



# Achieving Integration Between Compliance & Security in Banking

Presented by Jean Michel Kawkabani

November 2025



(France, UAE, KSA, Cyprus)

## Jean Michel Kawkabani, CISA

ENSAI-FRANCE | ArcShields Director | Cybersecurity Expert | IS Audit Expert | C-CISO | IT Risk | Advanced VAPT | UAB Technical Committee Member | Infosec lecturer at Saint Joseph University and ENA Lebanon.



Previous positions: Head of Information Security Dept.  
Head of IT audit, Head of MIS



Lecturer (Master in Systems and Network Security)




Lecturer-Information Security course



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

WHEN COMPLIANCE AND  
SECURITY ARE ON TWO  
DIFFERENT SILOED LEVELS...



Before the audit

During the audit

After the audit

SECURITY  
/COMPLIANCE





# Security/ Compliance

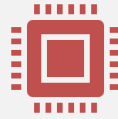
Compliance is periodic.  
Hackers Audit You  
every day!

# SOME MAP SECURITY BENEFITS TO COMPLIANCE LEVEL

**Pareto Principle** applied directly to cybersecurity, which is the foundational philosophy behind the **CIS Critical Security Controls (CIS Controls)**.

CIS Version	The "20% Effort" (Key Focus Area)	The "80% Benefit" (Mitigation)
CIS Controls v7/v8.1	The <b>Implementation Group 1 (IG1)</b> Safeguards (56 total)	<b>Up to 85% - 90%</b> of successful, non-targeted attacks.
Earlier Versions	The <b>First 5 or 6 Controls</b> (often called "Basic Cyber Hygiene").	<b>Around 85%</b> of common cyberattacks.

# Context & Rationale



Increasing regulatory scrutiny (Basel III, ISO 27001, GDPR, DORA, NIS2, NCA ECC, SAMA, PSD3, etc.)



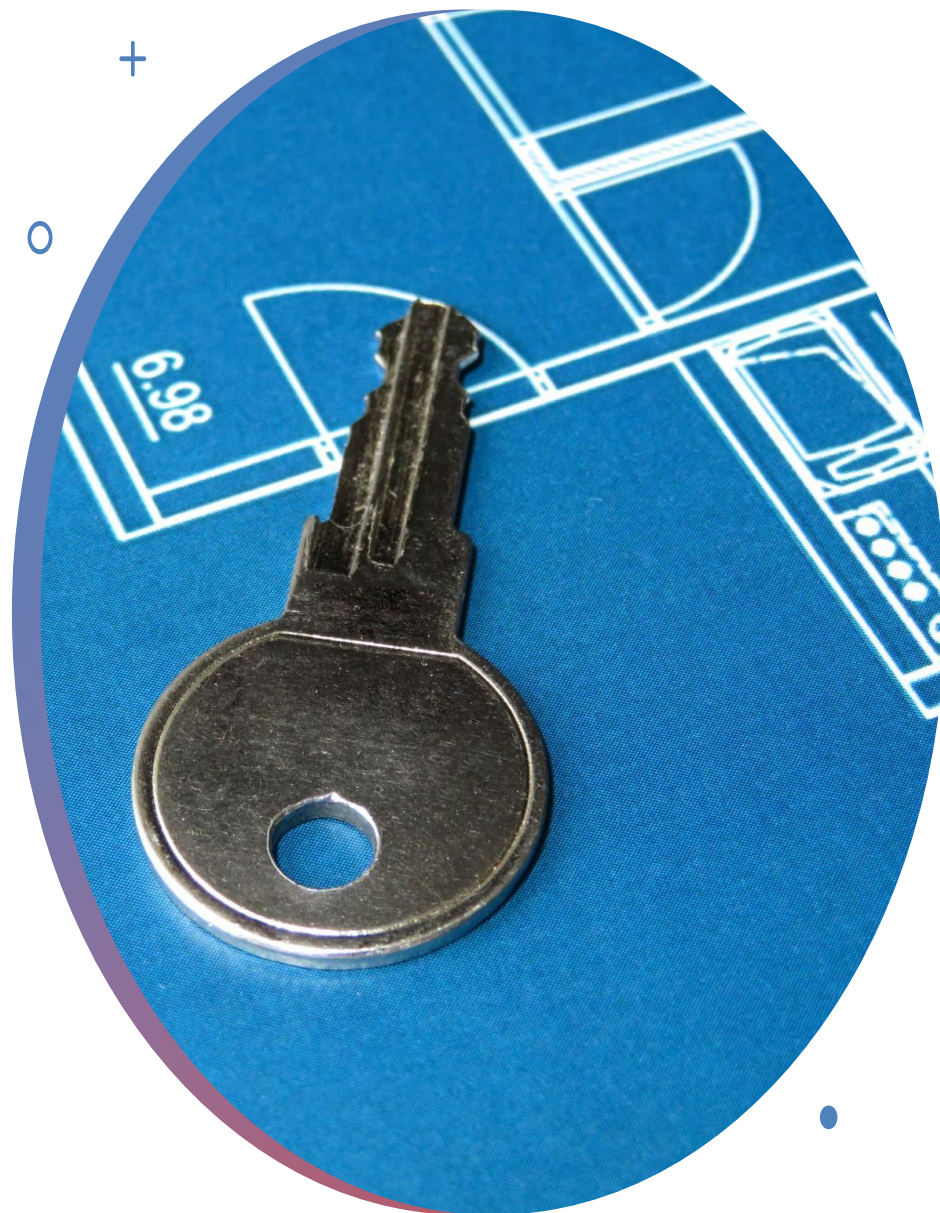
Rise in cyber threats targeting financial institutions



Siloed compliance and security teams create gaps and inefficiencies



**Integration ensures both regulatory alignment and technical protection**



# Key Functions

## Compliance

- Ensures adherence to laws, regulations, and policies
- Focuses on governance, audit, and accountability

## Security

- Protects assets, data, and systems from threats
- Focuses on Confidentiality, Integrity, and Availability



# Biggest shifts of the decade

Excluding local frameworks and regulations in each country



# Common Pain Points

Duplication of efforts (e.g.,  
redundant Risk Assessments)

Misaligned frameworks (e.g.,  
compliance using ISO 27001,  
security using NIST CSF)

Lack of shared visibility into risk  
metrics

Reactive instead of proactive  
coordination

# Integration Roadmap

01

Foundation  
and  
Assessment

02

Governance  
and  
Organization

03

Integrated  
GRC  
Platform

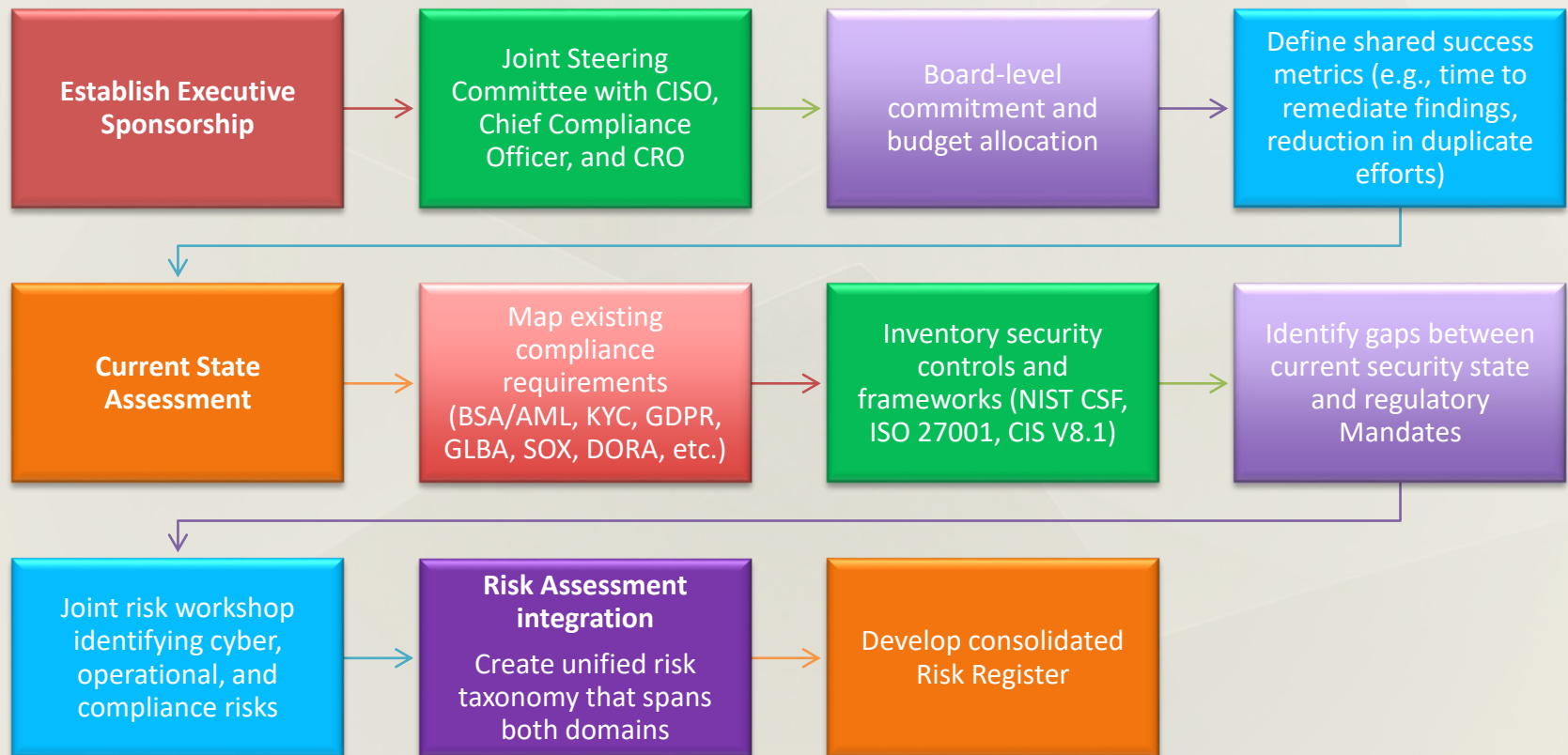
04

Process  
Integration

05

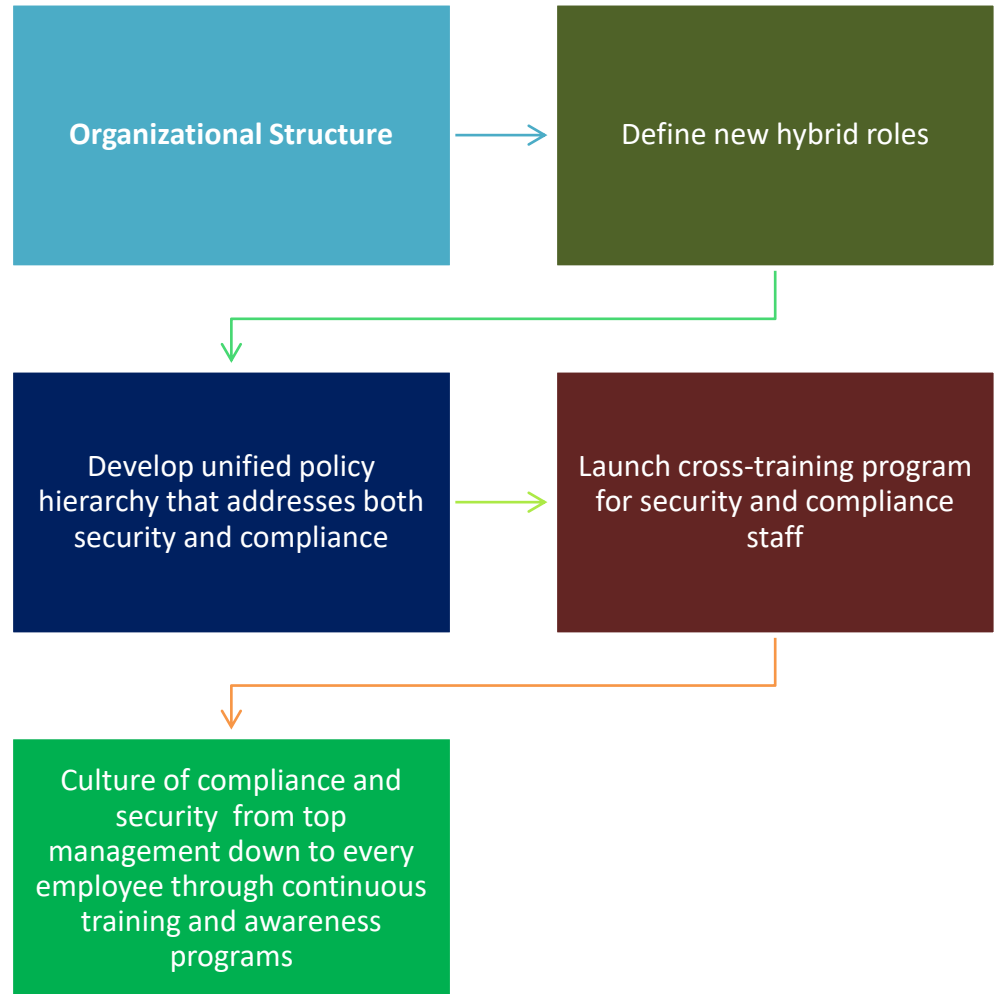
Optimization  
and Maturity

# 1-Foundation and Assessment





## 2-Governance and Organization



# 3- Integrated GRC platform

---

Platform supporting: Risk management (Cyber + Compliance + operational)

Control Mapping and Testing

Incident management with regulatory breach notification workflows

Automated regulatory reporting



## 4- Process Integration

### **Unified Incident Response**

Playbooks addressing both technical containment and regulatory reporting timelines

### **Integrated Third-Party Risk Management**


Consolidate vendor risk assessments and ratings (security & privacy & regulatory requirements)

Monitor third-party controls continuously (critical for DORA requirements)

### **Financial Crime & Cybersecurity Convergence**

Deploy AI/ML solutions for both transaction monitoring (AML) and anomaly detection (security)

**Share threat intelligence between fraud teams and security operations**



## 5- Optimization and Maturity

### Regulatory Technology Enhancement

Develop KRI (Key Risk Indicators) framework spanning both domains

### Continuous Improvement

Integrate advanced technologies **and AI and machine learning** into AML programs



# Benefits to the Bank



Improved efficiency and reduced duplication



Stronger regulatory defense posture



Enhanced board-level reporting on cyber & compliance risks



Reduced audit fatigue



Better customer trust through consistent management of security and compliance

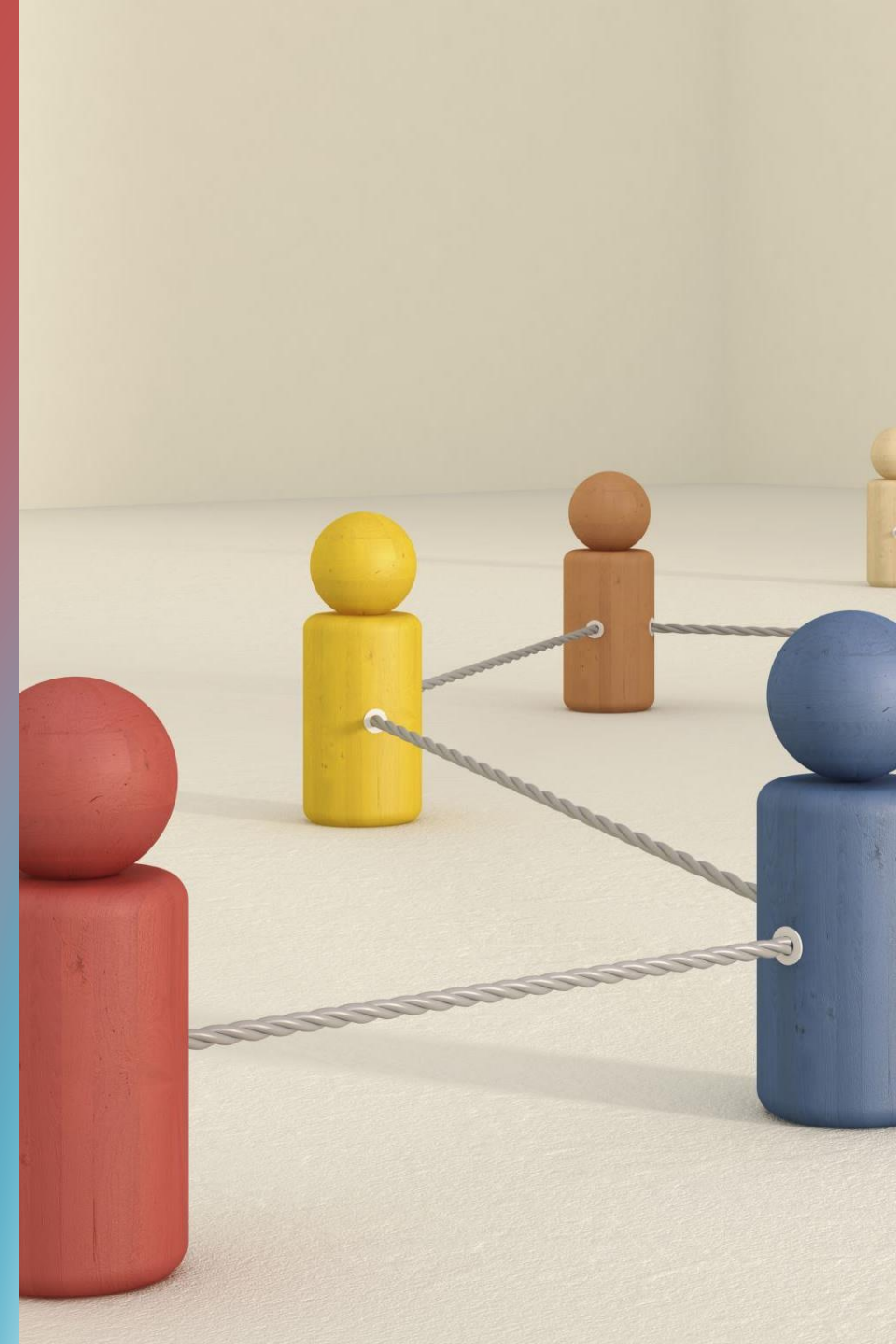
# Key KPIs

- % of common controls automated
- Number of joint audits completed
- Mean time to close compliance findings
- Reduction in duplicate assessments
- Overall risk reduction



# Conclusion

1. Integration between compliance and security transforms obligation into resilience.
2. Unified approach = better protection + smarter governance
3. Cross-functional collaboration is key
4. Continuous alignment with evolving regulatory and threat landscape is crucial



# SECURITY AND COMPLIANCE PARTNERSHIP

In banking, compliance  
builds trust

**AND**

Security Preserves it!





**THANK YOU**

