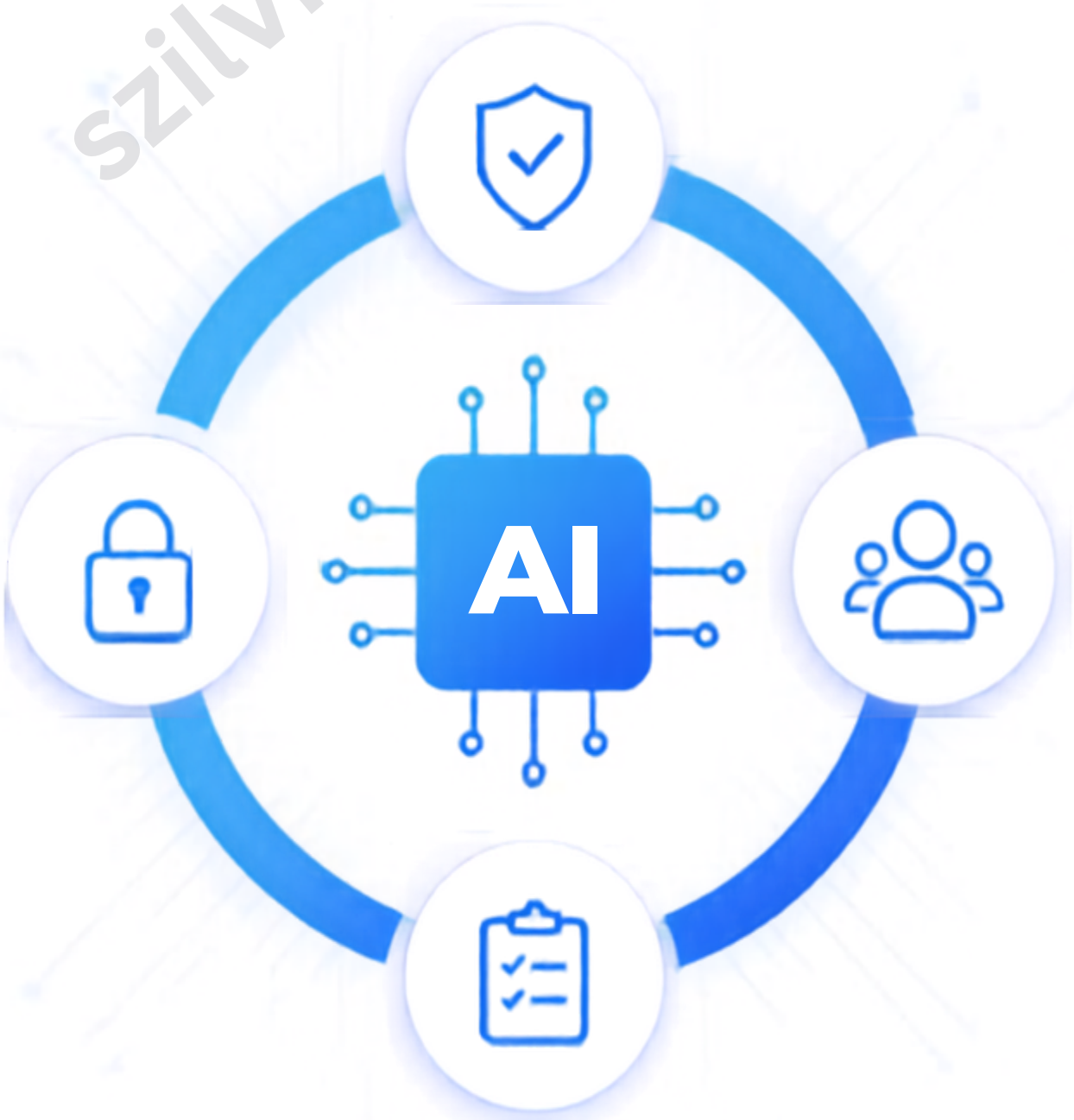




Cybersecurity and AI Management System





An AIMS

(such as frameworks aligned with ISO/IEC 42001)

establishes the policies, risk management protocols, and governance for an organization's AI lifecycle.



Cybersecurity

provides the technical safeguards needed to make that management system viable and secure.



“

Accuracy, robustness and cybersecurity

High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle.

”



Cybersecurity prEN 18282

prEN 18282 is a European draft standard titled "Artificial intelligence - Cybersecurity specifications for AI Systems", designed to support compliance with Article 15 of the EU AI Act.



Part 1
(normative)



Part 2
(guidance & examples)

Core Focus and Scope



Target:

Focused explicitly on high-risk artificial intelligence systems.



Goal:

Protect AI systems from cyber threats, attacks, and technical failures throughout their entire lifecycle.



Key Lifecycle Outcome Categories



Prevent



Detect



Respond



Resolve



Control





Other relevant directives and norms:



**EU Directive
2022/2555 - NIS2
(Network and
Information Security
Directive 2) in the EU**



**prEN 18286 -
AI Quality Management
System**



**ISO/IEC 42001 -
AI Management
System**



**ISO 27001 - global
standard for
Information Security
Management Systems**



**IEC 62443 for
industrial AI**



**NIST - voluntary set of
risk management
guidelines created in
the United States**

**Don't miss out on
the latest updates
on AI, technology,
and compliance.**

**Follow me on
LinkedIn!**