



PACIFICA

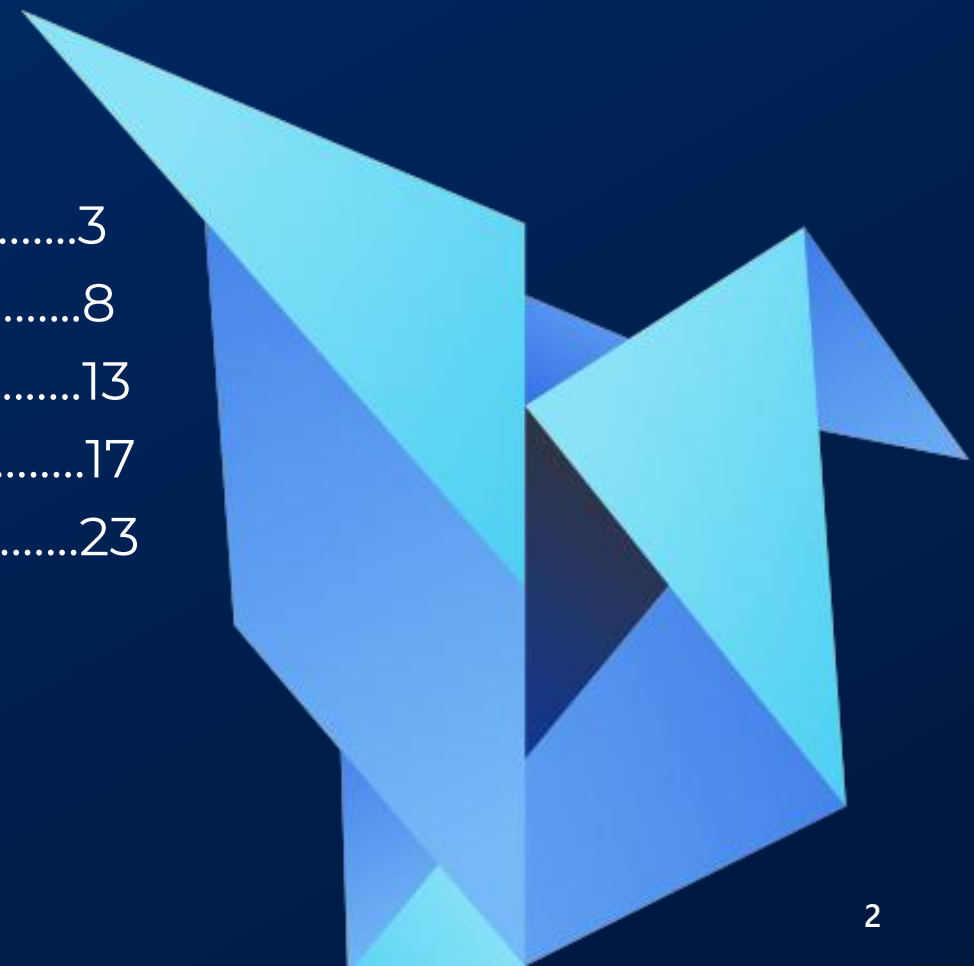
A NOVENTIQ Company

Information Security Management System and How to Live with It

Valery VELEV – Lead Auditor

Table of Contents

- Why Is It Important?3
- What Is ISMS? Breaking It Down Simply8
- “Challenges and Problems”13
- “How to Live with It?”17
- Security Culture as the Outcome23



Why Is It Important?



Why Is It Important?



An **Information Security Management System (ISMS)** is critical for several key reasons:

1. Protection of Business Assets
2. Economic Benefits
3. Compliance with Legislation
4. Ensuring Business Continuity
5. Building Trust
6. Systematic Approach to Security

ISMS is not an expense but a strategic investment in business resilience, reputation, and growth. It is a systematic approach that transforms security from a problem into a **competitive advantage**.

Not Boring Statistics, but Stories



Story 1: «Urgent Transfer from the Director»

Situation: An accountant received an email from a fake corporate account requesting an urgent money transfer. She complied.

Result: Direct financial loss, investigation, downtime.

Story 2: «GitHub Leak»

Situation: A developer, for convenience, posted a code fragment with cloud access keys on a public repository.

Result: Cryptocurrency ransomware, service downtime for days, reputational damage.

Conclusions



Threats are **not** about hackers in balaclavas.

Threats are about **human errors, flawed processes, and direct financial losses.**

The Goal of IS is not to Forbid, but to Enable



Myth: ISMS is about restrictions, complex passwords, and bureaucracy that hinders work.

Reality: ISMS is a systematic approach that enables:

1. Ensure business continuity (prevent it from stopping due to incidents)
2. Protect assets: money, data, reputation
3. Build trust with clients and partners
4. Comply with legal requirements

Analogy: Traffic rules don't prevent driving; they make it predictable and safe for all participants.

What Is ISMS?



ISMS Is Not Hardware, but a System



ISMS Is Not Hardware, but a **System**

This IS NOT: Just a firewall, antivirus, DLP, etc.

This IS: **A complex of interconnected elements**

The International Language of Security: ISO 27001 Standard

This is the most recognized global framework for building an ISMS.

It **doesn't dictate** which technologies to use **but specifies** what needs to be **managed** (risks, assets, incidents).

Core – the PDCA Cycle:

Plan: Define risks, policies, objectives.

Do: Implement protective measures.

Check: Monitor, conduct audits.

Act: Continuously improve the system.



What Does ISMS Consist Of? The Four Pillars



Documentation: «The Rules of the Game.» Policies, regulations, instructions (e.g., Password Policy).

Processes: «How We Play.» Regulations for incident management, access control, and changes.

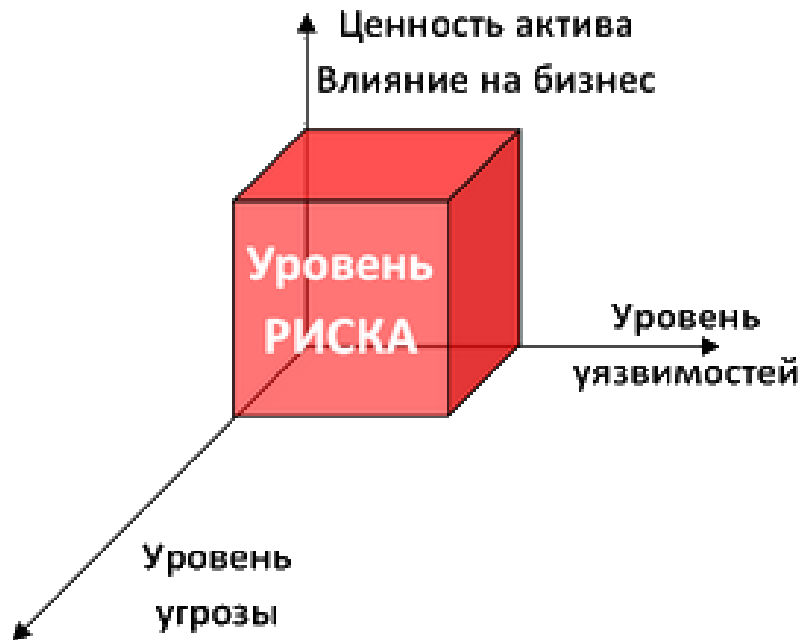
Technologies: «Tools for the Game.» Encryption, access control systems, antiviruses.

People: «The Players.» Training, awareness-raising, building a culture.

Focus on Risks

ISMS Philosophy: You can't protect everything. Protect what's important.

Formula: Risk = Threat × Vulnerability × Asset Value.



Example: Customer database (high value) + Weak password (vulnerability) + Threat of password cracking (threat) = High Risk! Priority for mitigation.

«Challenges and Problems»



Key Challenges

Lack of Management Support

Problem: Information security is seen as a cost, not an investment.

Result: Insufficient budget and authority.

Staff Resistance

Problem: New policies and procedures are perceived as obstacles to work.

Result: Employees find workarounds, nullifying ISMS effectiveness.

Unclear Responsibility Zones

Problem: It's unclear who is responsible for IS processes in departments.

Result: Processes are implemented formally or «left hanging.»

Technical and Organizational Complexities

Technical Barriers:

Integration into Existing IT Infrastructure: Challenges with connecting to legacy systems and diverse equipment.

Tool Selection: A vast market of solutions (SIEM, DLP, IDS/IPS), making it hard to choose without clear requirements.

«**Blind Spots**»: Not all assets are accounted for or protected (shadow IT).

Organizational Barriers:

Creating Policies from Scratch: Developing relevant and feasible IS policies requires deep business process audits.

Lack of Expertise: In-house IT specialists lack knowledge in IS risk management.

ISMS Support and Operation Challenges

Why does the hardest work begin after implementation?

«Paper» ISMS vs. «Living» ISMS

Risk: The system exists only on paper for auditors but isn't used in daily operations.

Continuous Monitoring and Improvement

Problem: Requires constant resources. Processes are rarely reviewed, become outdated, and fail to address new threats.

Incident Management

Problem: Without a streamlined process, incident response is delayed, increasing damage.

Regular Risk Reassessment

Problem: Business and technology change, but the risk map becomes outdated, rendering ISMS ineffective.

«How to Live with It?»



The Role of Leadership

Main Rule: Without top management support, ISMS is just a piece of paper.



What Leadership Must Provide:

- Funding and Resources
- Participation in Risk Assessment and Acceptance
- Public Support and Personal Example

For HR: Security from Day One

IS Briefing – a mandatory part of onboarding.

IS Compliance Clause in employment contracts.

Regular Training (e.g., mock phishing campaigns).

Exit Briefing upon termination (revoking access rights).

For Every Employee: 4 Simple Rules

Passwords: Use a password manager. Enable 2FA (two-factor authentication) wherever possible.

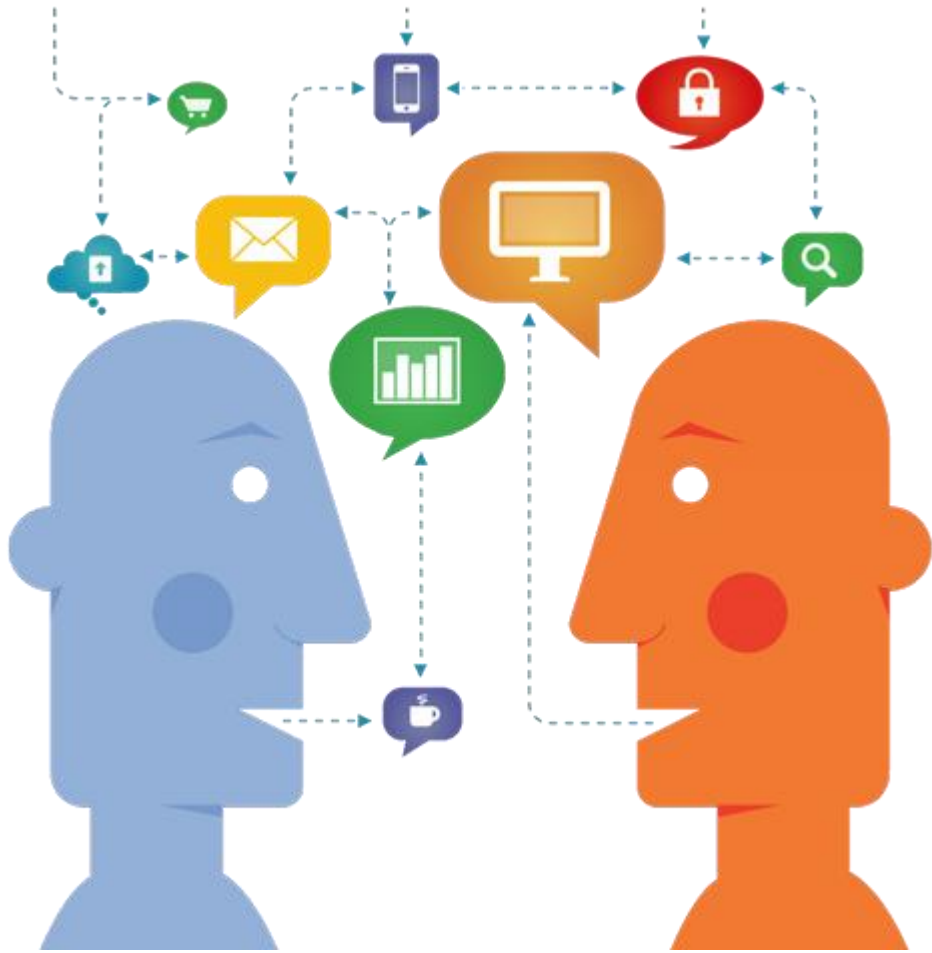
Phishing: Don't click links or open attachments in suspicious emails. If in doubt, call the sender!

Data: Work with confidential information only in approved corporate systems (not personal email/chats).



Cleanliness: Lock your computer when stepping away. Follow the clean desk policy.

For the IT Department: Not a Lone Hero, but a Partner



Communication with Business:

Understand which processes are critical to the business.

Automation:

Software updates, vulnerability scanning.

Incident Preparedness:

Conduct response drills before incidents occur.

Incident Lifecycle

Detection (someone notices and reports) → **Response** (IT isolates the threat) → **Mitigation** (removing malware) → **Recovery** (resuming operations) → **Lessons Learned** (the key stage!)



Important! Don't look for someone to blame; identify the process flaw and improve the system.

Security Culture Is the Outcome

The **goal** is not to scare but to build **habits**.

Encourage Reporting Suspicious Activity («If you see something, say something»).

Make Security Convenient (provide the right tools).

Motivate and Highlight Positive Examples.



Benefits and Outcomes

Before: IS was a cost center, a budget drain, and a source of inconvenience.

Now: ISMS is an investment in:

- Business Stability
- Reputation and Competitive Advantage
- Predictability and Manageability

Challenges Are Normal:

- Resistance to change is natural.
- Technical issues are resolved gradually.
- Budgets can always be optimized.

Success Depends On:

- ✓ Leadership Support (the #1 factor!)
- ✓ Realistic Planning
- ✓ Constant Communication
- ✓ Flexible Implementation Approach

Thank You for Your Attention!

ISMS is a marathon, not a sprint.

What matters is not perfect conditions but steady progress forward.



PACIFICA

A NOVENTIQ Company

