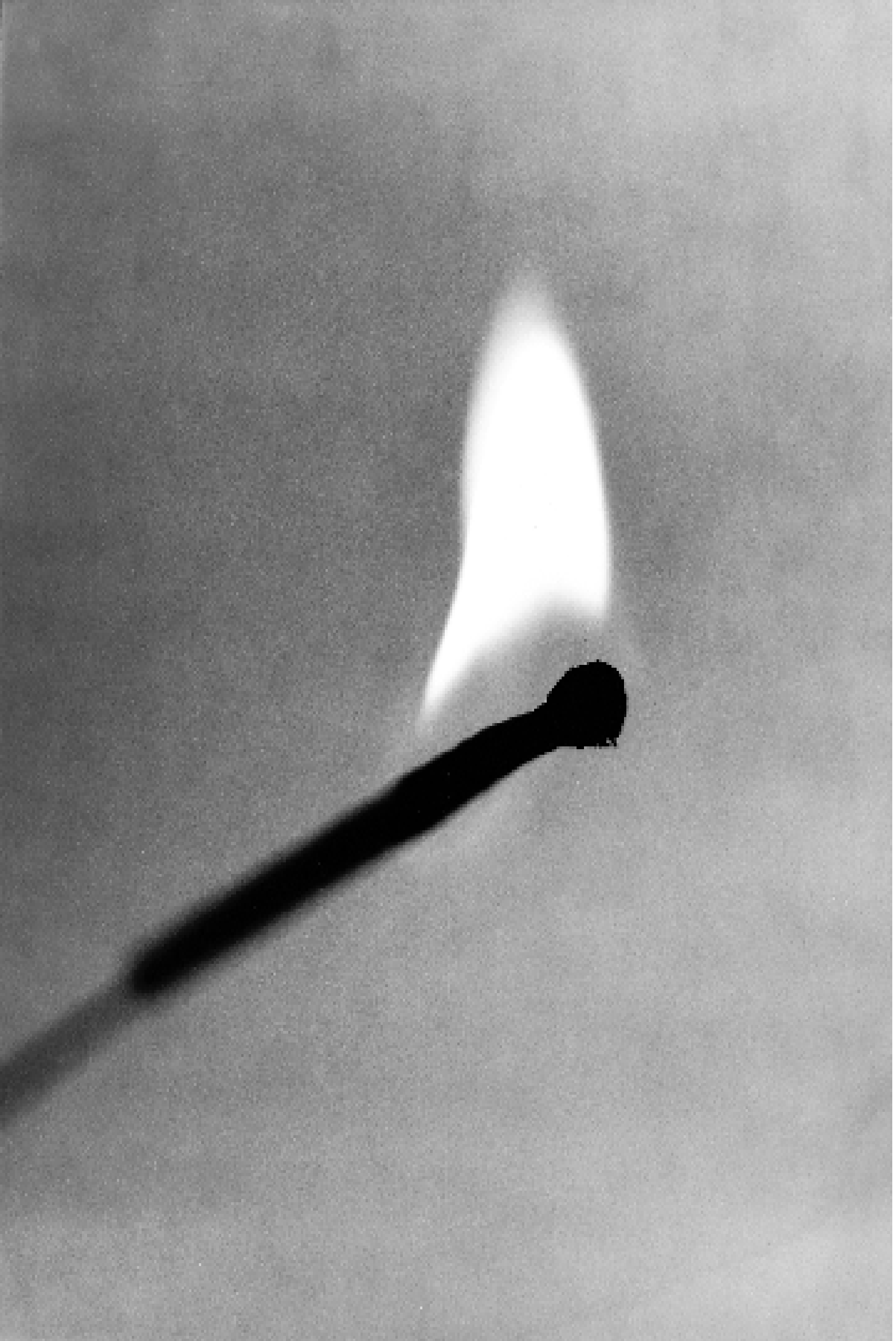
Economical aspects of IT Security Risk Management in Industry

Aleksander Poniewierski
Mirosław Ryba

Agenda

- IT Risk
- IT Risk Management – Risk Handling Strategies
- MIR-2M – Multidimensional IT Risk Management Methodology
- ORBI – IT Security Risk Assessment Methodology
- Summary



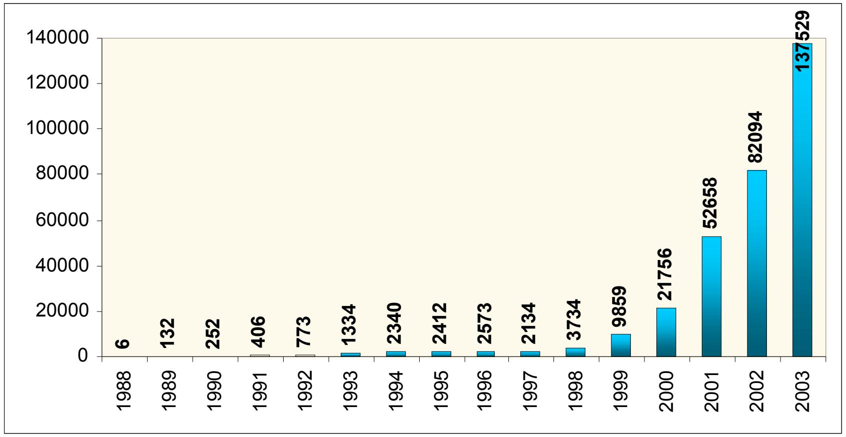
IT Risk

IT Facts, Losses & Research 1/2

- The world economy is virtually IT-dependent – most companies' functioning is based on IT systems.
- According to Contingency Planning Association Research; Strategic Research Corp. an average cost of one-hour-long malfunction amounts to:
  - 2.600.000 USD in case of credit card payment authorization center
  - 89.500 USD in case of plane tickets booking Internet system
- As the result of breaking into the bank accounts system one of the biggest and world best known financial giants reported losses, which may total even 700.000 USD
- Eurobank's main IT system was down for a few days – during the following week the clients had no access to their funds and could not be dealt with properly
- The most serious loss concerning a single attack reported in 2003 accounted to 35.000.000 USD (intellectual property theft)

IT Facts, Losses & Research 2/2

- An average hacking into an unprotected internet server takes place within 4 hours after its deployment
- In the recent years there has been a rocketing increase of the revealed information on IT systems' vulnerability, according to CERT/CC publications
- „Certified Fraud Examiners" organization estimates that an average entity in the USA loses around 6% of their annual revenues due to fraud activities
- Disguised annual loss of a single company related to IT intrusion are estimated at 500.000 USD
- It is estimated that companies lose up to 5% of their revenues due to 'non-business' use of the Internet by their employees



The number of incidents reported to CERT/CC in the years 1988–2003

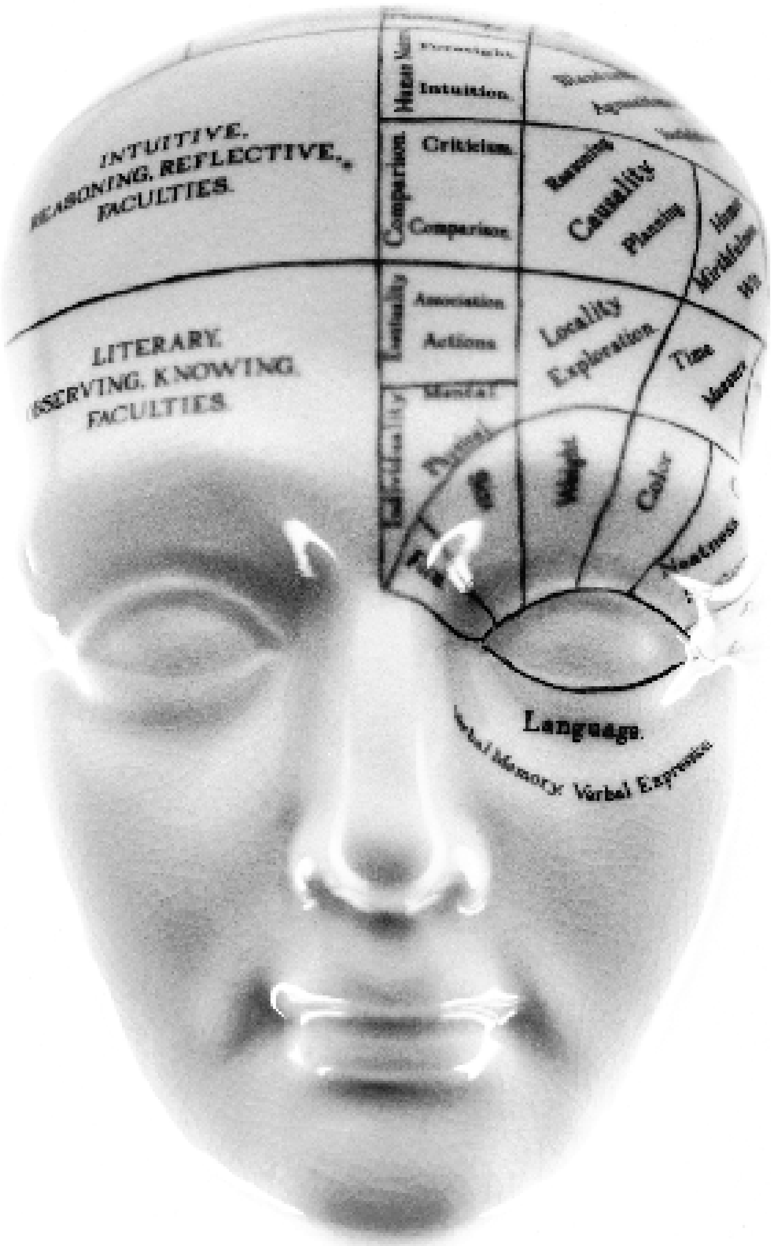
What Is IT Risk?

Risk categories:

- Confidentiality
- Integrity
- Availability

Applies to:

- Information protected by law regulations
- Business information

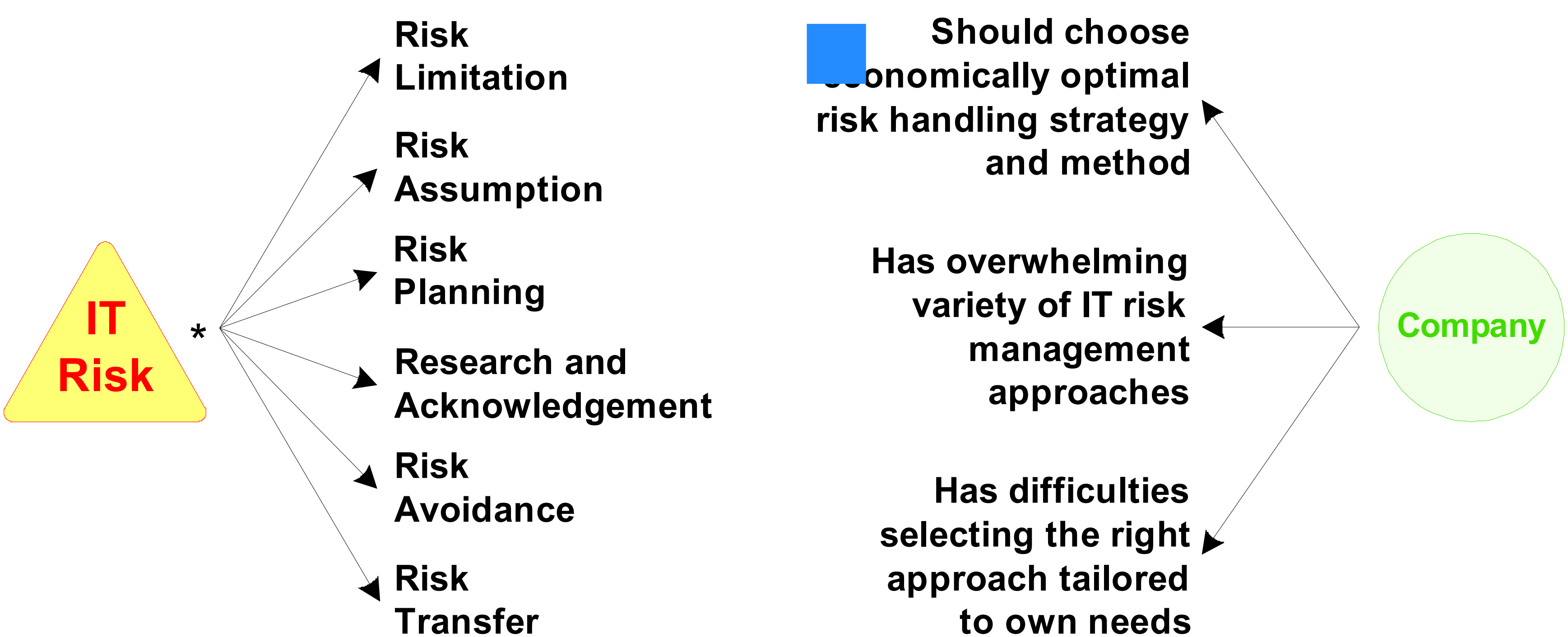


IT Risk Assessment

Risk Handling Strategies

IT Risk Assessment & Handling Problems

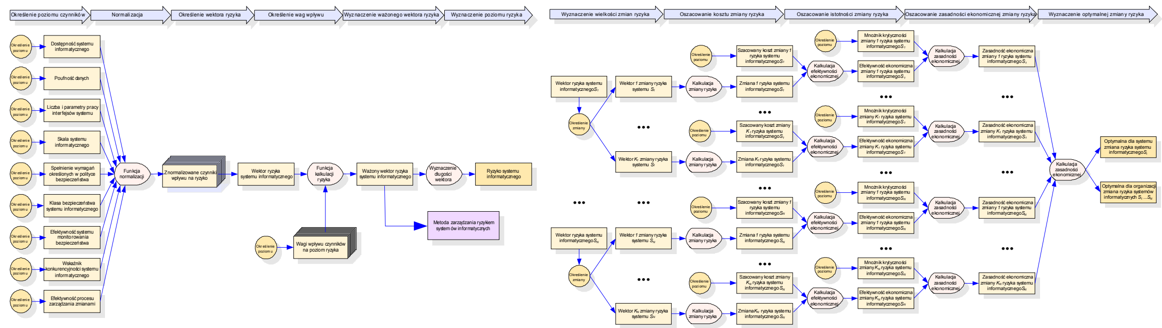
- Lack of credible, complete and integral base of statistical data enabling estimation of risk
- Lack of uniform approach to analyzing threats resulting from IT risks

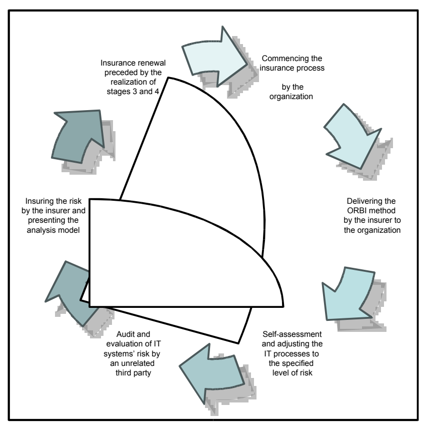


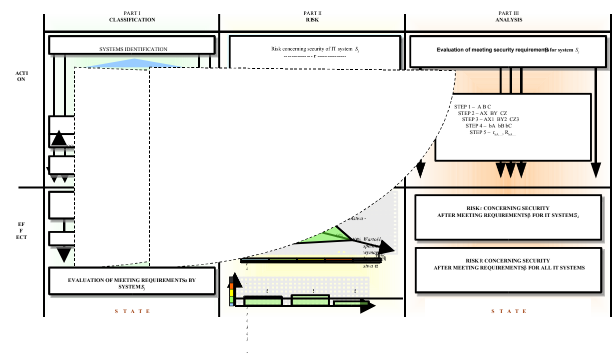
* Source: National Institute of Standards and Technology
SP800-30 Risk Management Guide for Information Technology Systems

IT Risk Handling Strategies

- **Risk Limitation** →
- Risk Assumption
- Risk Planning
- Research and Acknowledgment
- Risk Avoidance
- **Risk Transfer (Insurance)** →



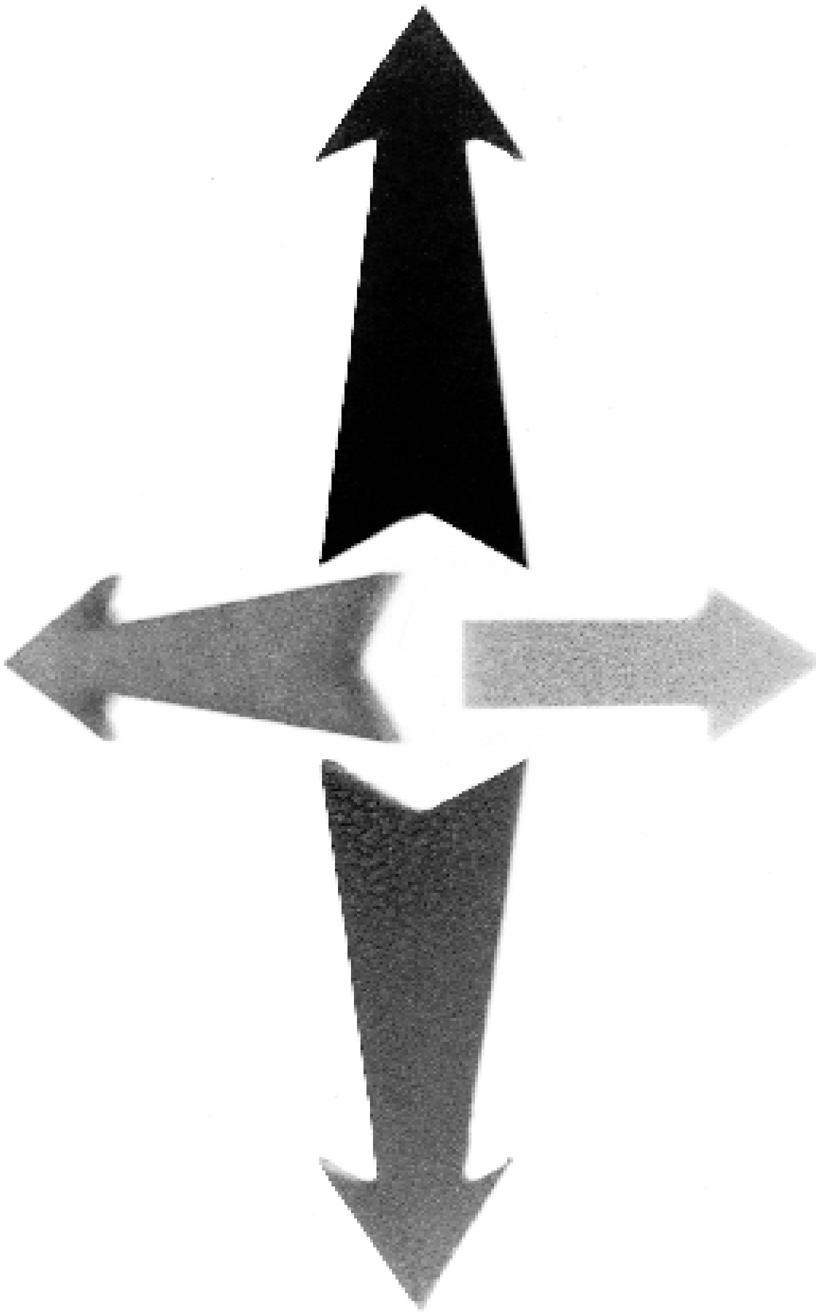




Inside perspective

Outside perspective

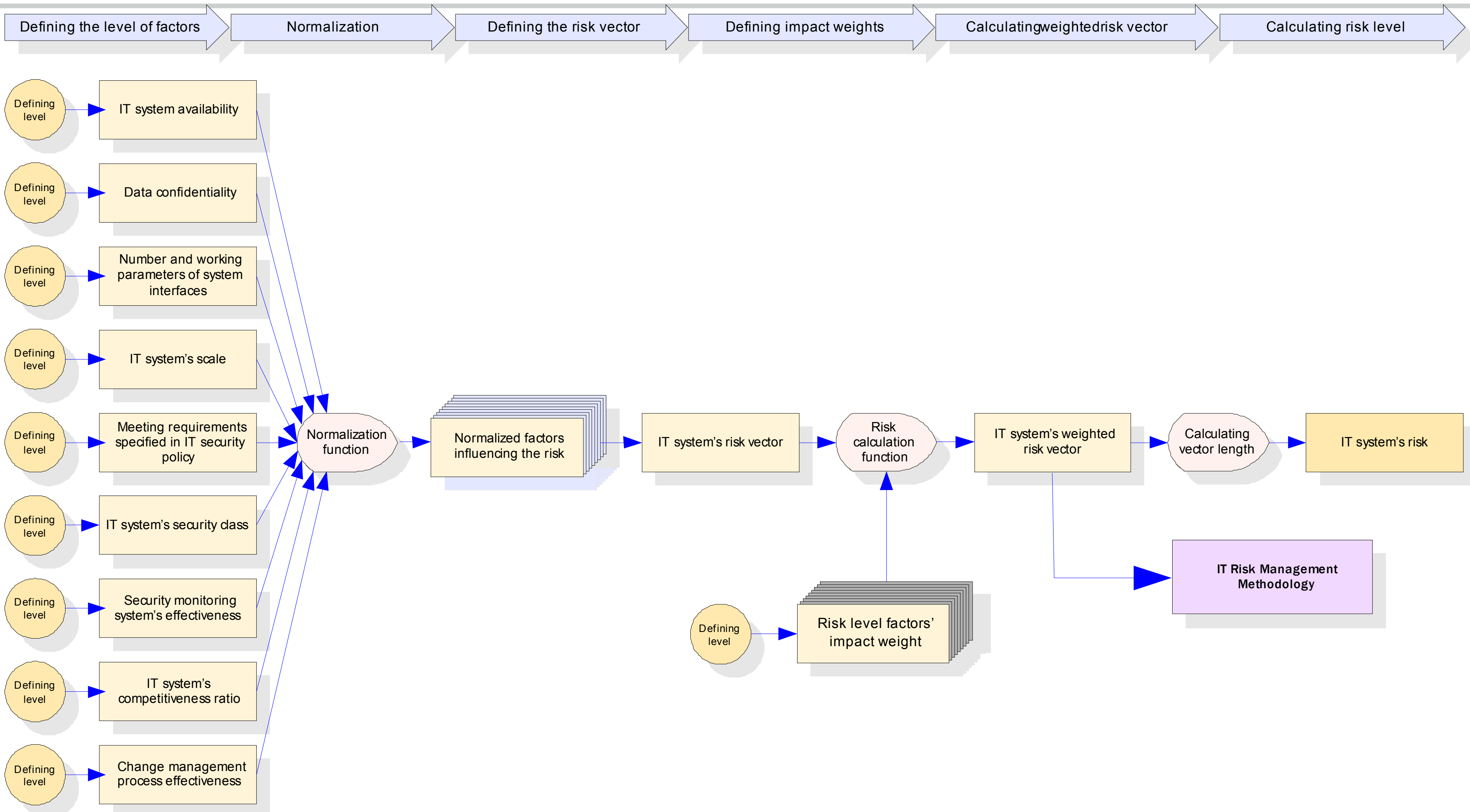
Quality In Everything We Do



MIR-2M – Multidimensional IT Risk Management Methodology

Author: Mirosław Ryba

MIR-2M – Risk Analysis



Quality In Everything We Do

MIR-2M – IT System Risk Vector

- **IT system risk vector** $\vec{R}_{S_i}$

$$\vec{R}_{S_i} = \varsigma_\lambda\left(\lambda_{S_i}\right)\cdot\vec{\lambda} + \varsigma_\rho\left(\rho_{S_i}\right)\cdot\vec{\rho} + \varsigma_\nu\left(\nu_{S_i}\right)\cdot\vec{\nu} + \varsigma_\omega\left(\omega_{S_i}\right)\cdot\vec{\omega} + \varsigma_\eta\left(\eta_{S_i}\right)\cdot\vec{\eta} + \varsigma_\theta\left(\theta_{S_i}\right)\cdot\vec{\theta} + \varsigma_\iota\left(\iota_{S_i}\right)\cdot\vec{\iota} + \varsigma_\kappa\left(\kappa_{S_i}\right)\cdot\vec{\kappa} + \varsigma_\varphi\left(\varphi_{S_i}\right)\cdot\vec{\varphi}$$

  - λ_{S_i} – system availability
  - ρ_{S_i} – data confidentiality
  - υ_{S_i} – number of system interfaces and working parameters
  - ω_{S_i} – system's scale
  - η_{S_i} – meeting security requirements
  - θ_{S_i} – DoD TCSEC security class
  - τ_{S_i} – security monitoring system's effectiveness
  - κ_{S_i} – competitiveness ratio
  - φ_{S_i} – change management process effectiveness

$$\varsigma_\lambda\left(\lambda_{S_i}\right) = \begin{cases} 1, & \text{when } \lambda_{S_i} = V \\ 3, & \text{when } \lambda_{S_i} = IV \\ 5, & \text{when } \lambda_{S_i} = III \\ 7, & \text{when } \lambda_{S_i} = II \\ 9, & \text{when } \lambda_{S_i} = I \end{cases}$$

$$\varsigma_\theta\left(\theta_{S_i}\right) = \begin{cases} 1, & \text{when } \theta_{S_i} = A \\ 2, & \text{when } \theta_{S_i} = B3 \\ 3, & \text{when } \theta_{S_i} = B2 \\ 4, & \text{when } \theta_{S_i} = B1 \\ 7, & \text{when } \theta_{S_i} = C2 \\ 8, & \text{when } \theta_{S_i} = C1 \\ 11, & \text{when } \theta_{S_i} = D \end{cases}$$

$$\varsigma_\rho\left(\rho_{S_i}\right) = \begin{cases} 1, & \text{when } \rho_{S_i} = E \\ 3, & \text{when } \rho_{S_i} = D \\ 5, & \text{when } \rho_{S_i} = C \\ 7, & \text{when } \rho_{S_i} = B \\ 9, & \text{when } \rho_{S_i} = A \end{cases}$$

$$\varsigma_\eta\left(\eta_{S_i}\right) = 1 + 10\cdot\left(1 - \frac{\eta_{S_i}}{100\%}\right)$$

$$\varsigma_\iota\left(\iota_{S_i}\right) = 11 - \sqrt[3]{\frac{\iota_{S_i}}{2}}$$

$$\varsigma_\nu\left(\nu_{S_i}\right) = \min\left(\sqrt[3]{\frac{1+\nu_{S_i}}{2}}\,,\ 10\right)$$

$$\varsigma_\kappa\left(\kappa_{S_i}\right) = \min\left(1 + \log_{3/2}\left(1+\kappa_{S_i}\right), 11\right)$$

$$\varsigma_\omega\left(\omega_{S_i}\right) = 1 + \omega_{S_i}$$

$$\varsigma_\varphi\left(\varphi_{S_i}\right) = 1 + \frac{100\% - \varphi_{S_i}}{10\%}$$

- **IT system weighted risk vector** $\vec{\Re}_{S_i}$

$$\vec{\Re}_{S_i} = \vec{\Psi} \otimes \vec{R}_{S_i}$$

where

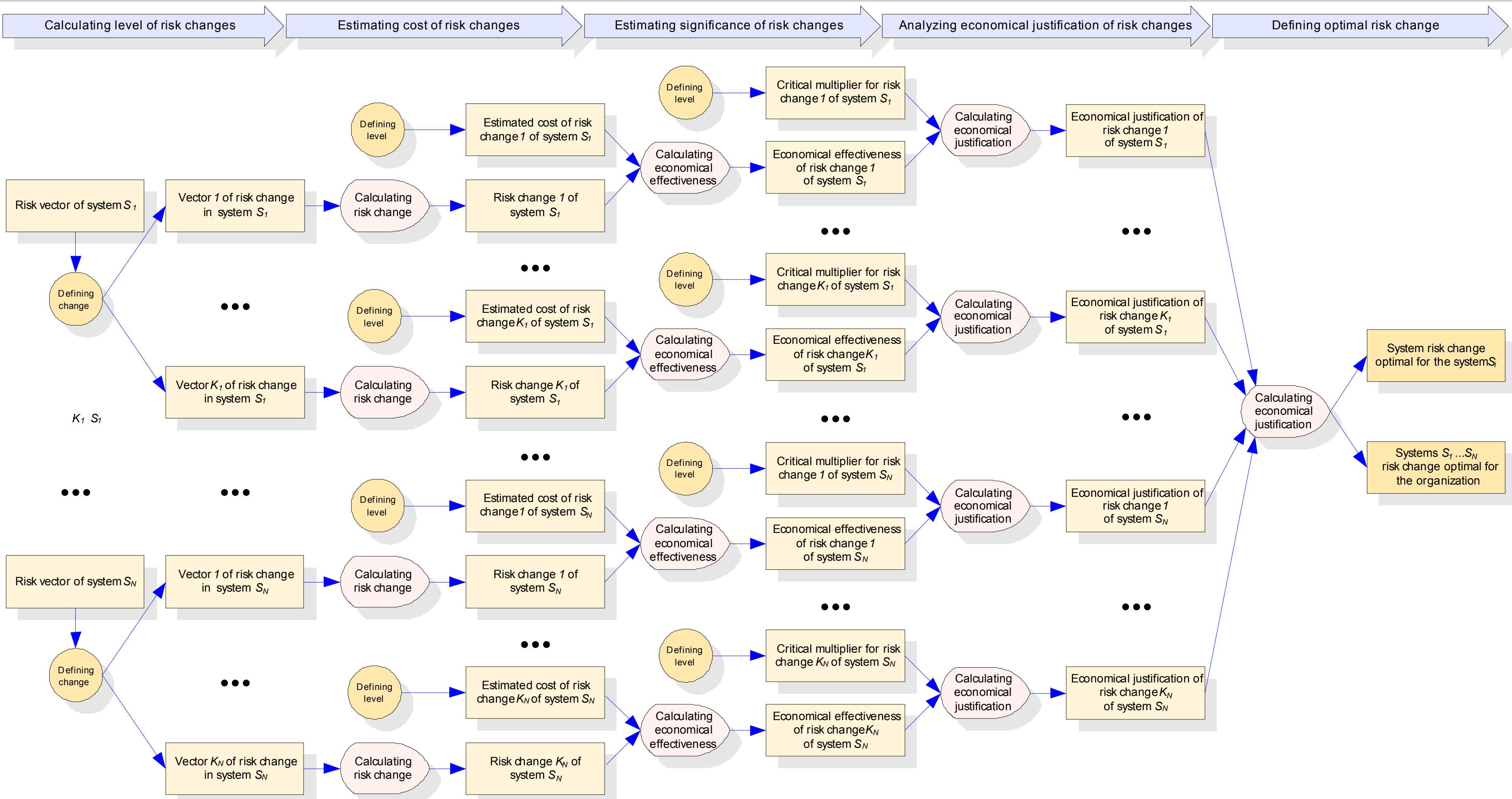
$$\vec{\Psi} = \left[\psi_{ij}\right] \in M^{m\times n}$$

$$\forall i \in \{1,\dots,m\};\ \forall j \in \{1,\dots,n\} \quad \psi_{ij} \geq 0{,}1 \quad \text{and} \quad \sum_i^m \sum_j^n \psi_{ij} = 10$$

$$\left[c_{ij}\right] = \left[a_{ij}\right] \otimes \left[b_{ij}\right]$$

$$c_{ij} = a_{ij}\cdot b_{ij}$$

MIR-2M – Risk Management



Quality In Everything We Do

MIR-2M – IT System Risk Change

- **IT system risk change vector** $\Delta\vec{R}_{S_i}^{h}$

$$\Delta\vec{R}_{S_i}^{k} = \vec{R}_{S_i}^{k} - \vec{R}_{S_i}$$

- **IT system weighted risk change** $\Delta R_{S_i}^{k}$

$$\Delta R_{S_i}^{k} = \left\| \vec{\Re}_{S_i}^{k} \right\| - \left\| \vec{\Re}_{S_i} \right\|$$

- **Estimated cost of IT system risk change** $\tilde{\Phi}_{\Delta\vec{R}_{S_i}^{k}}$

$$\tilde{\Phi}_{\Delta\vec{R}_{S_i}^{k}} = \sum_{l=0}^{L} \frac{{}^{l}U_{S_i}^{k} - {}^{l}I_{S_i}^{k} - {}^{l}M_{S_i}^{k} - \Delta\mu_{S_i}^{k}}{(1+r)^{l}}$$

$$NPV = \sum_{i=0}^{n} \frac{NCF_i}{(1+k)^{i}}$$

L – period, for which utilization of IT system S_i is planned (in years)

${}^{l}U_{S_i}^{k}$ – savings in year *i* resulting from the IT system S_i risk change represented by the vector $\Delta\vec{R}_{S_i}^{k}$

${}^{l}I_{S_i}^{k}$ – investment expenditure in year *i* on IT system S_i related to implementation of risk change represented by the vector $\Delta\vec{R}_{S_i}^{k}$

${}^{l}M_{S_i}^{k}$ – expenditure in year *i* related to maintenance of mechanisms in system S_i causing risk change represented by the vector $\Delta\vec{R}_{S_i}^{k}$

r – discount rate during the period, for which utilization of IT system S_i is planned

$\Delta\mu_{S_i}^{k}$ – change of ALE (Annual Loss Expectancy) for the IT system S_i

MIR-2M – Risk Change Economical Effectiveness

- **Economical effectiveness of IT system risk change**

$$\chi\left(\Delta\vec{R}_{S_i}^k\right) = \frac{\Delta R_{S_i}^k}{\widetilde{\Phi}_{\Delta\vec{R}_{S_i}^k}}$$

- **Change significance multiplier**

$$\hbar_{S_i}^k = \begin{cases} 2 & \text{when implementation of change represented by vector } \Delta\vec{R}_{S_i}^k \text{ is a legal obligation} \\ 1 & \text{when implementation of change represented by vector } \Delta\vec{R}_{S_i}^k \text{ is significant from the point of view of business processes} \\ 0 & \text{in other cases} \end{cases}$$

- **Economical justification of IT system risk change variants:**

$$\dot{\zeta}_{S_i}^k = \begin{cases} 2^{\hbar_{S_i}^k} \cdot \chi\left(\Delta\vec{R}_{S_i}^k\right) & , \left(\Delta R_{S_i}^k < 0\right) \wedge \left(\widetilde{\Phi}_{\Delta\vec{R}_{S_i}^k} > 0\right) \\ 0 & , \left(\Delta R_{S_i}^k > 0\right) \vee \left(\widetilde{\Phi}_{\Delta\vec{R}_{S_i}^k} < 0\right) \end{cases}$$

$$\ddot{\zeta}_{S_i}^k = \begin{cases} 2^{\hbar_{S_i}^k} \cdot \chi\left(\Delta\vec{R}_{S_i}^k\right) & , \left(\Delta R_{S_i}^k < 0\right) \wedge \left(\widetilde{\Phi}_{\Delta\vec{R}_{S_i}^k} < 0\right) \\ 0 & , \left(\Delta R_{S_i}^k > 0\right) \vee \left(\widetilde{\Phi}_{\Delta\vec{R}_{S_i}^k} > 0\right) \end{cases}$$

$$\dddot{\zeta}_{S_i}^k = \begin{cases} 2^{\hbar_{S_i}^k} \cdot \chi\left(\Delta\vec{R}_{S_i}^k\right) & , \left(\Delta R_{S_i}^k > 0\right) \wedge \left(\widetilde{\Phi}_{\Delta\vec{R}_{S_i}^k} > 0\right) \\ 0 & , \left(\Delta R_{S_i}^k < 0\right) \vee \left(\widetilde{\Phi}_{\Delta\vec{R}_{S_i}^k} < 0\right) \end{cases}$$

MIR-2M – Optimal Risk Change

- **IT system risk change optimal for the system** δ_{S_i}

$$\delta_{S_i} = \begin{cases} \dot{\delta}_{S_i} & , \text{ when } \dot{\delta}_{S_i} \neq 0 \\ \ddot{\delta}_{S_i} & , \text{ when } \left(\dot{\delta}_{S_i} = 0\right) \wedge \left(\neg\bar{\lambda} \vee \left(\bar{\lambda} \wedge \left(\ddot{\delta}_{S_i} \leq \dddot{\delta}_{S_i}\right)\right)\right) \\ \dddot{\delta}_{S_i} & , \text{ when } \left(\dot{\delta}_{S_i} = 0\right) \wedge \bar{\lambda} \wedge \left(\ddot{\delta}_{S_i} > \dddot{\delta}_{S_i}\right) \end{cases}$$

$$\dot{\delta}_{S_i} = \max\left(\left|\dot{\zeta}^{1}_{S_i}\right|, \left|\dot{\zeta}^{2}_{S_i}\right|, \ldots, \left|\dot{\zeta}^{K_i}_{S_i}\right| \right)$$

$$\ddot{\delta}_{S_i} = \max\left(\ddot{\zeta}^{1}_{S_i}, \ddot{\zeta}^{2}_{S_i}, \ldots, \ddot{\zeta}^{K_i}_{S_i} \right)$$

$$\dddot{\delta}_{S_i} = \min\left(\dddot{\zeta}^{1}_{S_i}, \dddot{\zeta}^{2}_{S_i}, \ldots, \dddot{\zeta}^{K_i}_{S_i} \right)$$

- **IT system risk change optimal for the organization** $\delta_{S(O)}$

$$\delta_{S(O)} = \begin{cases} \dot{\delta}_{S(O)} & , \text{ when } \dot{\delta}_{S(O)} \neq 0 \\ \ddot{\delta}_{S(O)} & , \text{ when } \left(\dot{\delta}_{S(O)} = 0\right) \wedge \left(\neg\bar{\lambda} \vee \left(\bar{\lambda} \wedge \left(\ddot{\delta}_{S(O)} \leq \dddot{\delta}_{S(O)}\right)\right)\right) \\ \dddot{\delta}_{S(O)} & , \text{ when } \left(\dot{\delta}_{S(O)} = 0\right) \wedge \bar{\lambda} \wedge \left(\ddot{\delta}_{S(O)} > \dddot{\delta}_{S(O)}\right) \end{cases}$$

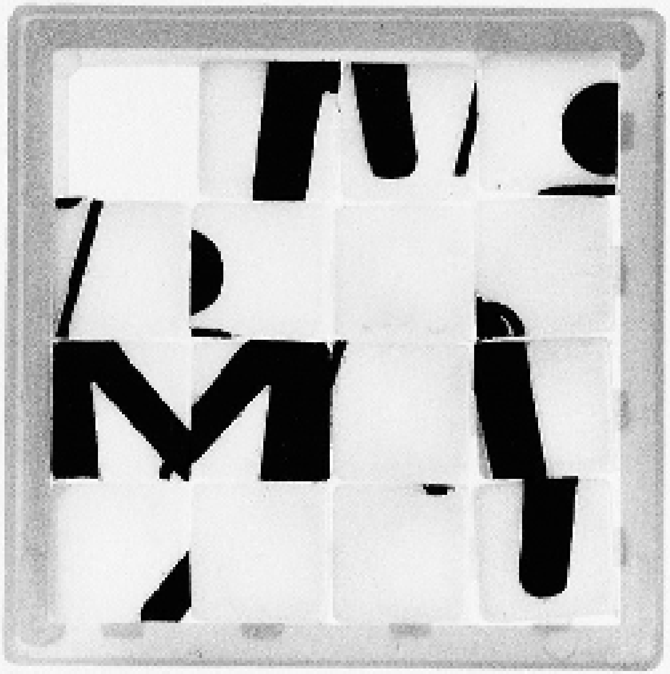
$$\dot{\delta}_{S(O)} = \max\left(\left|\dot{\zeta}^{1}_{S_1}\right|, \left|\dot{\zeta}^{2}_{S_1}\right|, \ldots, \left|\dot{\zeta}^{K_1}_{S_1}\right|, \left|\dot{\zeta}^{1}_{S_2}\right|, \ldots, \left|\dot{\zeta}^{k}_{S_i}\right|, \ldots, \left|\dot{\zeta}^{K_N}_{S_N}\right| \right)$$

$$\ddot{\delta}_{S(O)} = \max\left(\ddot{\zeta}^{1}_{S_1}, \ddot{\zeta}^{2}_{S_1}, \ldots, \ddot{\zeta}^{K_1}_{S_1}, \ddot{\zeta}^{1}_{S_2}, \ldots, \ddot{\zeta}^{k}_{S_i}, \ldots, \ddot{\zeta}^{K_N}_{S_N} \right)$$

$$\dddot{\delta}_{S(O)} = \min\left(\dddot{\zeta}^{1}_{S_1}, \dddot{\zeta}^{2}_{S_1}, \ldots, \dddot{\zeta}^{K_1}_{S_1}, \dddot{\zeta}^{1}_{S_2}, \ldots, \dddot{\zeta}^{k}_{S_i}, \ldots, \dddot{\zeta}^{K_N}_{S_N} \right)$$

- **Acceptance indicator for risk level increase** $\bar{\lambda}$

$$\bar{\lambda} = \begin{cases} 1 & \text{when the organization accepts increasing of risk level} \\ 0 & \text{when the organization rejects increasing of risk level} \end{cases}$$

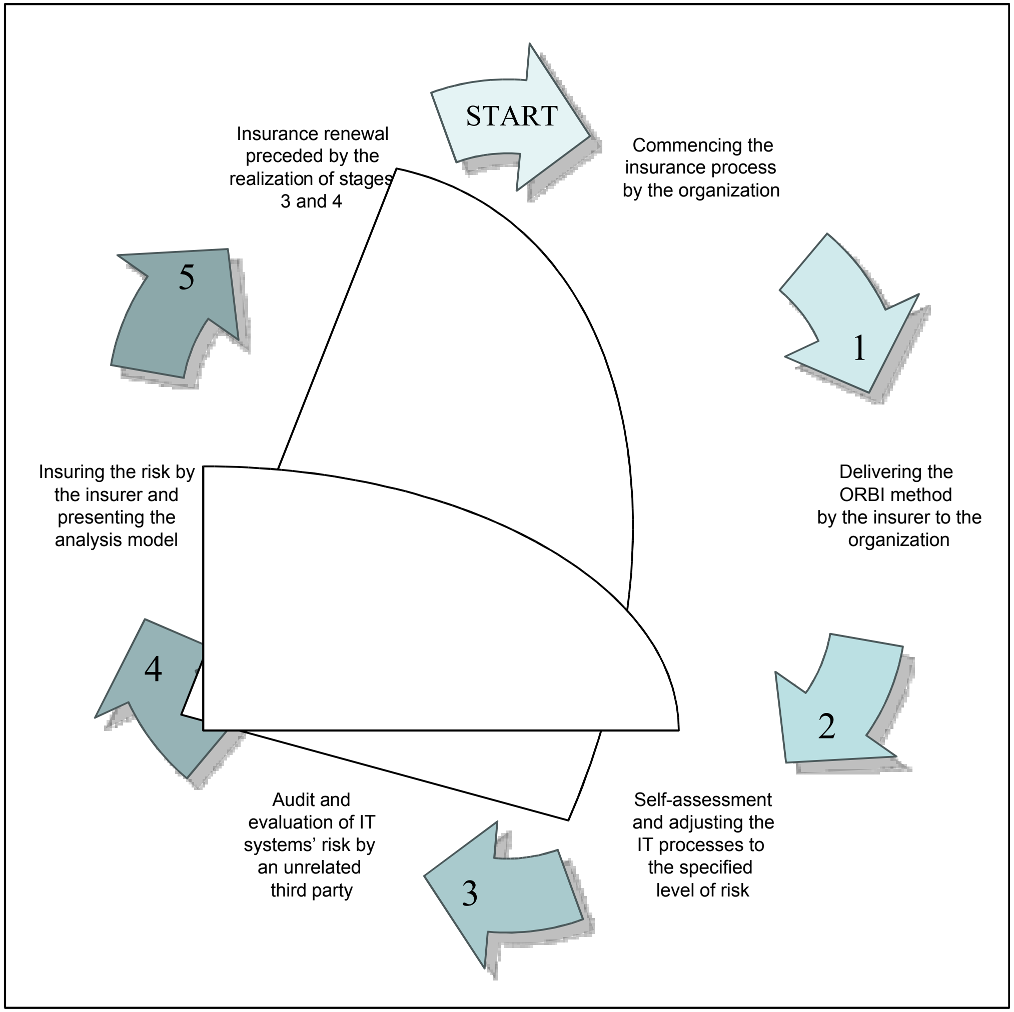


ORBI – IT Security Risk Assessment Methodology

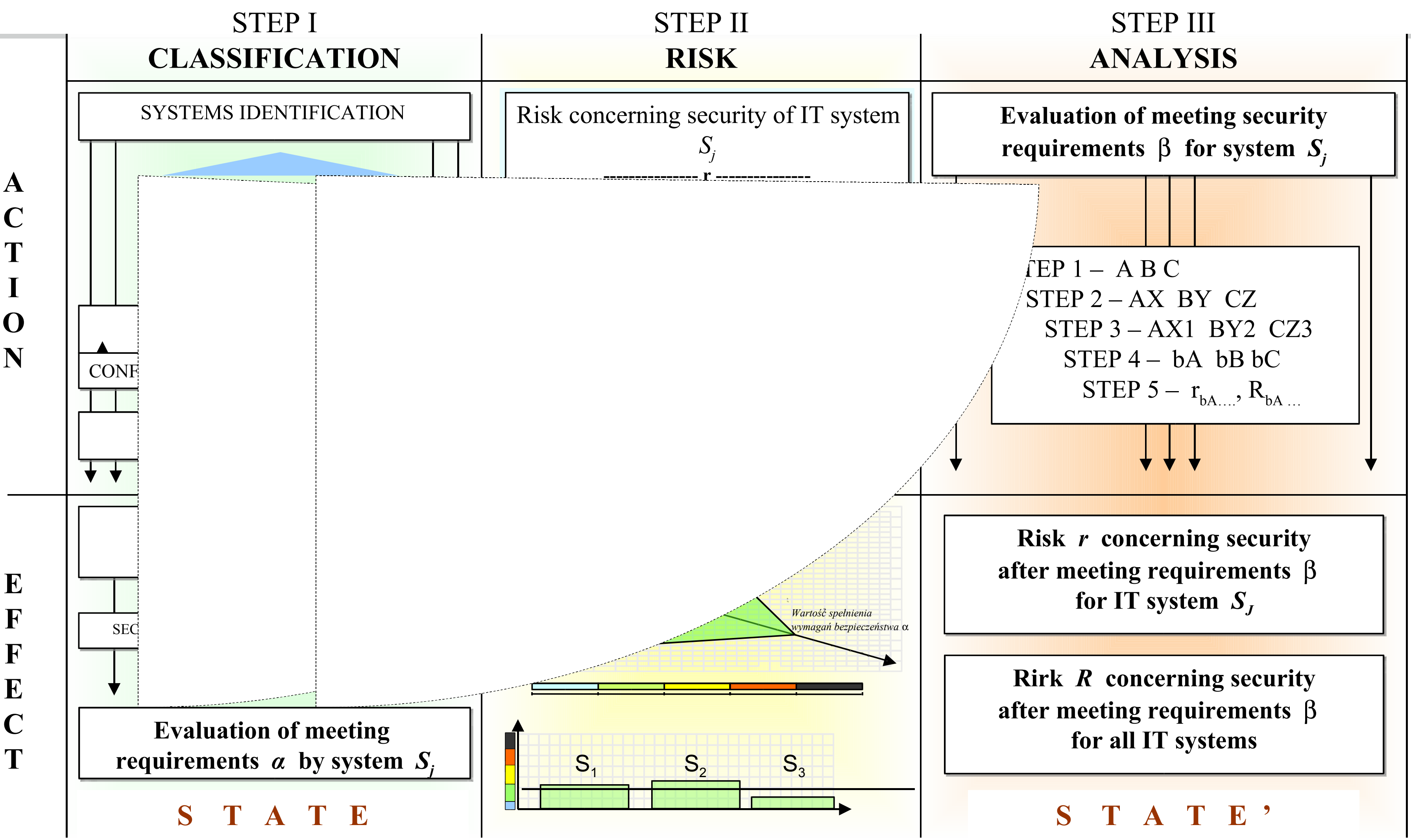
Author: Aleksander Poniewierski

ORBI – Goals and Actions

- Evaluate risk related to IT system security
- Provide credible information for the system's insurance
- Provide an evaluation and management tool for handling risk related to organization's IT system security



ORBI – Methodology



ORBI – Elements (1/2)

- **Evaluation of meeting the security requirements α**

$$\alpha = \frac{S}{T} * 100\% \quad \rightarrow \quad \beta = \frac{S'}{T'} * 100\%$$

$$S = \sum_i b_i * a_i * w_i \qquad S' = \sum_i b_i * a_i * w'_i$$

$$T = \sum_i b_i * a_i \qquad T' = \sum_i b_i * a_i$$

- a_i – value of requirement's adequacy
- b_i – value of priority of requirement for a certain security class
- w_i – value of meeting a requirement
- w'_i – value of meeting a requirement after introducing change to the system

- **IT system security risk r_j**

$$r_j = \frac{f(K) * f(J) * f(\alpha)}{6} \quad \rightarrow \quad r'_j = \frac{f(K) * f(J) * f(\beta)}{6}$$

$$f(\alpha) = 10\left(1 - \frac{\alpha}{100\%}\right) \qquad f(\beta) = 10\left(1 - \frac{\beta}{100\%}\right)$$

$$f(J) = \begin{cases} 1, & \text{when } J = 5 \\ 2, & \text{when } J = 4 \\ 3, & \text{when } J = 3 \\ 4, & \text{when } J = 2 \\ 5, & \text{when } J = 1 \end{cases} \qquad f(K) = \begin{cases} 1, & \text{when } K = D4 \\ 2, & \text{when } K = D3 \\ \ldots & \\ 15, & \text{when } K = A2 \\ 16, & \text{when } K = A1 \end{cases}$$

$K = M \times P$

$M = \{A,B,C,D\}$ – availability class

$P = \{1,2,3,4\}$ – confidentiality class

ORBI – Elements (2/2)

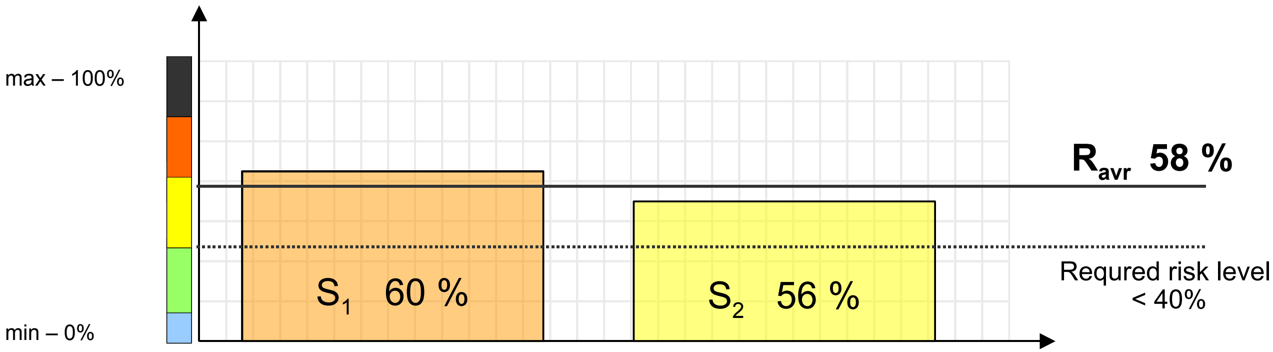
- **Relative value of risk concerning security of IT system**

$$R_j = \frac{r_j}{r_{\max}} * 100\% \qquad r_{\max} = \max(r_1, r_2, \ldots, r_J)$$

- **Average risk related to security of all IT systems $\Re$**

$$\Re = \frac{\sum_{j=1}^{J} r_j}{J}$$

J – number of IT systems in the organization



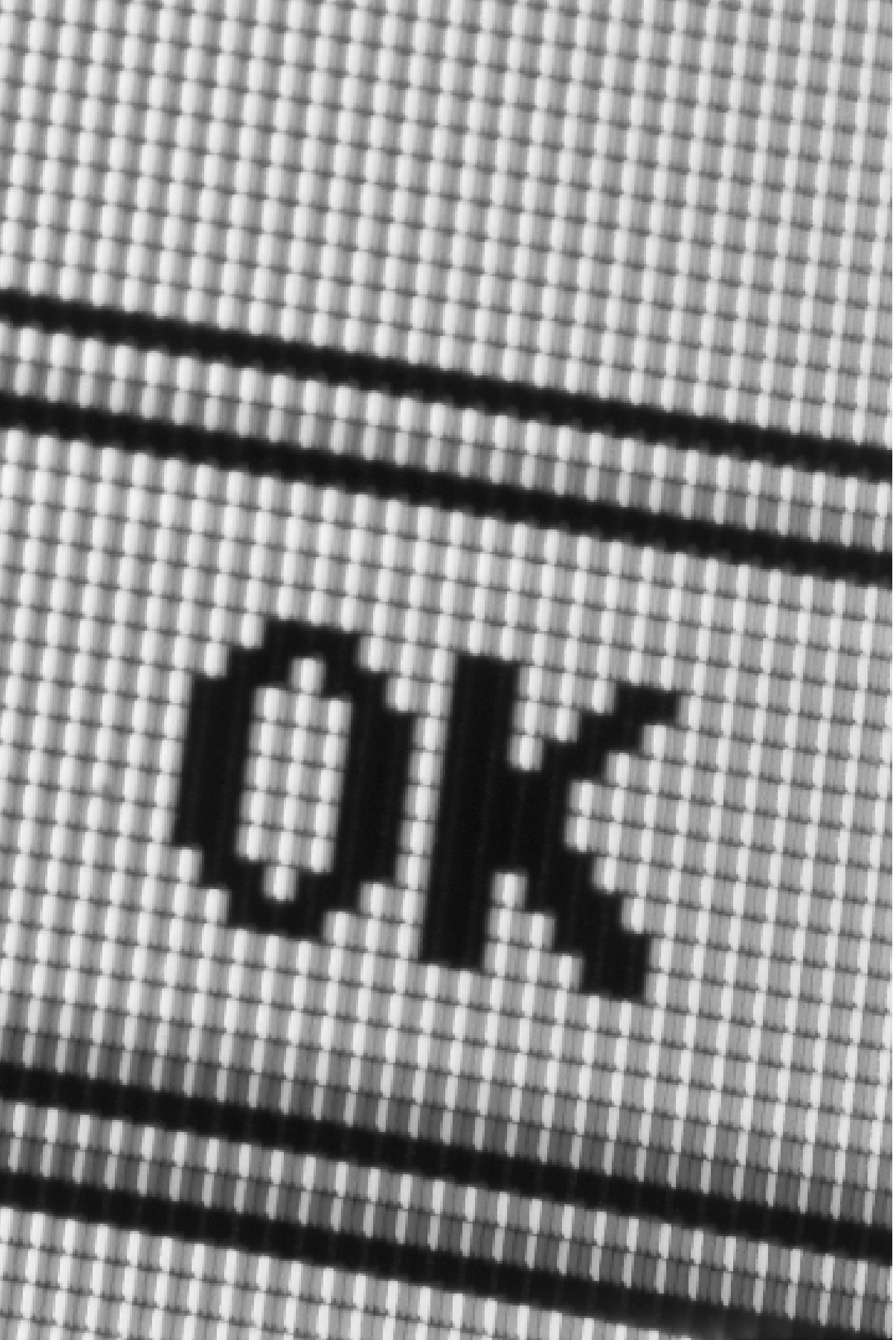
(e.g. insurance of IT systems is possible when $\Re < 40\%$)

ORBI – Application in Insurance

- Calculating insurance premiums for:
  - individual IT systems
  - all IT systems in the same security class
  - all IT systems in the same group of significance

- Calculating insurance premiums in case when the organization meets all security requirements concerning IT systems

- Creating knowledge base on the level of risk for the whole population of insured subjects, which in turn enables precise modeling of security requirements priority values



Summary

Summary

- Sudden growth of reliance of the modern economy on IT technologies implies a necessity of introducing dedicated IT risk assessment and management methodologies
- The methodologies must meet ever-increasing accuracy and effectiveness requirements
- Both MIR-2M and ORBI methodologies stress the importance of a fixed group of factors which play a substantial role in IT risk assessment
- Each of the factors is calculated in possibly precise way which ensures sufficient credibility of the overall IT risk analysis
- Accuracy of the determined IT risk level depends on the amount of time and other resources spent on IT risk analysis as well as appropriate selection of methodology

Contact Information

- Aleksander Poniewierski, Partner

  CISM, CISA, PMP, ISSPCS, CFE, CERT® CCSIH

  aleksander.poniewierski@pl.ey.com

  (+48 22) 557 63 48

- Mirosław Ryba, Senior

  CISA, CIA, ISSPCS, CFE, CERT® CCSIH

  miroslaw.ryba@pl.ey.com

  (+48 22) 557 63 43