

Audit Masters

10th Annual Internal Audit Forum



Assessing emerging cybersecurity risks in the digital landscape: implications for internal audit

Lior Segal, Advocate, CPA, MBA, CIA, CRMA, EQA, CISA, CISM, CRISC, CDPSE
Chief Audit Executive, Bezeq | Board member, IIA Israel

21 May 2025

\$8

Trillion

Cost of cybercrime
in 2023



\$250K+

PER SECOND

\$9.5

Trillion

Cost of cybercrime
in 2024



\$300K+

PER SECOND

\$10.5

Trillion

Cost of cybercrime
in 2025



\$330K+

PER SECOND

Source: Anthony Pugliese's presentation during International conference (July 2024)

RESEARCH

SECURITY

APRIL 16, 2025

Q1 2025 Global Cyber Attack Report from Check Point Software: An Almost 50% Surge in Cyber Threats Worldwide, with a Rise of 126% in Ransomware Attacks

NEWS

M&S suspends all online sales as cyber attack worsens

M&S shuts down online sales as it works to contain and mitigate a severe cyber attack on its systems

AI-Powered Malware: A New Frontier in Cybersecurity Threats

Apr 26, 2025



Digital Europe Programme: EU allocates €1.3bn for critical tech deployment

Technology | 28th March 2025



Table of contents

01

Introduction

02

Cybersecurity and
Digital transformation

03

Cybersecurity
elements

04

New cybersecurity
requirements

05

Practical
considerations

06

Concluding
remarks

Lior Segal- Few Words about me

- Over 20 years of experience in Audit, Risk and Control fields in Public companies, on management positions
- Chief Audit Executive at Bezeq, a large Telecommunications company
- Director, Treasurer and Secretary at IIA Israel
- A Public Speaker
- Teaches on various training and professional courses, including in Academics
- Audit Committee Member in a non-profit organization



- Bachelor of Law (LL.B), Bachelor of Accounting (B.A), M.B.A, dual majors: Finance & Accounting and Strategy & Entrepreneurship, Bachelor of Comprehensive Audit Studies
- An Advocate and a CPA
- A CIA, CRMA, CISA, CISM, CRISC, CDPSE, QAR (External Quality Assessor)

Please scan to connect in
LinkedIn->



What is Digital Transformation?



Create new and/or modify existing business processes, culture, and customer experiences, using digital technologies. This is done to meet changing business and market requirements.

Global digital transformation market is growing fast

Size, by Type, 2020 - 2030 (USD Trillion)

28.5%

Global Market CAGR,
2025 - 2030





We are deep on the Digital Transformation age

**Digital
transformation
expansion increases
the attack surface,
introducing new
threats**



Main vectors contributing to increased cybersecurity risks

More Tech =
More
Targets

Speed
rollout vs.
Security

Data
Explosion

Shadow IT &
Hidden
Hazards

Third-Party
Integrations

AI &
Automation

2024

1. Cybersecurity	73%
2. Human capital	51%
3. Business continuity	47%
4. Regulatory change	39%
5. Digital disruption (including AI)	34%
6. Financial liquidity	32%
7. Market changes/competition	32%
8. Geopolitical uncertainty	30%
9. Governance/corporate reporting	27%
10. Supply chain (including third parties)	26%
11. Organizational culture	26%
12. Fraud	24%
13. Communications/reputation	21%
14. Climate change/environment	19%
15. Health/safety	11%
16. Mergers/acquisitions	6%

2025

1. Cybersecurity	73%
2. Business continuity	51%
3. Human capital	49%
4. Digital disruption (including AI)	39%
5. Regulatory change	38%
6. Market changes/competition	32%
7. Financial liquidity	31%
8. Geopolitical uncertainty	30%
9. Governance/corporate reporting	25%
10. Organizational culture	24%
11. Fraud	24%
12. Supply chain (including third parties)	23%
13. Climate change/environment	23%
14. Communications/reputation	20%
15. Health/safety	11%
16. Mergers/acquisitions	6%

2028

1. Cybersecurity	69%
2. Digital disruption (including AI)	59%
3. Business continuity	47%
4. Human capital	42%
5. Climate change/environment	39%
6. Regulatory change	37%
7. Geopolitical uncertainty	31%
8. Market changes/competition	30%
9. Financial liquidity	25%
10. Supply chain (including third parties)	24%
11. Governance/corporate reporting	22%
12. Fraud	21%
13. Organizational culture	20%
14. Communications/reputation	15%
15. Health/safety	10%
16. Mergers/acquisitions	9%

Source: Risk in Focus 2025

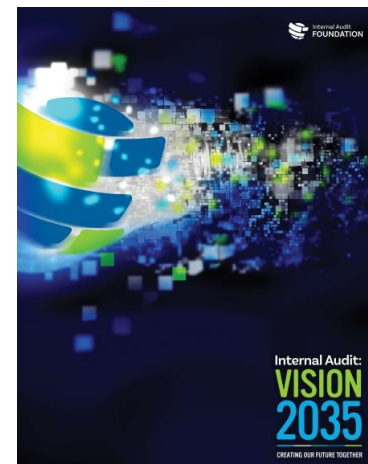
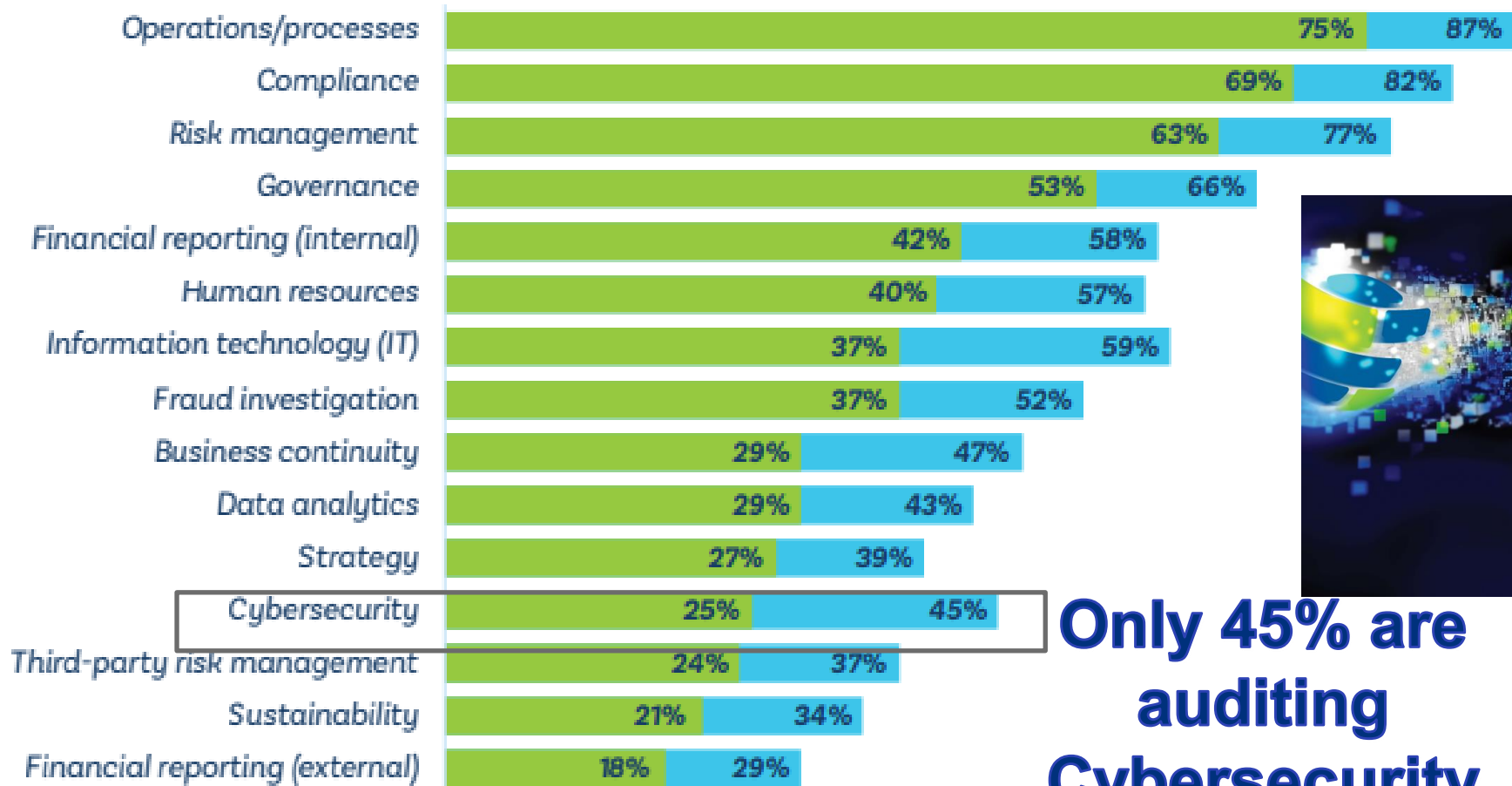


**How many of you are
auditing cybersecurity?**



Top Areas in Which Internal Auditors Provide Audit Services

■ Personally ■ Internal Audit Function



**Only 45% are
auditing
Cybersecurity**

**What do
Internal
auditors must
know about
cybersecurity?**



Standard 9.4 Internal Audit Plan

Requirements

The chief audit executive must create an internal audit plan that supports the achievement of the organization's objectives.

The chief audit executive must base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks. This assessment must be informed by input from the board and senior management as well as the chief audit executive's understanding of the organization's governance, risk management, and control processes. The assessment must be performed at least annually.

The internal audit plan must:

- Consider the internal audit mandate and the full range of agreed-to internal audit services.
- Specify internal audit services that support the evaluation and improvement of the organization's governance, risk management, and control processes.
- Consider coverage of information technology governance, fraud risk, the effectiveness of the organization's compliance and ethics programs, and other high-risk areas.
- Identify the necessary human, financial, and technological resources necessary to complete the plan.
- Be dynamic and updated timely in response to changes in the organization's business, risks operations, programs, systems, controls, and organizational culture.



Standard 3.1 Competency

Requirements

Internal auditors must possess or obtain the competencies to perform their responsibilities successfully. The required competencies include the knowledge, skills, and abilities suitable for one's job position and responsibilities commensurate with their level of experience. Internal auditors must possess or develop knowledge of The IIA's Global Internal Audit Standards.

Internal auditors must engage only in those services for which they have or can attain the necessary competencies.

Internal auditors must engage only in those services for which they have or can attain the necessary competencies. Internal auditors must ensure that the internal audit function collectively possesses the competencies to perform the internal audit services described in the internal audit charter or must obtain the necessary competencies. (See also Standards 7.2 Chief Audit Executive Qualifications and 10.2 Human Resources Management.)





What do IA need to know about cybersecurity?

- Basic understanding
- In depth knowledge
- No knowledge at all (we have professionals in the organization and can hire consultants)



As internal auditors, we must understand (at least) these elements



What are cyber threats?



Who carries out cyber attacks?



What are the goals of cyber attacks?



What drives the rapid evolution of cyber threats?



What are current and emerging cyber threats?



What is the impact of cyber attacks?



How can organizations defend against cyber attacks?

What are cyber threats?



- Any potential malicious activity or action that targets
 - Computer systems
 - Network
 - Devices
 - Digital infrastructure

With the intention to

- Compromise their security
- Exploit vulnerabilities
- Cause harm

Who carries out cyber threats?



Employees
with
privileges

Criminal
organizations

Nation-states

Terrorists'
bodies

Business
competitors

Other
malicious
entities

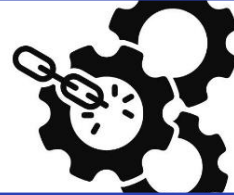
What are the threats aiming to achieve?



Gain
unauthorized
access



Steal
sensitive
information



Disrupt
operations



Cause
damage to
digital assets

Factors contributing to fast evolution of cyber threats



Cybercriminals
networks and
motivation



Ransomware
sophistication



Digital
transformation



Technological
advancement



Increased
connectivity and
interdependence



Geopolitical
tensions

Current and emerging cyber threats



Advanced
Persistent threats
(APTs)



Insider threats



Internet of things
(IoT) vulnerably



AI enabled Attacks

Current and emerging cyber threats cont.



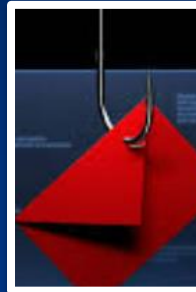
Data
Poisoning



DDoS



Ransomware



Phishing

Impact of cyber threats on organizations



Financial losses



Reputational damage



Operational disruptions



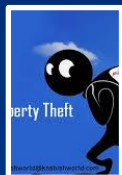
Legal claims



Regulatory sanctions



Identity theft



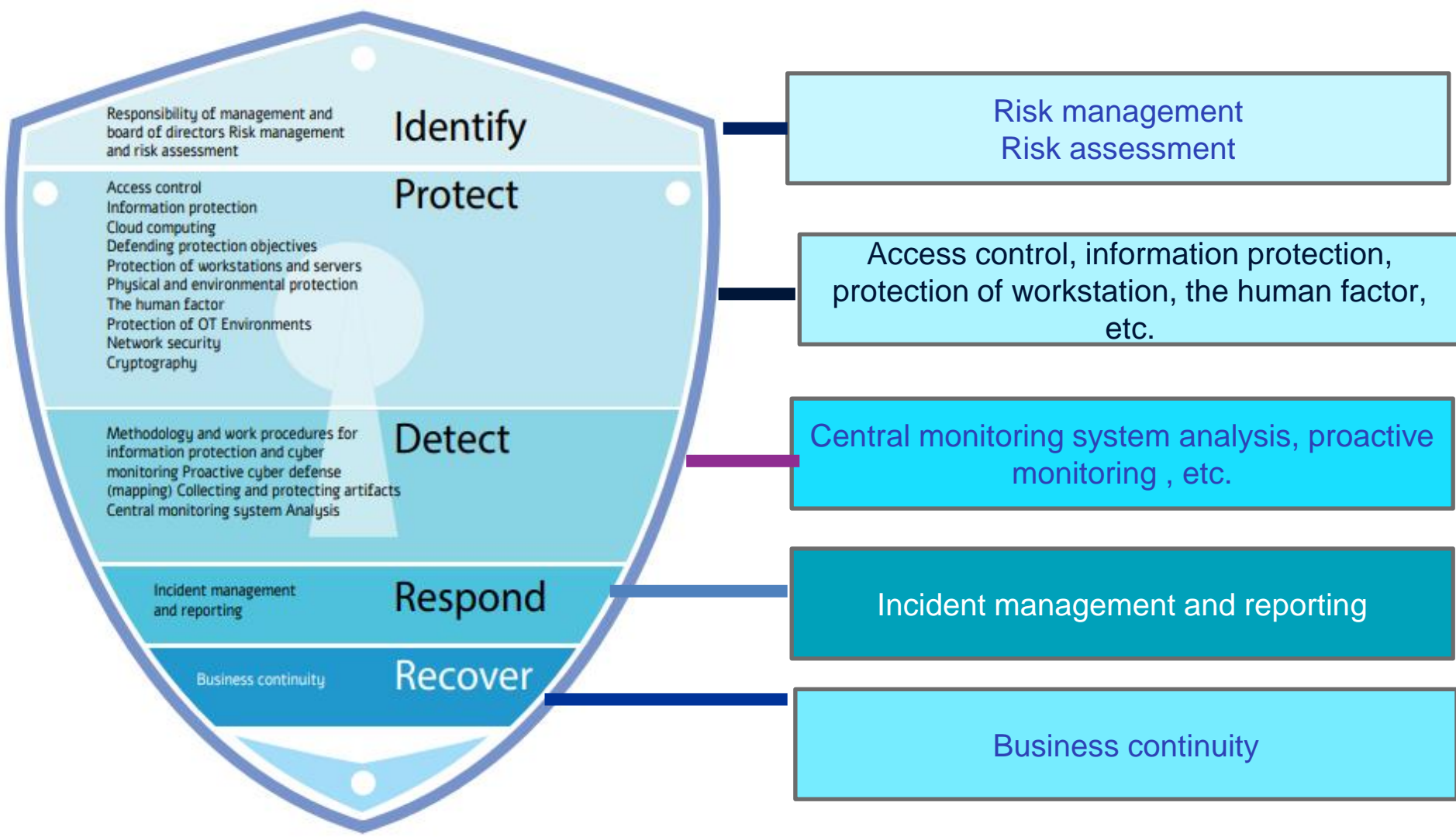
IP theft



Supply chain disruptions



Loss of competitive advantage



Where can Internal audit be involved?

Risk
assessment

Control
evaluation

Compliance
and regulatory
assurance

Incident
Response and
management

Monitoring and
reporting

Awareness
and training

Advisory

Vendor risk
management



Cybersecurity

Topical Requirement

Cybersecurity


Topical Requirement

User Guide




Topical requirement are applicable when

Subject of
an
engagement
in the
internal
audit plan



Identified
while
performing
an
engagement



Subject of
an
engagement
request
not on the
original
internal
audit plan

What needs to be assessed and evaluated?

Governance

Risk
Management

Controls

GOVERNANCE- REQUIREMENTS



1

A formal cybersecurity strategy and objectives are established and periodically updated

2

Policies and procedures are established and periodically updated

3

Roles and responsibilities are established, and a process exists to periodically assess

4

Relevant stakeholders are engaged to discuss and act on existing vulnerabilities and emerging threats

RISK MANAGEMENT- REQUIREMENTS*



1

Risk related processes include identifying, analyzing, mitigating, and monitoring cybersecurity threats and their effect

2

Cybersecurity risk management is conducted across the organization

3

Accountability and responsibility for cybersecurity are established

4

A process is established to quickly escalate any cybersecurity risk that reaches an unacceptable level

* There are more risk management requirements

CONTROLS- REQUIREMENTS*



1

A process is established to ensure both internal controls and vendor-based controls are in place

2

Training to develop and maintain technical competencies

3

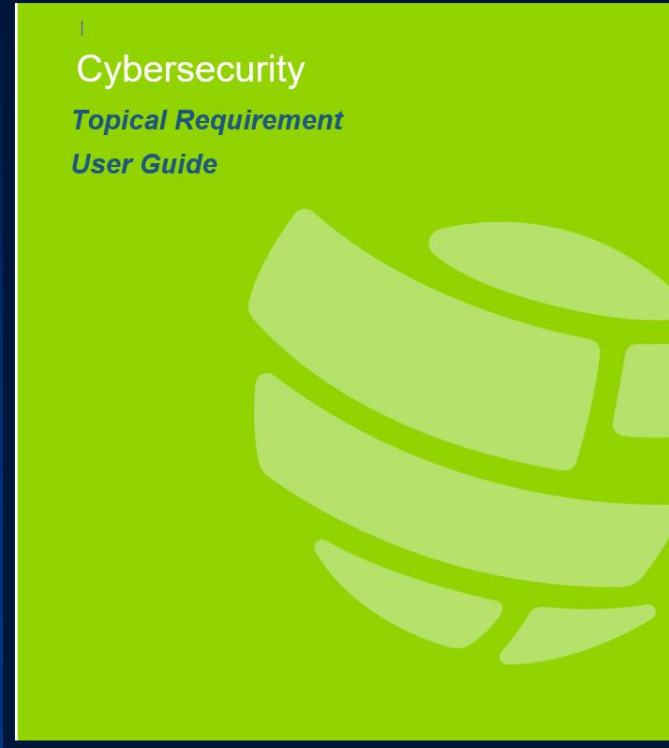
A process is established to continuously monitor and report emerging cybersecurity threats and vulnerabilities

4

Cybersecurity is included in the life cycle management

* There are more controls requirements

And what is in the user guide?



User guide includes

Applicability and Professional Judgment

Performance, Documentation and Reporting

Quality Assurance

Considerations for implementation on
Governance, RM and controls

Examples, Mapping to Frameworks,
Documentation Tool



**WELCOME TO
REALITY**

There are many cybersecurity engagements we should conduct

Network
Security
Assessment

Application
Security Audit

Access Control
and Identity
Management

Endpoint
Security

Cloud Security
Audit

Data Protection
and Privacy

Remote access

Incident
Response
Management

Physical
security

AI threats
protection

And much
more

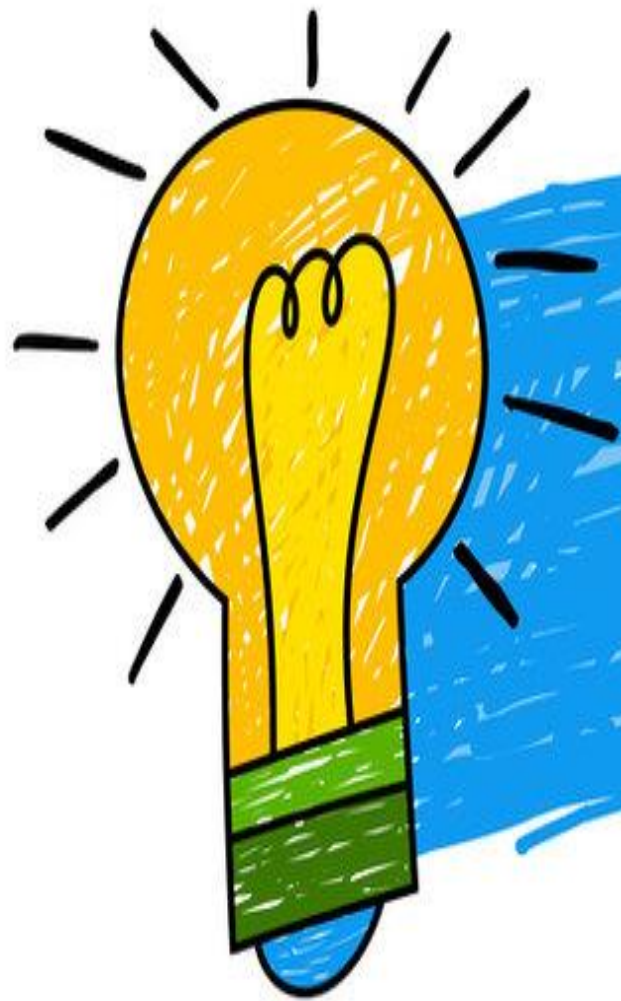
Some final thoughts



- Cyber threats are evolving faster than ever, fueled by the expanding digital ecosystem
- Digital transformation creates new opportunities but also emerging risks
- Internal auditors must evolve from checking controls **after** the fact, to being proactive advisors **during** digital initiatives
- We all should improve our cybersecurity understating, including the topical requirements

**Thank you
for listening**





Any Questions?

Thank you!

Thank you for attending and
participation

Lior Segal

📞 Phone: +972 506773706

✉ Email: lior.segal@gmail.com

in LinkedIn:

<https://www.linkedin.com/in/liorsegal>

