Risk Management and Assessment

Chris Hankin

Types of Risk

- Financial
- Equipment failure
- Safety

- Information security

Risk Management Process

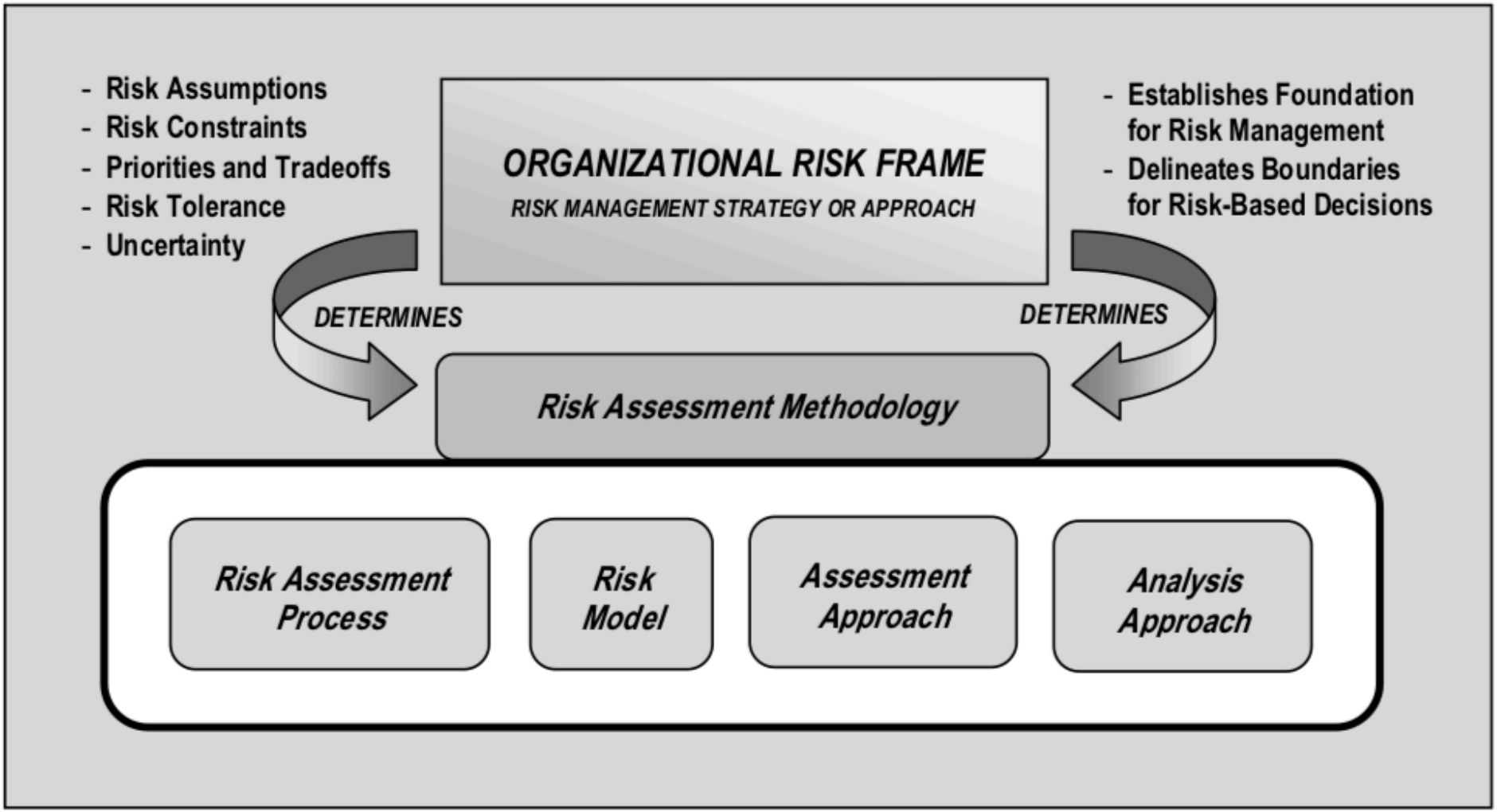
- Frame – framework for risk decisions; risk tolerance; safety and security; availability; and physical operating environment.
- Assess – identify threats and vulnerabilities; harm and likelihood; effect on physical process, dependent systems, and physical environment; and safety.
- Respond – to identification of risk (acceptance, avoidance, mitigation, sharing, transfer).
- Monitor – implementation; changes in environment; effectiveness and efficiency.

Framing Risk

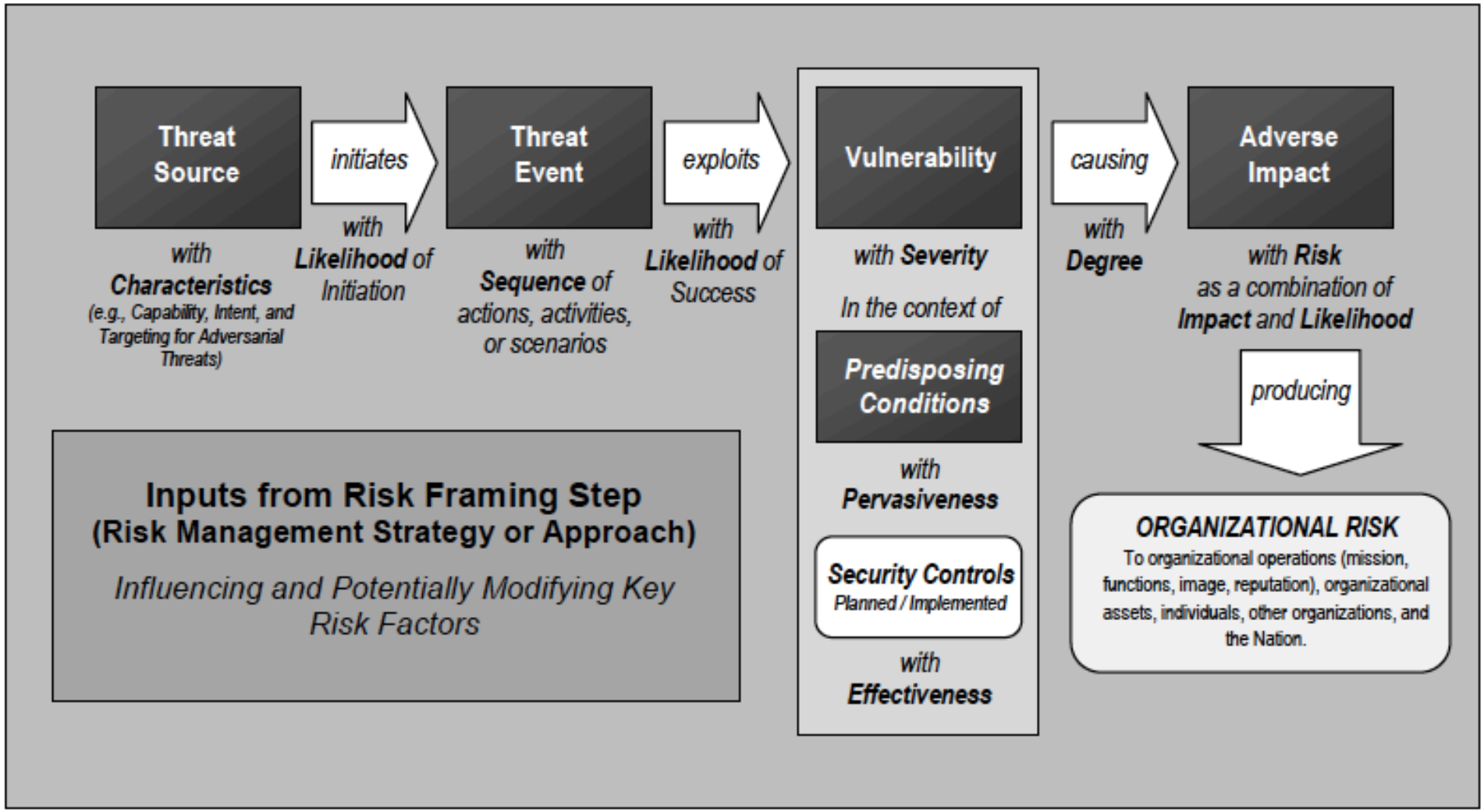
- Risk assumptions – threat, vulnerabilities, impact and likelihood
- Risk constraints
- Risk tolerance
- Priorities and trade-offs

Risk Assessment

- Tools, techniques and methodologies
- Roles and responsibilities
- Collection, processing and communication of risk assessment information
- Conduct of risk assessment
- Frequency
- Obtaining threat intelligence



From: NIST sp 800-30(r1) – Guide for conducting risk assessments



From: NIST sp 800-30(r1) – Guide for conducting risk assessments

Responding

- Alternative courses of action
- Evaluation of alternative courses
- Courses of action consistent with risk tolerance
- Implementation

- Accept; Avoid; Mitigate; Share; Transfer

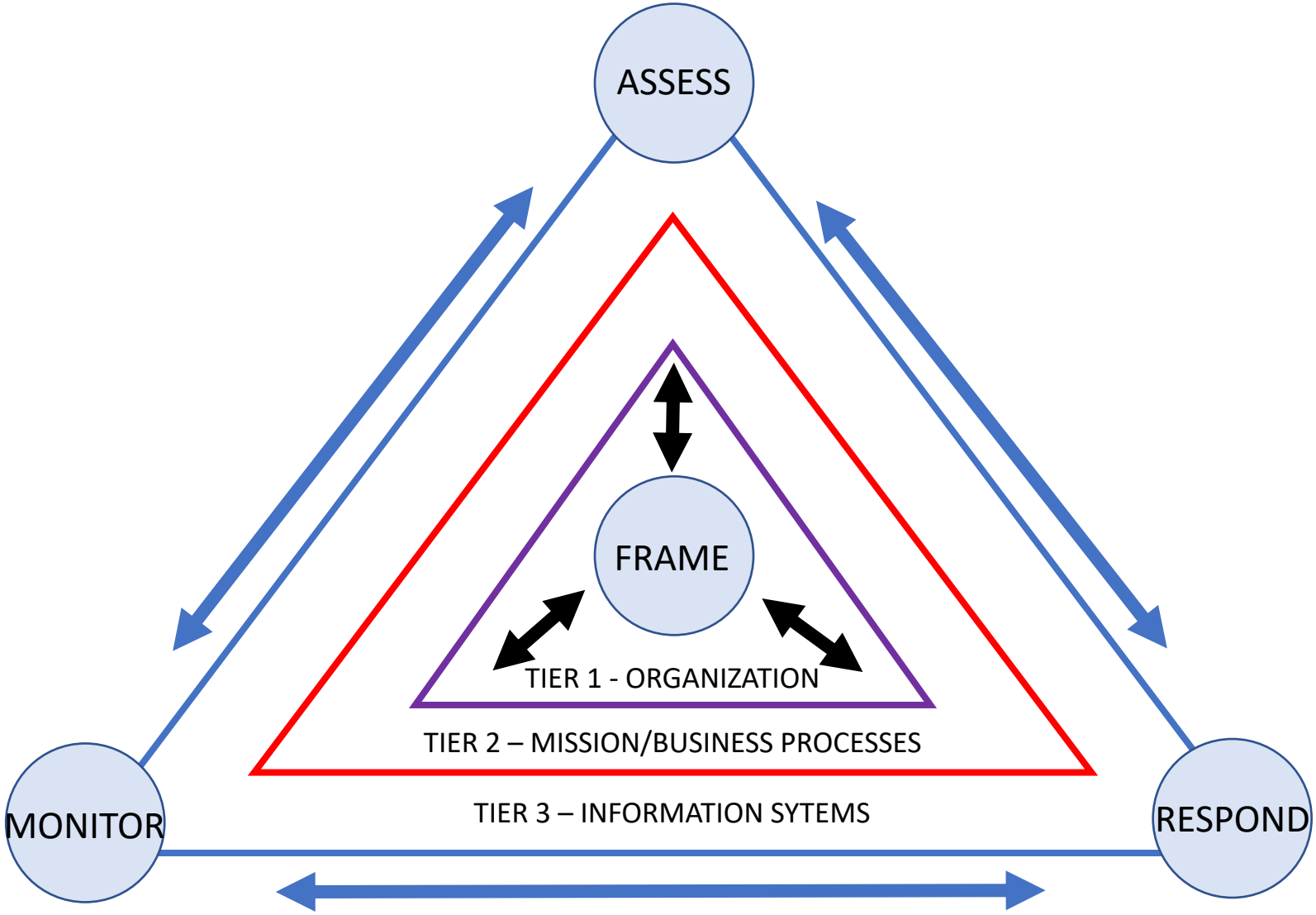
Monitoring

- Verification that planned risk response is implemented and compliant with any legal requirements
- Determining on-going effectiveness
- Identify risk-impacting changes to organizational information systems.

Three Tiers

- Organization
- Mission/Business Process
- Information System (IT and ICS)

Risk Management Process



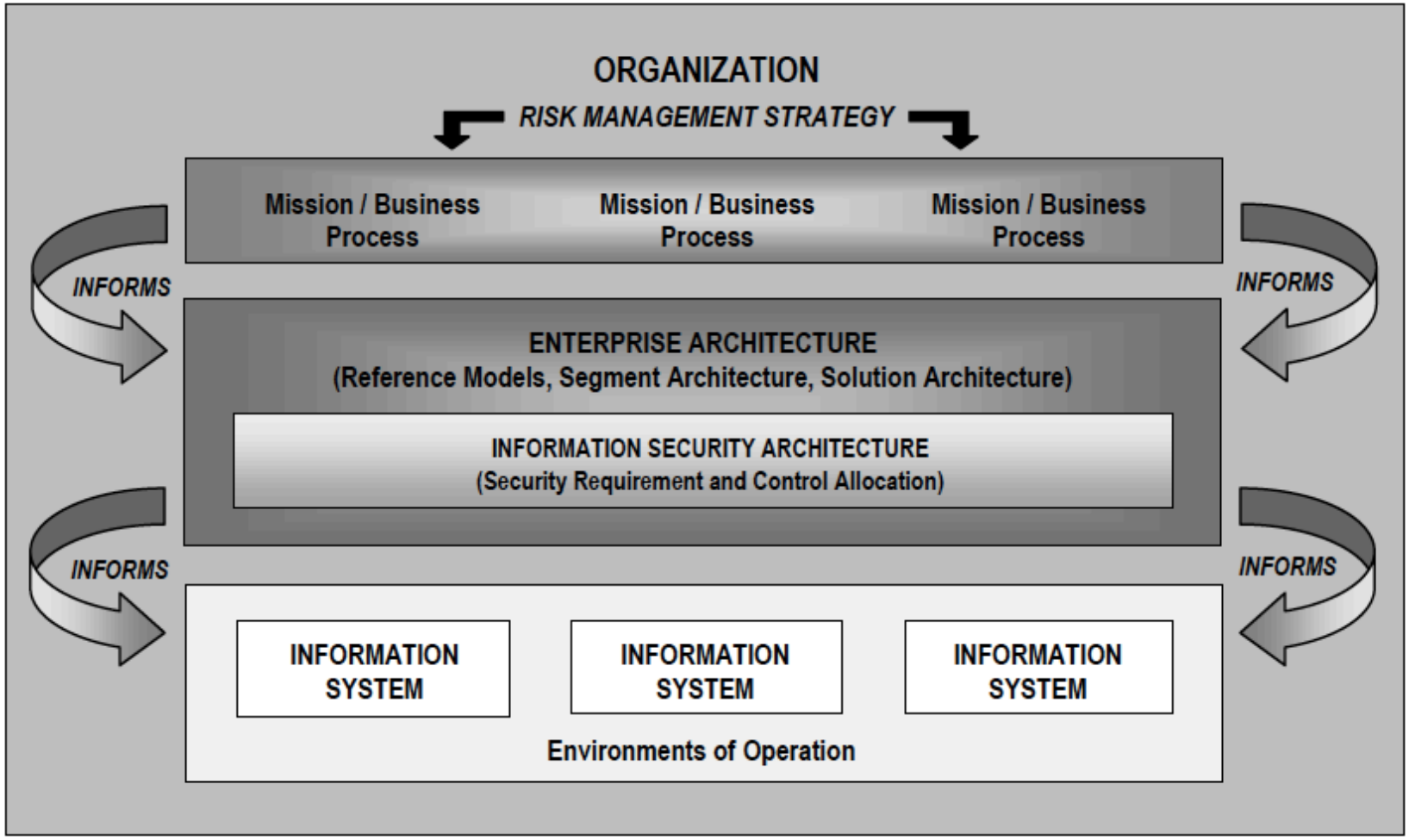
Organization

- Governance – strategic alignment; execution of risk management processes; effective and efficient allocation of resources; performance-based outcomes; and delivered value by optimized risk management investments.
- Risk Executive – individual or group
- Risk Management Strategy
- Investment strategy

Mission/Business Process

- Risk-aware mission/business processes
- Enterprise architecture – segmentation, redundancy and elimination of single points of failure
- Information Security Architecture – people, processes and technology

Mission/Business Process



From: NIST sp 800-39 – Managing Information Security Risk

Information Systems

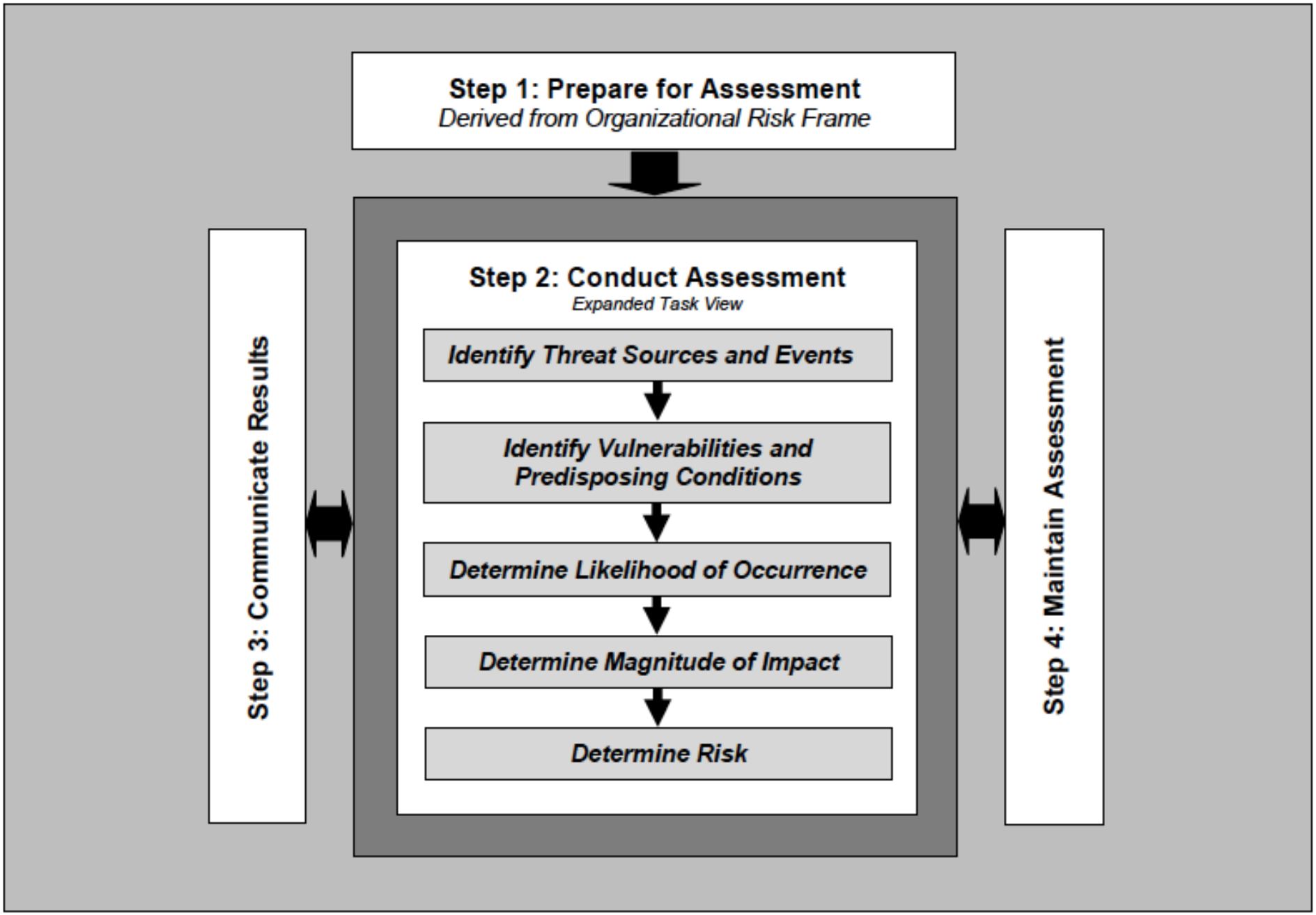
- Initiation - requirements
- Development/acquisition
- Implementation
- Operation/maintenance
- Disposal

Trust and Trustworthiness

- Trust: the belief that an entity will behave in a predictable manner in specified circumstances.
- Trustworthiness is an attribute of an entity.
- Trustworthiness of Information Systems:
  - Security functionality
  - Security Assurance

Organizational Culture

- Values, beliefs and norms
- Willingness to adopt new and leading edge technologies
- Inter-organization culture dis-connect can be the cause of problems.



From: NIST sp 800-30(r1) – Guide for conducting risk assessments

TABLE D-3: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY CAPABILITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

TABLE D-4: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY INTENT

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
High	80-95	8	The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks.
Moderate	21-79	5	The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organization's cyber resources by establishing a foothold in the organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the organization's missions/business functions to achieve these ends.
Low	5-20	2	The adversary actively seeks to obtain critical or sensitive information or to usurp/disrupt the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.
Very Low	0-4	0	The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.

TABLE D-5: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY TARGETING

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
High	80-95	8	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
Moderate	21-79	5	The adversary analyzes publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.
Low	5-20	2	The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class.
Very Low	0-4	0	The adversary may or may not target any specific organizations or classes of organizations.

TABLE E-4: RELEVANCE OF THREAT EVENTS

Value	Description
Confirmed	The threat event or TTP has been seen by the organization.
Expected	The threat event or TTP has been seen by the organization's peers or partners.
Anticipated	The threat event or TTP has been reported by a trusted source.
Predicted	The threat event or TTP has been predicted by a trusted source.
Possible	The threat event or TTP has been described by a somewhat credible source.
N/A	The threat event or TTP is not currently applicable. For example, a threat event or TTP could assume specific technologies, architectures, or processes that are not present in the organization, mission/business process, EA segment, or information system; or predisposing conditions that are not present (e.g., location in a flood plain). Alternately, if the organization is using detailed or specific threat information, a threat event or TTP could be deemed inapplicable because information indicates that no adversary is expected to initiate the threat event or use the TTP.

TTP = Tactics, techniques and procedures

TABLE F-2: ASSESSMENT SCALE – VULNERABILITY SEVERITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	0-4	0	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

TABLE F-5: ASSESSMENT SCALE – PERVASIVENESS OF PREDISPOSING CONDITIONS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Applies to **all** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
High	80-95	8	Applies to **most** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Moderate	21-79	5	Applies to **many** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Low	5-20	2	Applies to **some** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Very Low	0-4	0	Applies to **few** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).

TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

TABLE G-3: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT OCCURRENCE (NON-ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	**Level of Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Worked Example (Hacking Exposed)

- **Potential Threat Source(s)** Nation-state; insider; malware
- **Attack** Stack-based buffer overflow
- **Threat Vector** Web interface; local network
- **Vulnerability** CVE-2016-0868
- **Target** Allen-Bradley MicroLogix 1100

Worked Example (Hacking Exposed)

- **Potential Threat Source(s)** Nation-state; insider; malware
- **Attack** Stack-based buffer overflow
- **Threat Vector** Web interface; local network
- **Vulnerability** CVE-2016-0868
- **Target** Allen-Bradley MicroLogix 1100
- **Abuse case/objective** Execute code; gain control; modify configuration
- **Potential consequences** Loss of control/vision; data corruption; damage

Worked Example (Hacking Exposed) – connected device

- **Potential Threat Source(s)** Nation-state; insider; malware
- **Attack** Memory corruption via kernel-mode driver
- **Threat Vector** Malicious file opened in a web browser
- **Vulnerability** CVE-2016-0005 (0008, 0009)
- **Target** Workstation running Windows 7 SP1 and IE
- **Abuse case/objective** Execute code; gain control; pivot
- **Potential consequences** damage; pivoting

Worked Example (Hacking Exposed) - correlated

- **Potential Threat Source(s)** Nation-state; insider; malware
- **Attack** Stack-based buffer overflow
- **Threat Vector** Web interface; local network; engineering workstation
- **Vulnerability** CVE-2016-0868
- **Target** Allen-Bradley MicroLogix 1100
- **Abuse case/objective** Execute code; gain control; modify configuration
- **Potential consequences** Loss of control/vision; data corruption; damage

Worked Example (Hacking Exposed)

- Risk = F(Severity, Criticality, Likelihood, Impact)
- $F(s,c,l,i) = (s + 2c + 2l + 2i)/4$
- Even weighting
- Vulnerability severity: 9.8
- Asset criticality: 3.0
- Attack Likelihood: 2.5
- Impact: 3.0
- Risk: 6.7

Response

- Analyse different courses of action
- Conduct cost-benefit analyses
- Address scalability issues for large scale implementations
- Examine interactions/dependencies amongst risk mitigation approaches
- Assess any other factors

ICS Risk Assessment

- Impacts on safety and the use of safety assessments.
- Physical impact of a cyber incident on an ICS.
- The consequence of risk assessments of non-digital control components.

Safety

- UK HSE Guidance to Safety Inspectors – Major Accidents and Loss of Essential Services
- Protect, Detect and Respond
- Defence in Depth
  - Organizational counter-measures
  - Protective counter-measures
  - Detect and Respond counter-measures
- Inspectors assessing:
  - Adequacy of a cyber security management system
  - Adequacy of cyber security counter-measures

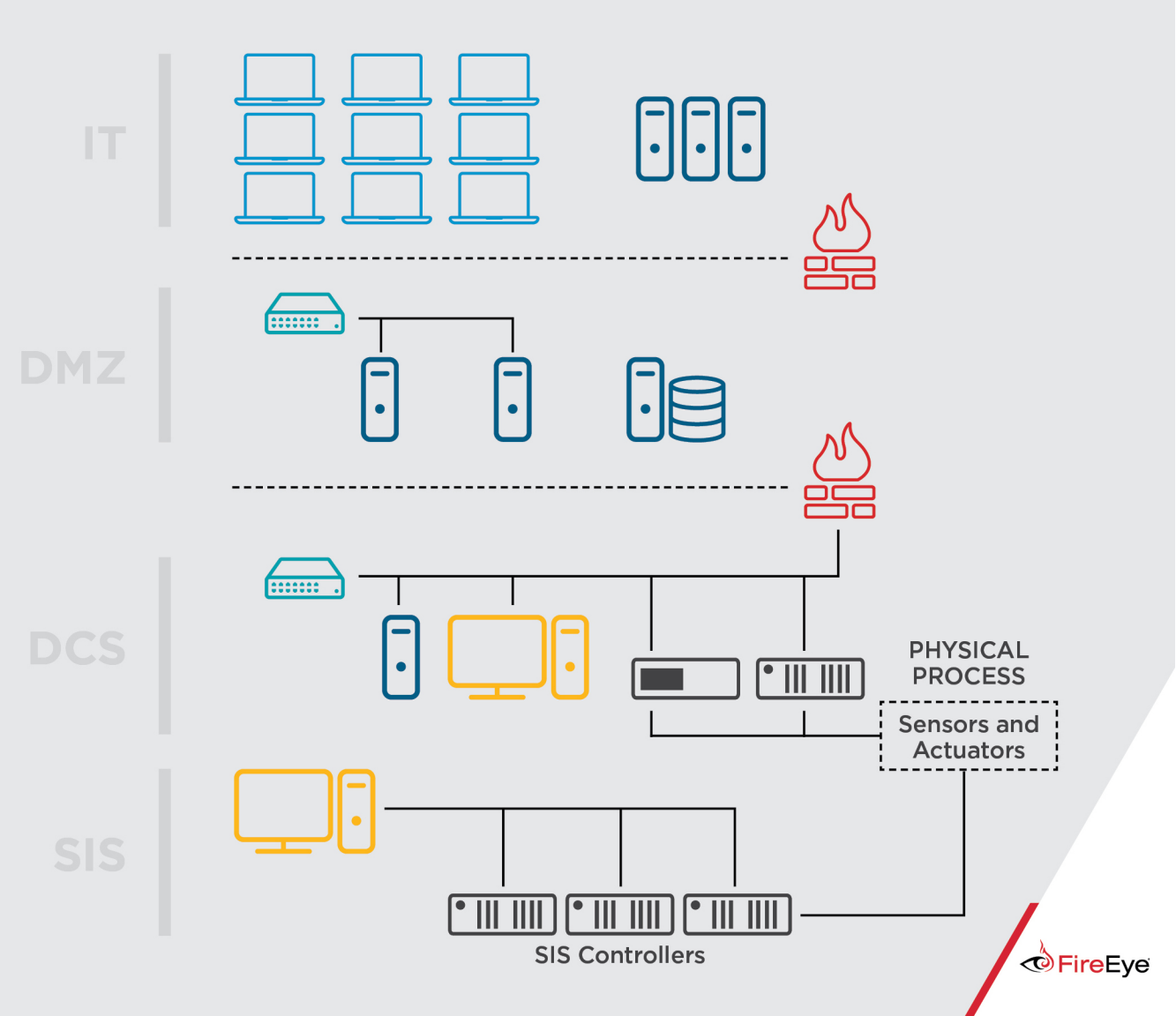
Physical Impacts

- How manipulation of sensors and actuators could create an impact
- What redundant controls exist to prevent an impact
- How a physical impact could emerge based on these conditions: for example, release of hazardous materials, explosions, …
- Focus on human safety, damage to the environment and damage to other critical infrastructures
- Cascading failure and short- or long-term outages

Non-digital Components

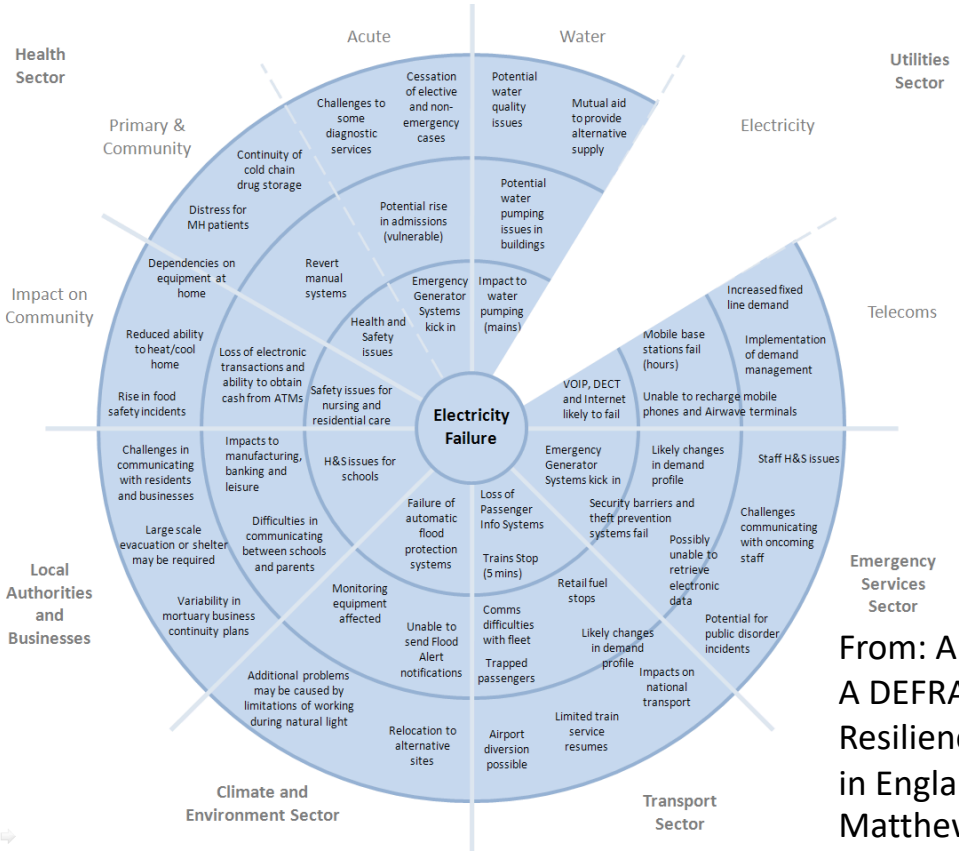
- Analog displays and alarms
- Manual control mechanisms
- Analog control systems

Safety Systems



Connected Systems

- Physical or Logical Dependencies



From: Anytown: Final Report
A DEFRA funded project - Community Resilience Funding for Local Resilience Forums in England
Matthew Hogan, London Resilience Team