundaries

CYBER RISK IS NOW AN ENTERPRISE RISK



IMPACTS ON THE ORGANIZATION



Financial Impact

Revenue loss, fines, litigation, ransom payments



Operational Disruption

Downtime, production halt, supply chain interruption



Regulatory & Legal Exposure

Non-compliance, investigation, penalties



Reputation Damage

Loss of customer trust, brand value erosion



Strategic Consequences

Delayed transformation, loss of competitive advantage



Societal & National Impact

Critical infrastructure and public services disruption

REAL-WORLD INCIDENTS – REAL LESSONS



SOLARWINDS 2020

Supply chain compromise affected thousands of organizations.

Lesson: Strengthen third-party risk management.



COLONIAL PIPELINE 2021

Ransomware disrupted fuel distribution across the United States.

Lesson: Assess operational resilience and continuity.



UBER 2022

Insider compromised systems and data.

Lesson: Improve identity and access governance.



MOVEit TRANSFER 2023

Mass data theft through third-party software vulnerability.

Lesson: Monitor and test third-party security.



CHANGE HEALTHCARE 2024

Ransomware caused nationwide healthcare payment disruption.

Lesson: Test incident response and recovery capability.



CROWDSTRIKE OUTAGE 2024

Faulty update caused global IT outage across multiple sectors.

Lesson: Manage technology concentration and resilience.



KEY TAKEAWAY

The question is no longer whether an organization will face a cyber incident.

The question is whether the organization is prepared to withstand, respond to, and recover from it.

Sources: WEF Global Risks Report 2025; IBM Cost of a Data Breach Report 2025; ENISA Threat Landscape 2025; NIST Cybersecurity Framework 2.0.



2

WHY INTERNAL AUDITORS MUST CARE ABOUT CYBER RISKS

From Traditional Assurance to Cyber Resilience Assurance



Cyber risk is no longer an IT issue. It is a **strategic, enterprise and board-level risk**.

THE THREE LINES MODEL FOR CYBERSECURITY

FIRST LINE Management and Operations



Owns and manages cyber risks

Key Responsibilities

- Implement security controls
- Protect information assets
- Manage day-to-day risks
- Execute cyber policies
- Respond to incidents

Examples

CIO, CISO, IT Operations, Business Units

MANAGE RISK

SECOND LINE Risk & Compliance Functions



Oversees and guides risk management

Key Responsibilities

- Establish risk frameworks
- Define risk appetite
- Monitor compliance
- Provide guidance & support
- Consolidate risk information

Examples

Risk Management, Compliance, Information Security, DPO

MONITOR & GUIDE RISK

THIRD LINE Internal Audit



Independently assures risk management effectiveness

Key Responsibilities

- Evaluate cyber governance
- Assess risk management
- Test controls & processes
- Review resilience & response
- Provide insights & advisory

Examples

Internal Audit (CAEs, Audit Teams)

INDEPENDENT ASSURANCE

BOARD / AUDIT COMMITTEE



Provides oversight and challenge

Key Responsibilities

- Set tone from the top
- Oversee cyber risk
- Approve risk appetite
- Monitor management
- Ensure accountability

Examples

Board of Directors, Commissioners, Audit Committee

OVERSIGHT & CHALLENGE

WHY IT MATTERS



Strategic Impact

Cyber risk can affect strategy, financial performance and long-term value.



Enterprise-Wide Impact

Cyber incidents can disrupt operations, supply chains, customers, data, and reputation.



Regulatory & Legal Exposure

Non-compliance can lead to fines, litigation and loss of license to operate.



Trust & Reputation

Stakeholders expect strong cyber resilience and responsible risk governance.



Board Accountability

Boards are increasingly held accountable for overseeing cyber risk and resilience.

REAL-WORLD EXAMPLES: LESSONS FOR INTERNAL AUDIT

EQUIFAX

Equifax Data Breach (2017)

147 million people affected.
Root causes: unpatched vulnerability, weak governance, inadequate oversight.

Lesson:

Cyber failures often start with governance failures.

Capital One

Capital One Cloud Breach (2019)

Over 100 million customer records exposed due to misconfigured cloud environment.

Lesson:

Digital transformation increases risk. Governance must evolve.

solarwinds

SolarWinds Supply Chain Attack (2020)

Compromised software update affected thousands of organizations globally.

Lesson:

Third-party and supply chain risk are now critical.

WEY TAKEAWAY



Internal Audit provides the independent assurance that cyber risks are identified, managed, and cyber resilience is continuously strengthened.

Internal Audit is the Board's trusted advisor in a digital-first era.

”

In the Governance 5.0 era, Internal Audit moves beyond compliance assurance to provide **assurance, insight, and foresight** on cyber resilience.

References:

- Institute of Internal Auditors (IIA). (2024). Global Internal Audit Standards.
- Institute of Internal Auditors (IIA). (2025). Cybersecurity Topical Requirement.
- NIST. (2024). Cybersecurity Framework 2.0.

IIA The Institute of Internal Auditors

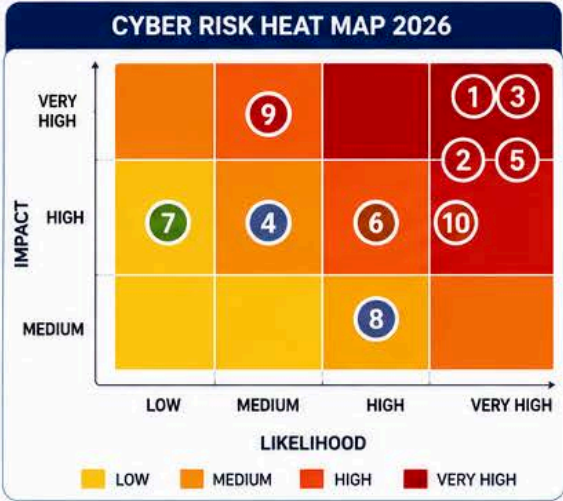
3

TOP EMERGING CYBER RISKS FACING ORGANIZATIONS IN 2026

What Internal Auditors Need to Watch

 Cyber threats are more sophisticated, more automated, more interconnected – and more impactful to the business.

#	EMERGING CYBER RISK	KEY DESCRIPTION	REAL-WORLD CASE EXAMPLE	BUSINESS IMPACT	INTERNAL AUDIT PRIORITY	KEY AUDIT FOCUS
1	 RANSOMWARE-AS-A-SERVICE (RaaS)	Ransomware kits and affiliates make attacks easy, scalable and highly profitable.	Colonial Pipeline (2021) Change Healthcare (2024)	 Shutdown, revenue loss, ransom payment	CRITICAL	Backups, incident response, recovery testing, resiliency
2	 AI-POWERED FRAUD & DEEPFAKES	AI enables convincing phishing, deepfake video/audio and automated social engineering.	Hong Kong Deepfake Fraud (2024)	 Fraudulent payments, executive impersonation	CRITICAL	AI governance, identity verification, awareness
3	 THIRD-PARTY & SUPPLY CHAIN ATTACK	Attackers compromise vendors or software providers to reach many organizations at once.	SolarWinds (2020) MOVEit (2023)	 Systemic compromise, supply chain disruption, regulatory exposure	CRITICAL	Vendor risk management, due diligence, continuous monitoring
4	 CLOUD SECURITY MISCONFIGURATION	Incorrect cloud settings, excessive privileges, and weak controls expose data and systems.	Capital One (2019)	 Data breach, service outage, compliance violations	HIGH	Cloud governance, access controls, configuration review
5	 CREDENTIAL THEFT & IAM FAILURE	Stolen credentials and weak identity controls remain a leading cause of breaches.	Uber Breach (2022)	 Unauthorized access, data theft, fraud	CRITICAL	MFA, privileged access management, periodic access review
6	 BUSINESS EMAIL COMPROMISE (BEC)	Attackers impersonate executives or vendors to trick employees into transferring funds.	Toyota Boshoku (2019) (US\$37M loss)	 Direct financial loss, payment disruption, reputational damage	HIGH	Payment controls, segregation of duties, out-of-band verification
7	 OPERATIONAL TECHNOLOGY (OT) ATTACKS	Increased connectivity exposes industrial control systems and critical infrastructure.	Oldsmar Water Facility (2021)	 Physical disruption, safety impact, production shutdown	HIGH	OT security, network segmentation, vulnerability management
8	 INSIDER THREAT	Malicious or negligent insiders can misuse access to steal or damage data and systems.	Tesla Insider Incident (2018)	 Data exfiltration, fraud, intellectual property loss	MEDIUM	User activity monitoring, least privilege, insider program
9	 NATION-STATE CYBER ATTACKS	State-sponsored actors target critical sectors for espionage, disruption or sabotage.	NotPetya (2017) Ukraine Attacks	 Severe disruption, national security risk, long-term strategic impact	HIGH	Threat intelligence, resilience planning, crisis readiness
10	 DATA PRIVACY BREACH	Exposure of personal or sensitive data leads to legal, regulatory and customer trust consequences.	Equifax (2017)	 Fines, litigation, loss of customer trust	HIGH	Data governance, privacy by design, encryption, DLP controls



WHY THESE RISKS MATTER TO THE BUSINESS

**FINANCIAL IMPACT**

Revenue loss, fraud, ransom payments, legal costs, regulatory fines.

**OPERATIONAL IMPACT**

System downtime, production stoppage, supply chain disruption, service interruption.

**REGULATORY & LEGAL IMPACT**

Non-compliance, investigations, sanctions, class action lawsuits.

**REPUTATION & TRUST IMPACT**

Loss of customer trust, brand damage, market value erosion.



KEY TAKEAWAY

Cyber risks in 2026 are more automated, interconnected, and business-focused. Internal Audit must evolve to provide assurance over cyber resilience, governance and preparedness – not just IT controls.



INTERNAL AUDIT IMPERATIVE

- Understand evolving threats and exposures
- Assess governance, controls and resilience
- Provide insight, challenge and foresight
- Strengthen organization's ability to anticipate, respond and recover



SOURCES

- World Economic Forum – Global Risks Report 2025
- ENISA – Threat Landscape 2025
- Verizon – Data Breach Investigations Report 2025
- IBM – Cost of a Data Breach Report 2025
- CrowdStrike – Global Threat Report 2025
- NIST Cybersecurity Framework 2.0 (2024)
- CISA Cybersecurity Advisories

4

AI AND CYBERSECURITY: FRIEND AND FOE

Why Internal Auditors Must Understand AI Governance



AI IS A DOUBLE-EDGED SWORD: IT POWERS OUR DEFENSE, BUT EMPOWERS OUR ADVERSARIES.

GOVERNANCE DETERMINES WHETHER AI BECOMES AN ASSET OR A LIABILITY.



AI: OUR POWERFUL ALLY IN CYBER DEFENSE



THREAT DETECTION

AI detects anomalies and threats faster than humans.



FRAUD DETECTION

AI identifies suspicious transactions in real time.



SECURITY MONITORING

AI analyzes millions of events and prioritizes real threats.



PREDICTIVE INTELLIGENCE

AI predicts emerging attack patterns and enables proactive defense.



VULNERABILITY MANAGEMENT

AI finds and prioritizes vulnerabilities more accurately.



AUTOMATION & RESPONSE

AI automates routine tasks and accelerates incident response.



AI: A FORCE MULTIPLIER FOR ATTACKERS



AI-POWERED PHISHING

AI creates highly personalized, convincing phishing messages.

Example:

AI-generated phishing email bypassing traditional filters.



DEEPFAKE FRAUD

AI generates fake voice, video and identities for impersonation.

Example:

Hong Kong Deepfake Fraud (2024) – US\$25 million lost.



AUTOMATED SOCIAL ENGINEERING

AI scales social engineering attacks to thousands instantly.

Example:

Automated spear phishing campaigns.



AI-ASSISTED MALWARE

AI helps attackers write code, find vulnerabilities and automate attacks.

Example:

AI tools used to develop malware and exploits.



PROMPT INJECTION ATTACKS

Attackers manipulate AI systems to extract data or bypass controls.

Example:

Bypassing LLM restrictions to access sensitive data.



DATA LEAKAGE VIA AI TOOLS

Sensitive data shared with public AI tools may be exposed.

Example:

Samsung GenAI Data Leakage (2023).

NEW AI RISKS FOR ORGANIZATIONS



MODEL RISK

Inaccurate or hallucinated outputs.



DATA PRIVACY RISK

Exposure of sensitive data in AI systems.



BIAS & ETHICAL RISK

AI may create biased or discriminatory outcomes.



EXPLAINABILITY RISK

AI decisions may be difficult to explain.



REGULATORY RISK

Increasing AI regulations and compliance obligations.



THIRD-PARTY AI RISK

Dependence on external AI providers and models.



SHADOW AI RISK

Unauthorized use of AI tools by employees.



SECURITY RISK

AI systems can be hacked or manipulated.



REPUTATIONAL RISK

Unethical or poor AI outcomes damage trust.



OPERATIONAL RISK

Over-reliance on AI may disrupt operations.

NIST AI RISK MANAGEMENT FRAMEWORK (AI RMF 1.0)



GOVERN

Establish accountability and oversight.



MAP

Understand AI context, use cases and risks.



MEASURE

Assess, analyze and track AI risks and impacts.



MANAGE

Respond to risks and continuously improve controls.

Internal Audit provides independent assurance across all four functions.

WHAT INTERNAL AUDITORS SHOULD FOCUS ON



AI Governance Framework



AI Risk Management



Data Protection & Privacy



AI Model Validation



Third-Party AI Providers



AI Ethics & Fairness



Regulatory Compliance



AI Monitoring & Incident Response

KEY QUESTIONS INTERNAL AUDITORS SHOULD ASK

- Does the organization have an approved AI governance framework?
- Has AI risk been incorporated into the enterprise risk management?
- Are AI models independently validated before deployment?
- Is sensitive data properly classified and protected in AI workflows?
- Are AI decisions explainable and auditable?
- Are third-party AI providers subject to due diligence and monitoring?
- Is the use of AI tools by employees authorized and monitored?
- Are there procedures to respond to AI-related incidents?

KEY TAKEAWAY

AI is transforming how organizations operate and how cybercriminals attack. Internal Audit must ensure AI is used responsibly, securely, ethically, and in alignment with the organization's objectives and stakeholder expectations.

SOURCES:

- NIST AI Risk Management Framework 1.0 (2023)
- McKinsey Global AI Survey 2024
- OECD AI Principles (2019)
- Gartner – AI and Cybersecurity Research (2024)
- World Economic Forum – Global Risks Report 2025
- IBM Cost of a Data Breach Report 2025



**GOVERN AI TODAY
SECURE TOMORROW**

5

CYBER GOVERNANCE: WHAT SHOULD BOARDS AND AUDIT COMMITTEES OVERSEE?

Cybersecurity is a governance issue. **Strong governance** creates cyber resilience.

 **Board Oversight**
Sets Direction &
Risk Appetite

 **Management**
Manages Risk &
Implements Controls

 **Internal Audit**
Provides Independent
Assurance

 **Resilient Organization**
Creates Long-term
Value & Trust

WHY BOARDS MUST CARE



STRATEGY

Enables digital transformation and competitive advantage



FINANCIAL IMPACT

Ransom, downtime, litigation, fines, and shareholder value



OPERATIONS

Business interruption and supply chain disruption



REPUTATION

Loss of customer trust and brand damage



REGULATORY EXPECTATIONS

Increasing laws, standards, and disclosure requirements



ENTERPRISE RESILIENCE

Ability to anticipate, withstand, respond and recover

BOARD CYBER GOVERNANCE OVERSIGHT DASHBOARD

Governance Area	Board Responsibility	Key Board Question	Management Responsibility	Internal Audit Assurance Role
 Cyber Strategy	Approve strategic direction	Is cybersecurity aligned with business strategy?	Execute cyber strategy	Assess governance effectiveness
 Risk Appetite	Define acceptable cyber risk level	How much cyber risk can we tolerate?	Operate within approved risk appetite	Evaluate risk governance
 Risk Management	Monitor significant cyber risks	What are our top cyber risks?	Identify, assess and mitigate risks	Review risk assessment process
 Governance & Accountability	Establish accountability and oversight	Who owns cyber risk and is accountable?	Assign roles and ensure accountability	Assess governance structure
 Cyber Resilience	Oversee resilience and preparedness	Can we continue operating during a cyber crisis?	Build and test resilience capabilities	Evaluate resilience readiness
 Incident Response	Monitor crisis readiness	Are we prepared for major cyber incidents?	Maintain incident response capability	Test incident response readiness
 Third-Party Risk	Oversee ecosystem and vendor risk	Are vendors exposing us to cyber threats?	Manage and monitor third parties	Review third-party controls
 AI Governance	Oversee AI-related risks and opportunities	Is AI governed responsibly?	Implement AI risk controls	Assess AI governance framework
 Compliance	Ensure regulatory compliance	Are we meeting legal and regulatory obligations?	Implement compliance programs	Validate compliance effectiveness
 Reporting & Metrics	Receive meaningful cyber intelligence	Are we receiving reliable and timely information?	Produce accurate cyber reports	Assess reporting quality
 Talent & Culture	Promote skills, culture and awareness	Do we have the right people and culture?	Build skills and cyber awareness	Evaluate training and culture effectiveness
 Business Continuity	Ensure recovery capability	How quickly can we recover critical operations?	Maintain BCP/DR plans and test regularly	Test recovery plans and effectiveness

NIST CYBERSECURITY FRAMEWORK 2.0



KEY QUESTIONS EVERY BOARD SHOULD ASK

- What are our most significant cyber risks?
- Which critical processes would be most impacted?
- Can we survive a prolonged cyberattack?
- What is our maximum probable cyber loss?
- Do we have adequate cyber insurance?
- Have we tested incident response and recovery plans?
- Are our vendors and partners secure?
- How is AI risk being governed?
- Do we receive meaningful cyber metrics and reports?
- Do we have the right cyber talent and culture?
- Are we meeting regulatory expectations?
- How quickly can we restore critical operations?

ROLES IN CYBER GOVERNANCE



Board of Directors

Oversight, Direction, Accountability



Audit Committee

Independent Oversight & Challenge



Management

Ownership, Execution, Resources



CISO / CIO

Cyber Defense, Technology Leadership



Risk Management

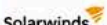
Risk Identification, Monitoring, Reporting



Internal Audit

Independent Assurance & Insight

LESSONS FROM MAJOR CYBER INCIDENTS

Incident (Year)	What Happened	Governance Weakness	Board Lesson	Internal Audit Lesson
 EQUIFAX	147M people affected due to data breach	Weak oversight, patch management failures	Cyber risk must be visible to the Board	Review governance, reporting and escalation
 Solarwinds	Supply chain attack impacted thousands	Inadequate third-party risk management	Ecosystem risk is board-level risk	Assess vendor risk management
 Colonial Pipeline (2021)	Ransomware caused fuel supply disruption	Security gaps and resilience weakness	Operational impact can be severe	Evaluate resilience and business continuity
 CHANGE HEALTHCARE	Ransomware disrupted healthcare services	Incident response and communication gaps	Recovery capability is critical	Test incident response and recovery
 Hong Kong Deepfake Fraud (2024)	\$25M transferred after deepfake video call	Weak identity verification and approval controls	AI introduces new governance risks	Assess AI governance and controls

INTERNAL AUDIT ASSURANCE FOCUS AREAS



KEY TAKEAWAY: Technology provides protection. Governance provides direction. Internal Audit provides assurance. Together, they create cyber resilience.

SOURCES:

- NIST Cybersecurity Framework 2.0 (2024)
- IIA Global Internal Audit Standards (2024)
- NACD Cyber-Risk Oversight Framework
- ISO/IEC 27001:2022
- COBIT 2019
- World Economic Forum – Cyber Resilience Framework

6 CYBER AUDITING IN PRACTICE: What Should Internal Auditors Audit?

From understanding risks to providing assurance that cyber governance, controls and resilience are effective.



OBJECTIVE

Provide independent assurance that cyber risks are identified, managed and monitored effectively.



FOCUS

Governance, Controls, Resilience, Compliance and Emerging Risks (AI).



OUTCOME

Stronger cyber resilience, trust, and sustainable organizational value.

1 CYBER AUDIT UNIVERSE 2026

Audit Domain	What Internal Audit Evaluates	Risk Level
Cyber Governance	Oversight structure, policies, board reporting, accountability	CRITICAL
Cyber Risk Management	Risk identification, assessment, appetite, KRIs, ERM integration	CRITICAL
Identity & Access Mgmt	User lifecycle, MFA, privileged access, access recertification	CRITICAL
Data Protection & Privacy	Data classification, encryption, DLP, privacy compliance	CRITICAL
Cloud Security	Cloud governance, configuration, shared responsibility, CSPM	HIGH
Third-Party Risk Mgmt	Vendor due diligence, contracts, monitoring, ongoing assessment	CRITICAL
Security Operations (SOC)	Monitoring, SIEM, alert triage, threat intelligence, log mgmt	HIGH
Incident Response	IR plan, escalation, communication, forensics, lessons learned	CRITICAL
Business Continuity & DR	BCP/DR plans, testing, RTO/RPO, resilience and recovery	CRITICAL
AI Governance	AI policies, model risk, data quality, ethics, human oversight	HIGH
Operational Technology (OT)	ICS/SCADA security, network segmentation, safety impact	HIGH
Cyber Awareness & Culture	Training, phishing tests, culture measurement, reporting	HIGH

4 RISK TO AUDIT ENGAGEMENT MAPPING (Examples)

Emerging Cyber Risk	Recommended Audit Engagement
Ransomware	Incident Response & Resilience Audit
AI Deepfake Fraud	AI Governance & Identity Verification Audit
Third-Party / Supply Chain Attack	Third-Party Cyber Risk Audit
Cloud Misconfiguration	Cloud Security & Configuration Audit
Credential Theft / Privileged Misuse	IAM & Privileged Access Audit
Business Email Compromise (BEC)	Payment Controls & Fraud Prevention Audit
Data Leakage	Data Protection & Privacy Audit
Insider Threat	User Behavior & Access Audit
Nation-State / Advanced Persistent Threat	Threat Detection & SOC Effectiveness Audit
OT / ICS Attack	Operational Technology Security Audit

2 CYBER AUDIT APPROACH & METHODOLOGY



5 TOP 10 CYBER AUDIT PRIORITIES FOR 2026

#	Audit Priority	Why It Matters	Priority
1	Cyber Governance & Oversight	Foundation of accountability and direction	CRITICAL
2	Cyber Risk Management	Ensures risks are identified and managed	CRITICAL
3	Identity & Privileged Access	Top attack vector in most breaches	CRITICAL
4	Incident Response & Preparedness	Speed of response reduces impact	CRITICAL
5	Business Continuity & Resilience	Ensures operations can be restored	CRITICAL
6	Third-Party / Vendor Risk	Ecosystem risk is growing rapidly	CRITICAL
7	Data Protection & Privacy	Regulatory, financial and reputational impact	CRITICAL
8	Cloud Security Governance	Increasing adoption, increasing risk	HIGH
9	AI Governance & Model Risk	Emerging risk area with high impact	HIGH
10	Cyber Awareness & Culture	People are the first and last line of defense	HIGH

3 NIST CSF 2.0 MAPPED TO INTERNAL AUDIT FOCUS

NIST Function	Purpose	Internal Audit Focus
GOVERN	Set direction, establish oversight and accountability	Evaluate governance structure, policies, risk appetite and board reporting.
IDENTIFY	Understand assets, data, risks and business context	Review risk assessment, asset inventory and critical process identification.
PROTECT	Implement safeguards to ensure delivery of services	Assess control design and effectiveness (preventive controls).
DETECT	Identify cybersecurity events and anomalies	Evaluate monitoring, logging, alerting and threat detection capabilities.
RESPOND	Take action regarding detected events	Assess incident response processes, communication and escalation.
RECOVER	Restore services and learn from incidents	Evaluate recovery plans, testing, RTO/RPO and improvement activities.

6 THIRD-PARTY CYBER RISK AUDIT CHECKLIST (Key Areas)

☒ Vendor inventory & criticality	☒ Incident notification obligations
☒ Cyber due diligence & risk rating	☒ Subcontractor & supply chain risk
☒ Contractual cybersecurity requirements	☒ Data handling & privacy compliance
☒ Ongoing monitoring & performance	☒ Exit & offboarding management

7 CYBER AUDIT MATURITY MODEL



KEY TAKEAWAY: Internal Audit adds the most value when it provides independent assurance that cyber governance, controls, resilience and emerging technology (including AI) are effective and aligned with organizational objectives.

REFERENCES:

- IIA Global Internal Audit Standards (2024)
- IIA Cybersecurity Topical Requirement (2025)
- NIST Cybersecurity Framework 2.0 (2024)
- COBIT 2019 Framework
- ISO/IEC 27001:2022
- NIST AI Risk Management Framework 1.0



**ASSURE TODAY
RESILIENT TOMORROW**

FROM PERIODIC AUDITING TO CONTINUOUS CYBER ASSURANCE

The Future of Internal Audit in a Real-Time Risk Environment

Cyber risks never sleep. Assurance should not be once a year.

“In a world where cyber threats evolve every hour, assurance delivered once a year is no longer enough.”

TRADITIONAL AUDIT vs CONTINUOUS CYBER ASSURANCE

	TRADITIONAL AUDIT	CONTINUOUS CYBER ASSURANCE
Timing	Annual / Periodic	Continuous / Near Real-Time
Focus	Historical	Current & Predictive
Audit Method	Sample-Based Testing	Continuous Monitoring
Coverage	Limited Sample	Full Population
Reporting	Quarterly / Annual Reports	Real-Time Dashboards
Risk Detection	After the Event (Reactive)	Before the Event (Proactive)
Technology	Manual, Spreadsheets	AI, Analytics, Automation
Audit Objective	Compliance Assurance	Resilience Assurance
Audit Role	Reviewer	Trusted Risk Advisor
Outcome	Findings & Recommendations	Continuous Confidence

CONTINUOUS CYBER ASSURANCE FRAMEWORK



ENABLING TECHNOLOGIES

SIEM Real-time threat visibility and monitoring	CCM Continuous controls monitoring	DATA ANALYTICS Identify trends, outliers and risk indicators	AI / ML Predict risks, anomalies and emerging threats	AUTOMATION Automate testing, evidence collection and reporting	DASHBOARDS Real-time visualization for management and boards
---	--	--	---	--	--

CONTINUOUS CYBER ASSURANCE DASHBOARD (EXAMPLES)

Critical Vulnerabilities (Open > 30 Days) 24 Target: < 10 ↑	Privileged Accounts Without Review 7.2% Target: < 5% ↑	Incident Response (MTTR) 1.8 hrs Target: < 4 hrs ↓	Backup Success Rate 98.6% Target: > 95% ✓
High Risk Vendors Without Assessment 18% Target: < 10% ↑	Cloud Misconfigurations (Critical) 32 Target: < 20 ↑	Phishing Failure Rate 11.5% Target: < 10% ↑	AI Systems Without Risk Assessment 6 Target: 0 ↑

EVOLUTION OF INTERNAL AUDIT

1.0 Compliance Focused Focus on rules and compliance	2.0 Risk-Based Auditing Focus on key risks	3.0 Strategic Auditing Focus on value, strategy and performance	4.0 Data Analytics Enabled Focus on data insights and continuous testing	5.0 Continuous Assurance & AI-Powered Focus on real-time assurance, prediction and resilience
---	---	--	---	--

CONTINUOUS ASSURANCE MATURITY MODEL

Level 1 Reactive Audit after incidents Limited visibility	Level 2 Compliance Focused Periodic testing Compliance orientation	Level 3 Risk-Based Focus on high risk areas Better insight	Level 4 Resilience Oriented Assure preparedness & recovery Proactive insight	Level 5 Continuous Assurance Real-time monitoring AI-driven insights Predictive assurance
---	--	--	--	--

REAL-WORLD EXAMPLES OF CONTINUOUS ASSURANCE

JPMORGAN CHASE & CO. - Real-time monitoring of threats, network behavior, identities and vulnerabilities - Advanced threat intelligence and automation - Continuous visibility supports resilience at scale	Microsoft - Trillions of security signals daily across the ecosystem - AI-driven threat detection and response - Security as a continuous learning system	Capital One - Cloud-native architecture with automation - Continuous monitoring of cloud and data risks - Digital organization needs digital assurance
---	---	--



KEY TAKEAWAY: Move from asking "Did controls work?" to "Are controls working right now?"
Continuous Cyber Assurance provides timely insights, strengthens resilience and creates continuous confidence for the Board.

SOURCES / REFERENCES

- Institute of Internal Auditors (IIA), Global Internal Audit Standards (2024)
- IIA, Vision 2035: The Future of Internal Auditing
- ISACA, Continuous Auditing and Monitoring Guidance

- Gartner, Continuous Controls Monitoring Research
- NIST Cybersecurity Framework 2.0 (2024)
- Microsoft Digital Defense Reports
- JPMorgan Chase Cybersecurity Disclosures
- Capital One Technology Risk Governance Publications

CYBER RESILIENCE: MEASURING READINESS, RESPONSE, AND RECOVERY

The goal is not to prevent every incident, but to survive, recover and grow stronger

“ CYBERSECURITY PROTECTS SYSTEMS.
CYBER RESILIENCE PROTECTS THE ORGANIZATION. ”

THE CYBER RESILIENCE LIFECYCLE



KEY RESILIENCE METRICS FOR THE BOARD

READINESS INDICATORS	RESPONSE INDICATORS	RECOVERY INDICATORS
- Critical Asset Inventory Completeness: 95% - Vulnerability Remediation Rate: 92% - Third-Party Assessment Coverage: 90% - Employee Awareness Completion Rate: 96%	- Mean Time to Detect (MTTD): < 24 hrs - Mean Time to Respond (MTTR): < 4 hrs - Critical Incidents Escalated Effectively: 100% - Crisis Management Activation Speed: < 30 min	- RTO Achievement Rate: 96% - RPO Achievement Rate: 95% - Backup Restoration Success Rate: 98% - BC/DR Testing Success Rate: 94%

CYBER RESILIENCE vs. CYBERSECURITY

	CYBERSECURITY (Traditional Focus)	CYBER RESILIENCE (Modern Focus)
Objective	Prevent attacks	Continue operations despite disruption
Success Measure	No incidents occurred	Rapid recovery and minimal disruption
Focus	Protection of systems	Survival and adaptation
Perspective	Technology-centric	Enterprise-wide (People, Process, Tech)
Scope	Security controls	Governance, operations, recovery
Board Question	Are we protected?	Can we survive a disruption?
Internal Audit Focus	Control effectiveness	Resilience capability and outcomes
Timing	Point-in-time	Continuous / Real-time

WHAT INTERNAL AUDIT SHOULD ASSESS

Governance	Is cyber resilience embedded in governance structures?
Risk Management	Are resilience risks incorporated into ERM?
Business Continuity	Can critical processes continue during disruption?
Disaster Recovery	Can technology services be restored within required timelines?
Incident Response	Are response capabilities tested and validated?
Third-Party Resilience	Can critical vendors recover from disruption?
AI Resilience	Can AI systems fail safely and recover effectively?
Lessons Learned	Are improvements implemented after incidents and exercises?

CYBER RESILIENCE STRESS TESTING PROGRAM



REAL-WORLD RESILIENCE LESSONS

INCIDENT	WHAT HAPPENED	RESILIENCE LESSON	INTERNAL AUDIT LESSON
Maersk (NotPetya, 2017)	Global operations disrupted; thousands of systems impacted	Strong recovery capability enabled business restoration	Assess recovery readiness and response capability
Colonial Pipeline (2021)	Ransomware attack halted fuel distribution	Operational continuity is critical	Review BCP, ICS security and crisis management
Change Healthcare (2024)	Cyberattack disrupted healthcare payment processing	Ecosystem resilience is essential	Evaluate third-party resilience and continuity
SolarWinds (2020)	Supply chain compromise affected many organizations	Vendor risk is part of resilience	Strengthen vendor risk assurance

RECOVERY TIME EXPECTATIONS BY BUSINESS SERVICE

BUSINESS SERVICE	MAX TOLERABLE DOWNTIME	TARGET RTO	TARGET RPO
Online Banking	Hours	< 4 hours	< 15 minutes
Payment Processing	Hours	< 2 hours	< 5 minutes
Trading Systems	Minutes – Hours	< 1 hour	< 5 minutes
Customer Service Platform	1 Day	< 8 hours	< 1 hour
ERP Systems	1 – 2 Days	< 24 hours	< 4 hours
Email Systems	1 Day	< 12 hours	< 2 hours
HR Systems	Several Days	< 48 hours	< 8 hours

CYBER RESILIENCE MATURITY MODEL



KEY TAKEAWAY: The most resilient organizations are not those that avoid every incident, but those that can anticipate, withstand, respond, recover, and adapt.

SOURCES / REFERENCES

- NIST Cybersecurity Framework 2.0 (2024)
- NIST SP 800-61 Rev.3 – Incident Response
- ISO 22301:2019 – Business Continuity Management
- ISO/IEC 27001:2022
- World Economic Forum – Cyber Resilience Framework
- IBM Cost of a Data Breach Report
- Industry Reports: Maersk (NotPetya, 2017), Colonial Pipeline (2021), Change Healthcare (2024)



THE FUTURE CYBER AUDITOR

Skills and Competencies for Internal Audit 5.0

Cyber resilience does not begin with technology. It begins with people.

“The future auditor does not compete with technology. The future auditor leverages technology to create value.”

FROM YESTERDAY TO TOMORROW

	TRADITIONAL AUDITOR (Yesterday)	MODERN AUDITOR (Today)	FUTURE AUDITOR 5.0 (Tomorrow)
Focus	Compliance & Control	Risk-Based Assurance	Risk-based & Strategic Assurance
Approach	Sample Testing	Data Analytics	Continuous Assurance
Technology	Spreadsheets	Analytics Tools	AI & Automation
Perspective	Historical	Current-State	Future-State
Reporting	Audit Findings	Risk Insights	Predictive Intelligence
Value to Board	Compliance Assurance	Risk Assurance	Resilience Assurance

CYBER COMPETENCIES EVERY AUDITOR SHOULD UNDERSTAND

DOMAIN	AUDIT RELEVANCE
Cyber Governance	Assess oversight, accountability and policies
Identity & Access Management	Review access controls and privileged access
Cloud Security	Evaluate cloud governance and configurations
Data Protection & Privacy	Assess data classification and privacy controls
Incident Response	Evaluate readiness and response capability
Third-Party Risk	Assess vendor and ecosystem exposure
Business Continuity & Resilience	Evaluate continuity and recovery readiness
AI Governance	Review AI risks, ethics and model governance
Vulnerability Management	Assess vulnerability scanning and remediation
Threat Intelligence	Evaluate threat monitoring and intelligence use

INTERNAL AUDIT 5.0 COMPETENCY FRAMEWORK



T-SHAPED AUDITOR: BROAD KNOWLEDGE. DEEP EXPERTISE.

THE T-SHAPED AUDITOR MODEL

BROAD KNOWLEDGE (HORIZONTAL)

- ✓ Governance
- ✓ Risk Management
- ✓ Business Strategy
- ✓ Operations
- ✓ Technology Awareness
- ✓ Industry Knowledge
- ✓ Communication



DEEP EXPERTISE (VERTICAL)

- ✓ Cybersecurity
- ✓ Data Analytics
- ✓ AI Governance
- ✓ Financial Controls
- ✓ IT Audit
- ✓ Digital Assurance
- ✓ Specialized Domains

The future auditor combines a wide understanding of the business with deep expertise in high-risk, high-technology areas.

TOP 10 SKILLS FUTURE AUDITORS MUST MASTER (2026–2035)

1	Cybersecurity Literacy	Understand cyber risks, controls and threats	CRITICAL ★★★★★
2	Data Analytics	Analyze data to generate actionable insights	CRITICAL ★★★★★
3	AI Literacy	AI governance, model risk and AI assurance	CRITICAL ★★★★★
4	Risk Management	Identify, assess and respond to enterprise risks	CRITICAL ★★★★★
5	Business Acumen	Connect risks to business objectives	CRITICAL ★★★★★
6	Communication & Influence	Present insights clearly to drive decisions	CRITICAL ★★★★★
7	Technology Governance	Evaluate IT governance and digital risks	HIGH ★★★★★
8	Critical Thinking	Assess ambiguity and complex situations	HIGH ★★★★★
9	Continuous Assurance	Monitor controls and risks in near real-time	HIGH ★★★★★
10	Change Management	Adapt to change and drive transformation	HIGH ★★★★★

KEY CERTIFICATIONS SUPPORTING FUTURE AUDITORS

CERTIFICATION	FOCUS AREA	RELEVANCE
CIA – Certified Internal Auditor	Internal Auditing	Foundation for all auditors
CISA – Certified Information Systems Auditor	Information Systems Audit	IT & Digital Assurance
CRISC – Certified in Risk & Information Systems Control	IT Risk Management	Risk & Control Focus
CISSP – Certified Information Systems Security Professional	Cybersecurity	Cyber Literacy
CGEIT – Certified in Governance of Enterprise IT	IT Governance	Technology Governance
ISO 27001 Lead Auditor	Information Security Management	Security Assurance
Data Analytics Certifications (e.g., Power BI, Alteryx)	Data Analytics	Data-Driven Assurance
AI Governance Certifications (e.g., AI Ethics, Model Risk)	AI Risk & Governance	Emerging Audit Domain

INTERNAL AUDIT TALENT TRANSFORMATION ROADMAP



REAL-WORLD EXAMPLES

JPMorganChase	Microsoft	DBS
- Multidisciplinary audit teams (auditors, data scientists, cyber experts) - Data-driven and continuous audit capabilities - Focus on risk intelligence and value creation	- AI-supported assurance and automation - Continuous monitoring at scale - Future-ready audit function	- Strong investment in digital transformation and risk intelligence - Data-driven, technology-enabled internal audit - Focus on digital and cyber risks

WHAT MAKES A FUTURE AUDITOR SUCCESSFUL?



KEY TAKEAWAY: The future of Internal Audit is not about auditors competing with technology. It is about auditors leveraging technology, deepening their expertise, and strengthening their business acumen to provide resilience assurance and create lasting value.

SOURCES / REFERENCES

- IIA Global Internal Audit Standards (2024)
- IIA Vision 2035
- NIST NICE Workforce Framework
- ISACA Cybersecurity Skills Framework
- World Economic Forum – Future of Jobs Report
- Deloitte – Future of Internal Audit
- Gartner – Future of Audit Research
- Microsoft Digital Defense Report
- JPMorgan & DBS Annual Reports



10 KEY TAKEAWAYS AND ACTION PLAN

Empowering Internal Auditors to Navigate Emerging Cyber Risks

“The future of Internal Audit is not about auditing more controls. It is about helping organizations become more resilient in an increasingly uncertain digital world.”



WHAT WE HAVE LEARNED – 5 KEY REALITIES

1 CYBER RISK IS A BUSINESS RISK



- Affects strategy, operations, finance, reputation and compliance
- Must be governed at the enterprise level

2 AI IS BOTH AN OPPORTUNITY & A RISK



OPPORTUNITIES

- Threat detection
- Fraud detection
- Risk monitoring

RISKS

- Deepfake fraud
- Prompt injection
- Model risks
- Data leakage
- Ethical concerns

AI governance is a critical audit domain

3 GOVERNANCE DETERMINES RESILIENCE



- Technology alone is insufficient
- Strong governance drives accountability, preparedness and recovery capability
- Foundation of cyber resilience

4 INTERNAL AUDIT MUST EVOLVE



FROM

- Compliance
- Controls
- Historical review

TO

- Cyber resilience
- AI governance
- Continuous assurance
- Emerging risks
- Strategic insight

The profession is expanding, not shrinking

5 PEOPLE MATTER MOST



- Technology enables resilience
- People create resilience
- Future auditor combines
 - ✓ Audit expertise
 - ✓ Cyber literacy
 - ✓ AI awareness
 - ✓ Business acumen
 - ✓ Communication skills

ACTION PLAN FOR BOARDS & AUDIT COMMITTEES

- Elevate cyber risk to a strategic agenda
- Integrate cyber risk into enterprise risk management
- Strengthen cyber governance and accountability
- Demand meaningful cyber metrics and reporting
- Oversee AI governance and ethical use
- Monitor cyber resilience and recovery readiness
- Conduct regular cyber stress tests and simulations
- Ensure continuous internal audit coverage

ACTION PLAN FOR CHIEF AUDIT EXECUTIVES (CAEs)

- Update the cyber audit universe and risk assessment
- Adopt risk-based cyber audit planning
- Incorporate AI governance and model risk audits
- Expand third-party and supply chain risk audits
- Evaluate cyber resilience and business continuity
- Increase continuous assurance and automation
- Strengthen data analytics and audit technology
- Develop and retain cyber, AI and analytics talent

ACTION PLAN FOR INTERNAL AUDITORS

- Build strong cybersecurity literacy
- Develop data analytics and visualization skills
- Understand AI governance and emerging AI risks
- Learn cloud, identity and data risk management
- Understand cyber resilience and incident response
- Improve communication and storytelling skills
- Adopt continuous learning and professional curiosity
- Become a trusted advisor and strategic partner

THE INTERNAL AUDIT 5.0 ROADMAP



INTERNAL AUDIT'S FUTURE ROLE



FINAL REFLECTION



The question facing Internal Audit is no longer:

“Did the controls work?”

The question is:

“Can the organization achieve its objectives despite uncertainty, disruption, and cyber threats?”

FINAL TAKEAWAY



CLOSING MESSAGE

The organizations that thrive in the Governance 5.0 era will not necessarily be those with the most technology. They will be those with the strongest governance, the highest resilience, the best prepared people, and Internal Audit functions capable of providing confidence in an increasingly uncertain world.

THANK YOU

Questions & Discussion

Empowering Internal Auditors to Navigate Emerging Cyber Risks



KEY REFERENCES

IIA Global Internal Audit Standards (2024)

IIA Vision 2035

NIST Cybersecurity Framework 2.0

NIST AI Risk Management Framework (AI RMF 1.0)

World Economic Forum Global Risks Report

World Economic Forum Cyber Resilience Framework

ISACA Cybersecurity & Governance Guidance

Deloitte Future of Internal Audit

Gartner Future of Audit Research