Strengthening Organizational Cybersecurity Through a phased

ISMS Implementation Roadmap

International Regulatory Conference

Ohrid, May.2026

Nadica Josifovski

Advisor to the Director for Information Security

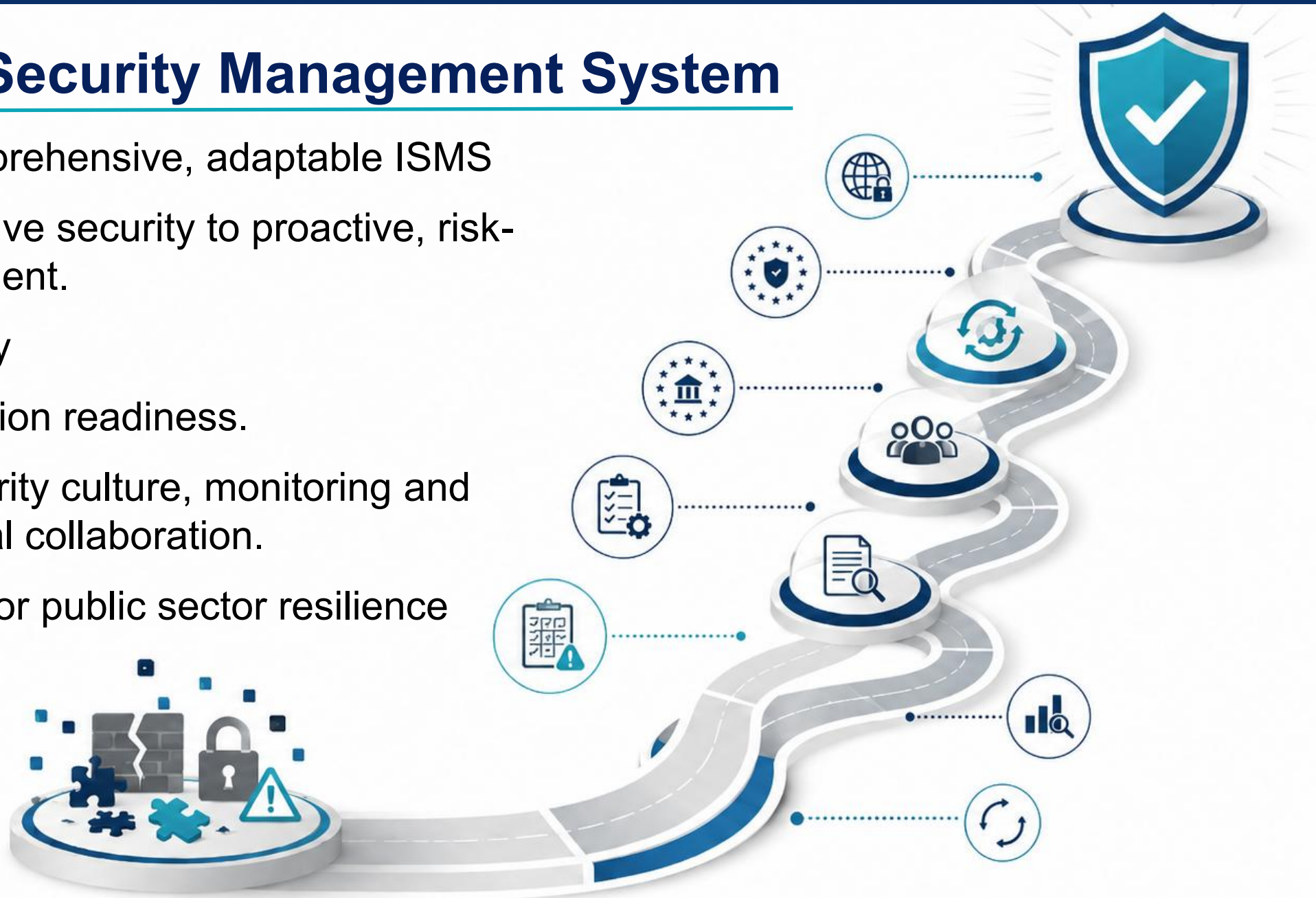
nadica.josifovski@aec.mk

Public Sector Cybersecurity Challenge

- Improved public services
- Higher exposure to cybersecurity risks
- limited capacity, weak coordination
- Fragmented, ad-hock and reactive cybersecurity practices
- Inconsistent risk management
- Regional assessments

Information Security Management System

- ✓ A practical, comprehensive, adaptable ISMS
- ✓ Move from reactive security to proactive, risk-based management.
- ✓ Increase maturity
- ✓ support certification readiness.
- ✓ Strengthen security culture, monitoring and cross-institutional collaboration.
- ✓ ISMS roadmap for public sector resilience



Frameworks Mapping

1

NIS2 Directive

achievements baseline

- Regulatory baseline
- Outcome-focused
- WB6 aligning with EU

2

NIST CSF

Structure and priorities

- Functional model
- Risk-based approach
- Phased implementation

3

ISO/IEC 27001

certifiable model for implementation

- Deepest control granularity
- Certification readiness
- Auditability

Strong **conceptual alignment** between the frameworks

ISMS Implementation Roadmap

1

Governance & Foundation

2

Risk & Asset Baseline

3

Security Controls Implementation

4

Monitoring & Detection

5

Incident Response & Recovery

6

Compliance & Continuous Improvement

Phase 1

Governance &Foundation

- High management **commitment**
- ISMS **scope**,
- **governance** structure
- security **policy**
- **roles** and responsibilities

Establish the ISMS foundation.

Phase 2

Risk & Asset Baseline

- Risk **methodology**
- Risk **register**
- Asset **inventory**
- Risk **treatment** plan.

Create a clear baseline of assets and risks to prioritize mitigation work.

Phase 3

Security Controls Implementation

- Security **controls**
- **Access** management
- Awareness **training**
- Security **policies**

Put the planned safeguards into practice and embed security into daily operations.

Phase 4

Monitoring &Detection

- **Logging** systems
- **Monitoring** processes’
- **Alerting** and **detection** mechanisms.

Increase visibility so security events can be identified and acted on early.

Phase 5

Incident Response & Recovery

- Incident **response** plan
- **Reporting** procedures
- Disaster **recovery**
- **Continuity** plans.

Prepare the public institutions+ to respond quickly and recover with minimal disruption.

Phase 6

Compliance & Continuous Improvement

- **Audit** reports
- **KPIs**
- **Compliance** monitoring
- ISMS **improvement** cycle,
- Plan-Do-Check-Act model .

Track performance and use findings to strengthen the ISMS over time.

ISMS Roadmap Timeline by Institution Maturity level

ISMS Roadmap Phase	I1 – Initial Cybersecurity Maturity	I2 – Intermediate Cybersecurity Maturity	I3 – Advanced Cybersecurity Maturity
Phase 1 – Governance & Foundation	6–12 months	3–6 months	1–3 months
Phase 2 – Risk & Asset Baseline	6–9 months	3–6 months	2–4 months
Phase 3 – Security Controls Implementation	12–24 months	6–12 months	3–9 months
Phase 4 – Monitoring & Detection	6–12 months	4–8 months	2–6 months
Phase 5 – Incident Response & Recovery	6–12 months	4–8 months	2–6 months
Phase 6 – Compliance & Continuous Improvement	Continuous process (initial establishment: 6–12 months)	Continuous process (initial establishment: 4–8 months)	Continuous process (initial establishment: 3–6 months)

ISMS Implementation: Summary of Impact

Challenges

- limited resources
- skills gaps
- resistance to change
- evolving threats.

Key Enablers

- leadership commitment
- phased guidance,
- recognized standards, and
- practical tools for monitoring, auditing, and risk management.

Benefits

- move from reactive security to proactive risk management
- Improving governance, improving data protection,
- Optimized resource use,
- Better resilience,
- Increased public trust

ISMS Implementation: Summary of Impact

Positive Outcomes

Short term:

- improves coordination and response
- Improve resilience

Long term:

- building security culture,
- institutional stability,
- digital service resilience,
- Build trust.

Sustainability & success

Embedding ISMS activities into public institutions governance, risk management, daily operations, awareness, monitoring, audits, and continuous improvement cycles.

Cyber threats cannot be completely eliminated,
but a well-implemented ISMS enables public sector entities to manage risks proactively, minimize impact, and protect their most valuable assets.

Thank You!

nadica.josifovski@aec.mk