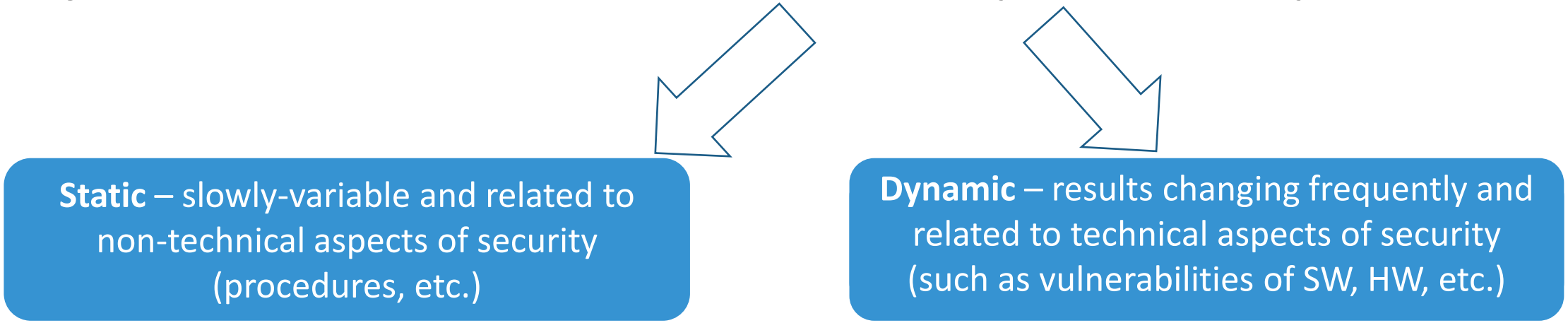
CYBERSECURITY RISK MANAGEMENT SUBSYSTEM ON THE BASIS OF THE NCP NATIONAL CYBERSECURITY PLATFORM

MAREK JANISZEWSKI, ANNA FELKNER, PIOTR LEWANDOWSKI
RESEARCH AND ACADEMIC COMPUTER NETWORK (POLAND)

Aims

- Building situational awareness on the basis of static and dynamic risk analysis



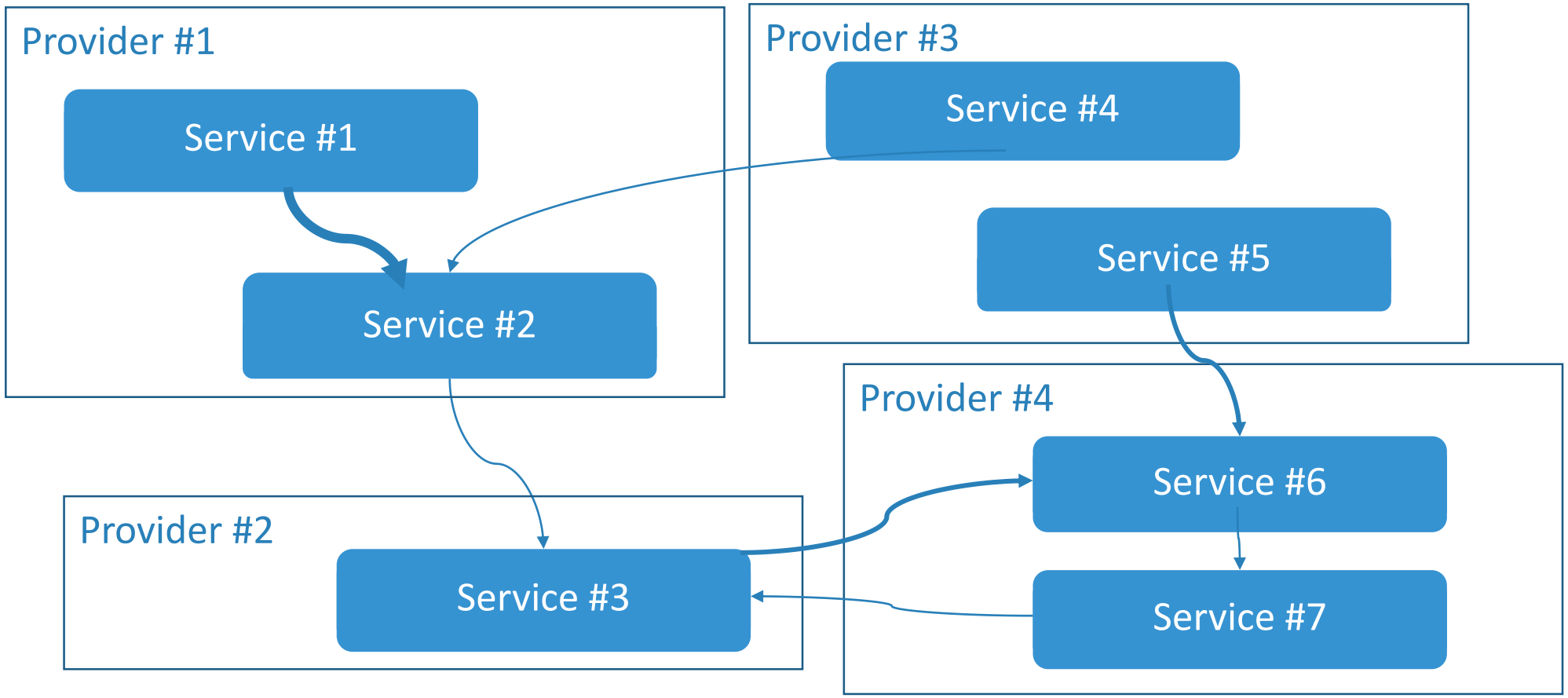
- The risk is calculated at various levels (services, groups of services, sectors, national cyberspace)
- The results can be used as an input to strategic decisions (such as setting the alert level) and to indicate sectors or even specific institutions, services or types of service that require special attention

Approach and assumptions

- Quantitative and unified methodology to risk analysis
- The risk evaluation with regard to mutual relationships between the services
- Taking into account the technology (software, hardware) used by service providers and their specificity
- No central entity which aggregates crucial and detailed information (e.g. about internal IT infrastructure of each service provider)
- The risk assessment is based on various types and sources of actionable information

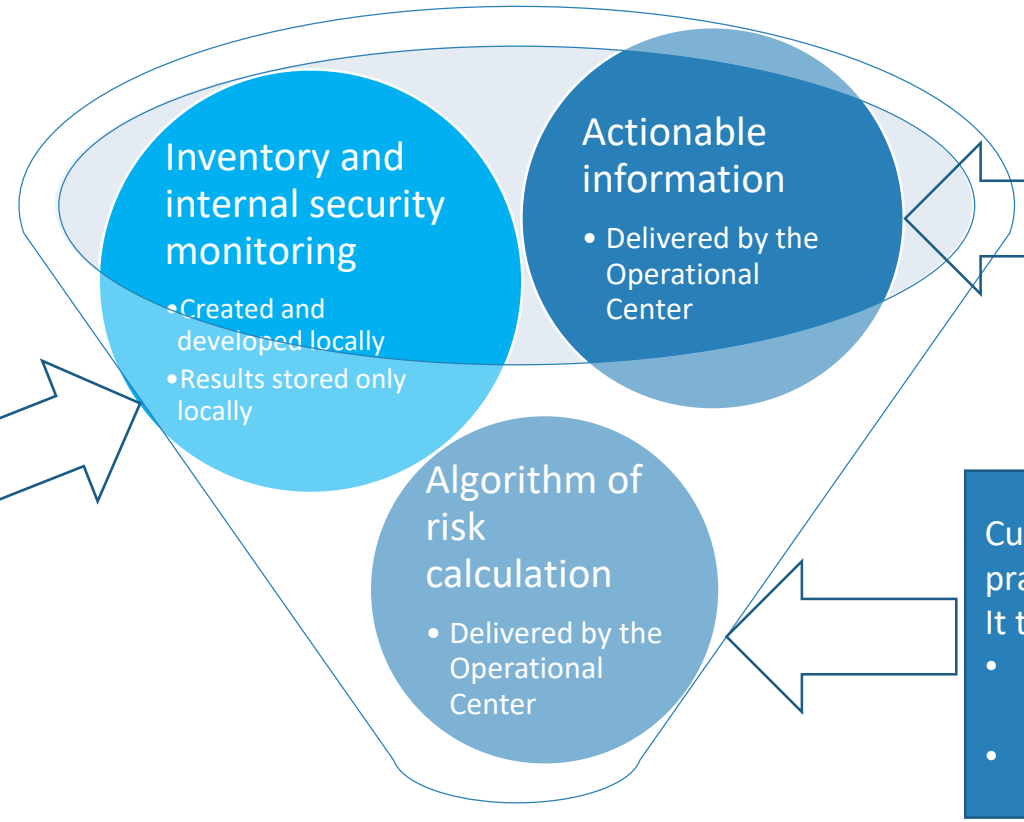
The model of services

Map of services (illustrating the links between services)



Each link is characterized by critacality - C_i^j in the context of information security attributes (CIA)

Risk analysis
performed by the Client



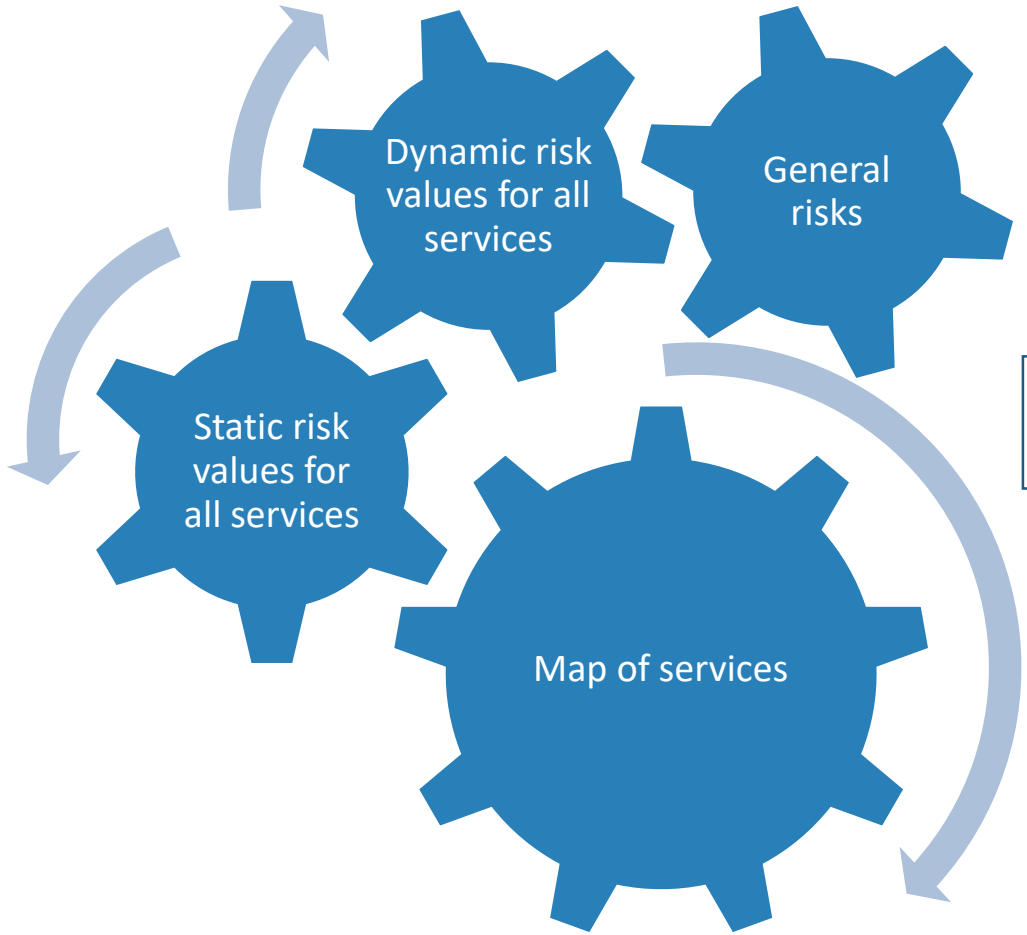
Supported by:
- Administrator's knowledge
- GRC systems
- CMDB
- ITAM systems
- Scanners
- SIEM systems
- IPS/IDS systems
- …

Types of information:
- well-known vulnerabilities
- Indicators of Compromise (IoC)
- Cyber Threats Intelligence (CTI) reports
- …

Currently one algorithm, but in practice it can be easily changed
It takes into consideration e.g.:
- Impact of vulnerabilities (as CVSS value)
- Severity of incidents

Set of values of the dynamic risk for the service U_i: $[R^1_{U_i}, \ldots, R^l_{U_i}]$;
$R^1_{U_i}, \ldots, R^l_{U_i} \in [0,10]$

Risk analysis
performed by the Operational Center



results

- External risk values for all services
- Overall risk values for all services
- Overall risk values for sectors or groups of services
- Overall risk value for the cyberspace

Responsibilities and tasks

Client

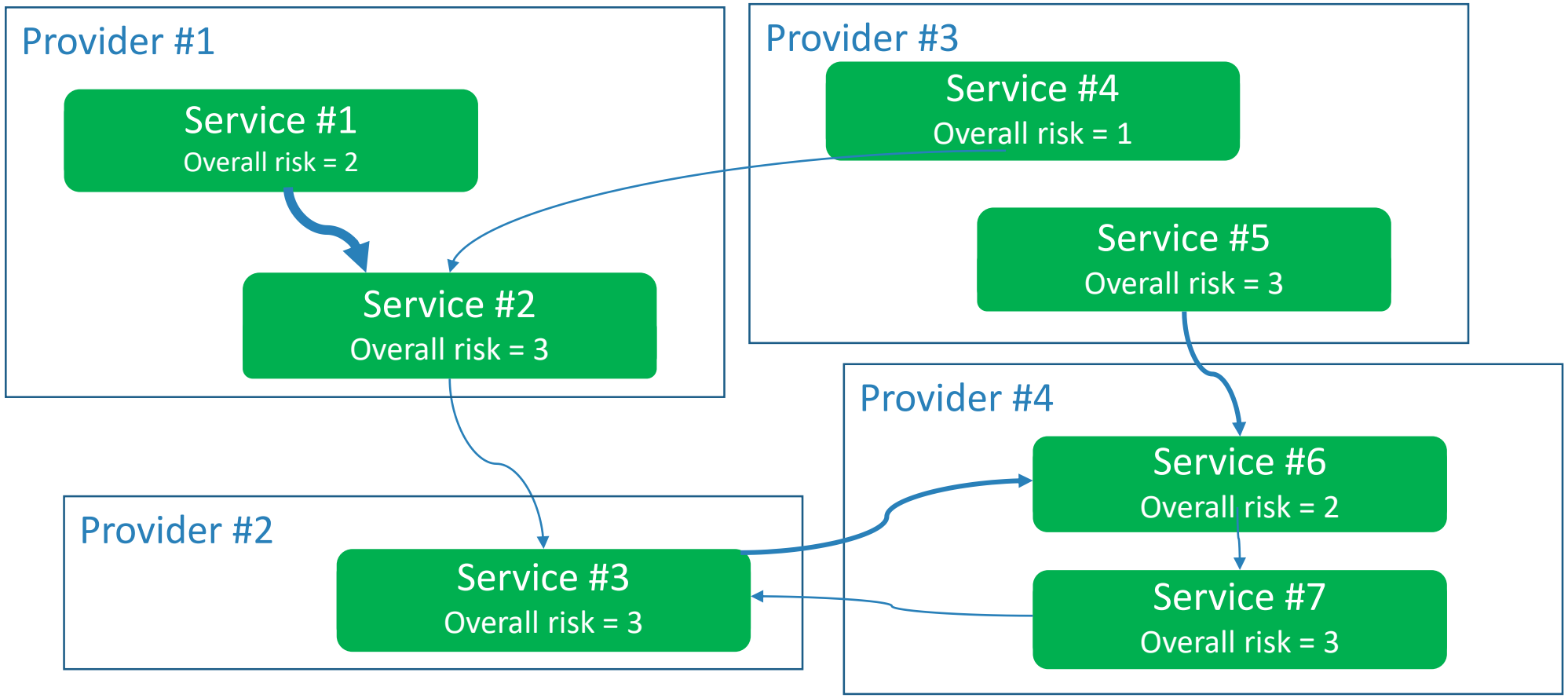
- Reports security incidents
- Indicates the relationships with other services/providers
- Performs dynamic risk analysis in compliance with the algorithm provided by the Operational Center
  - The accuracy depends on the maturity of the client

Operational Center

- Aggregates and analyses reported security incidents
- Maintains the Map of relationships
- Provides actionable information
- Calculates overall risks
- Generates alerts and recommendations on the basis of risk evaluation
- Performs simulations
  - „WHAT IF" – how „a change" impacts the security of the related services, providers, sectors, and the cyberspace

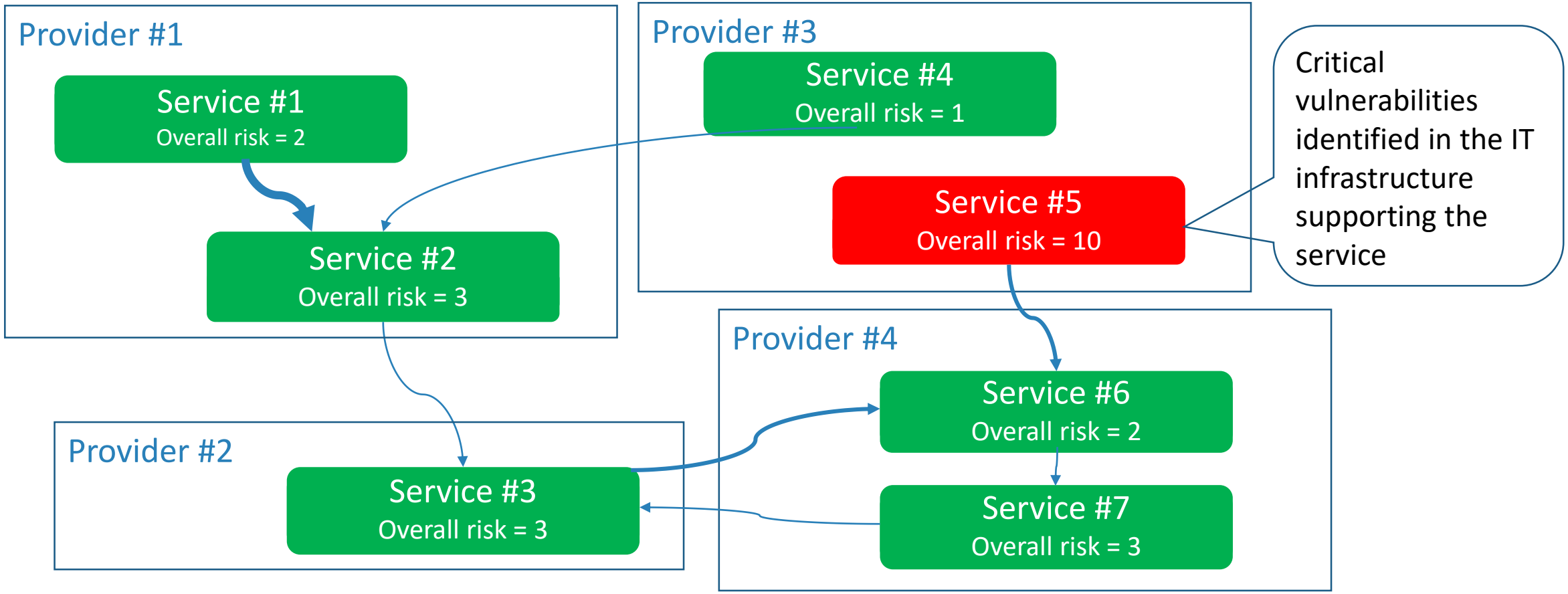
The model of services

Risk propagation



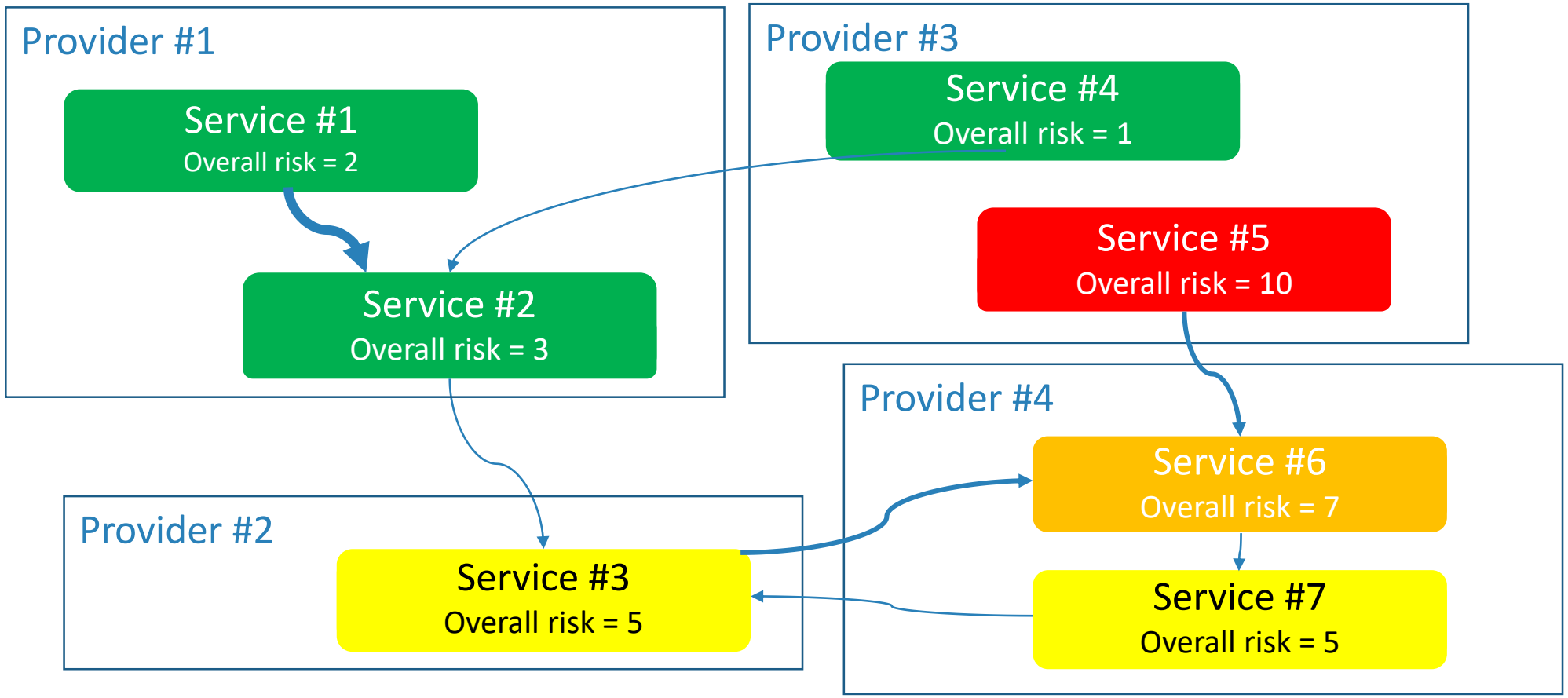
The model of services

Risk propagation



The model of services

Risk propagation



Summary

- An approach to the national-level cyber risk assessment
- Quantitative results
- Many additional information can be included in the risk assessment

- **The approach needs practical verification and validation in operational environment**

NCP NATIONAL CYBERSECURITY PLATFORM

NASK

Warsaw University of Technology

NATIONAL CENTRE FOR NUCLEAR RESEARCH ŚWIERK

INSTYTUT ŁĄCZNOŚCI PAŃSTWOWY INSTYTUT BADAWCZY

The National Centre for Research and Development

CYBERSECIDENT/369195/I/NCBR/2017