أرامكو السعودية
saudi aramco

ICS Cybersecurity Threat Modeling

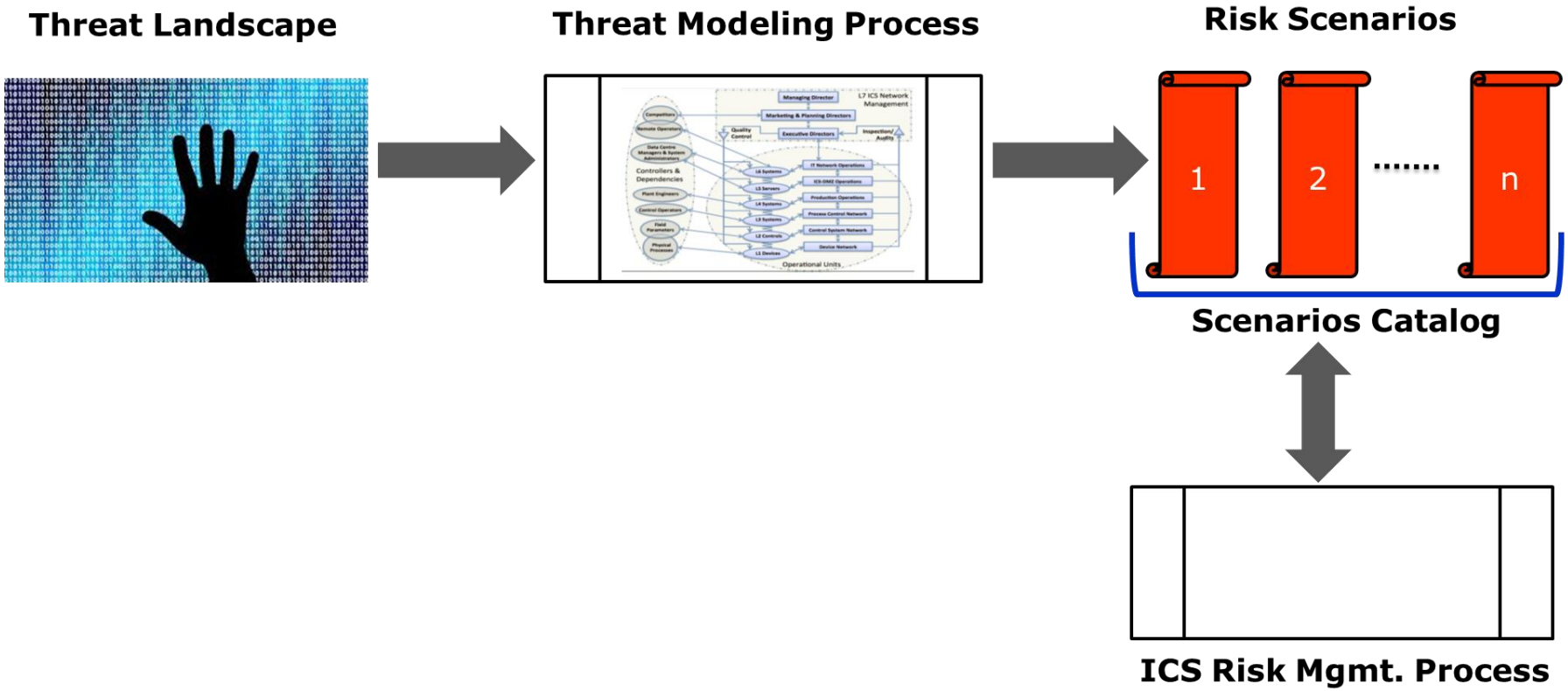
Salem S. Elwi

where energy is opportunity™

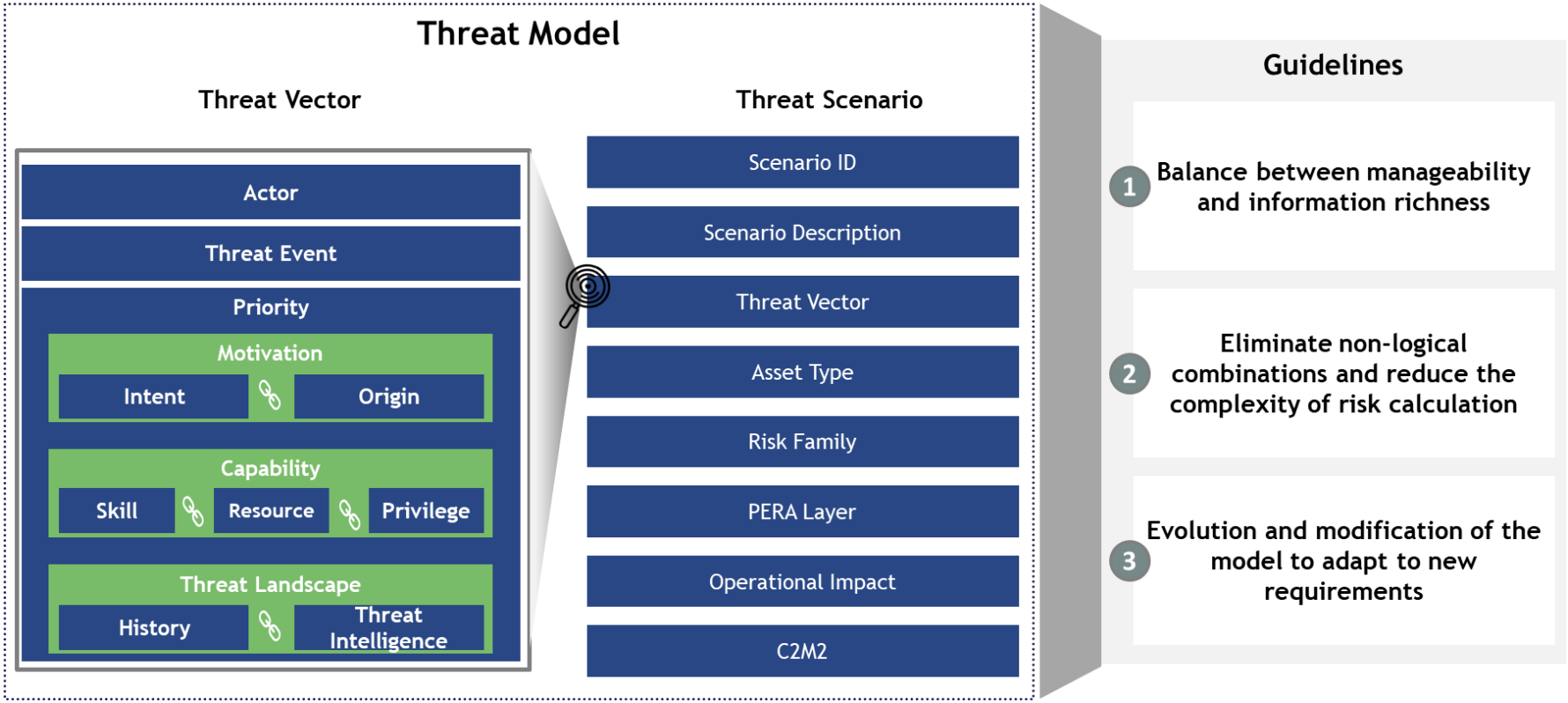
Key Points

1. Threat Modeling and Risk Management
2. Value Realization
3. Future Value Maximization

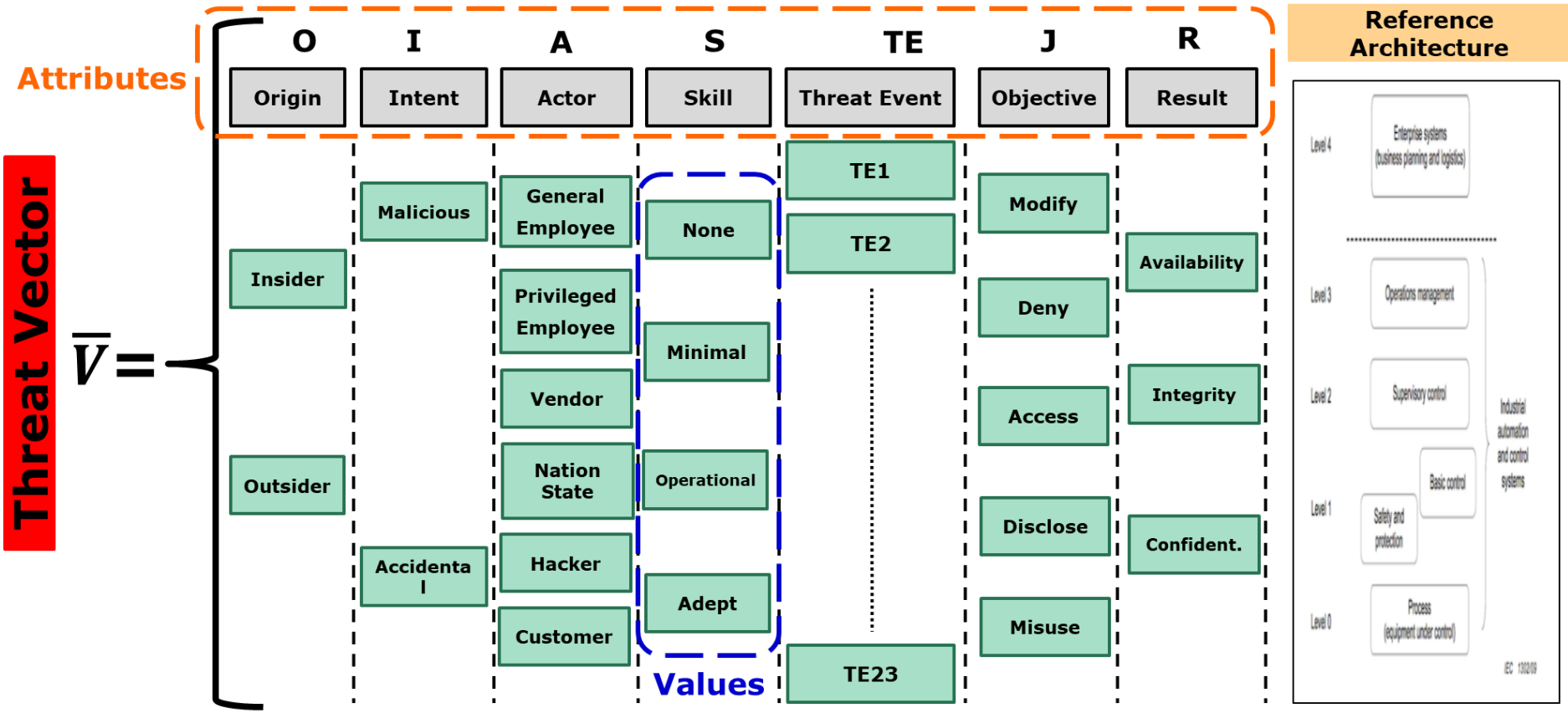
Risk Management Framework



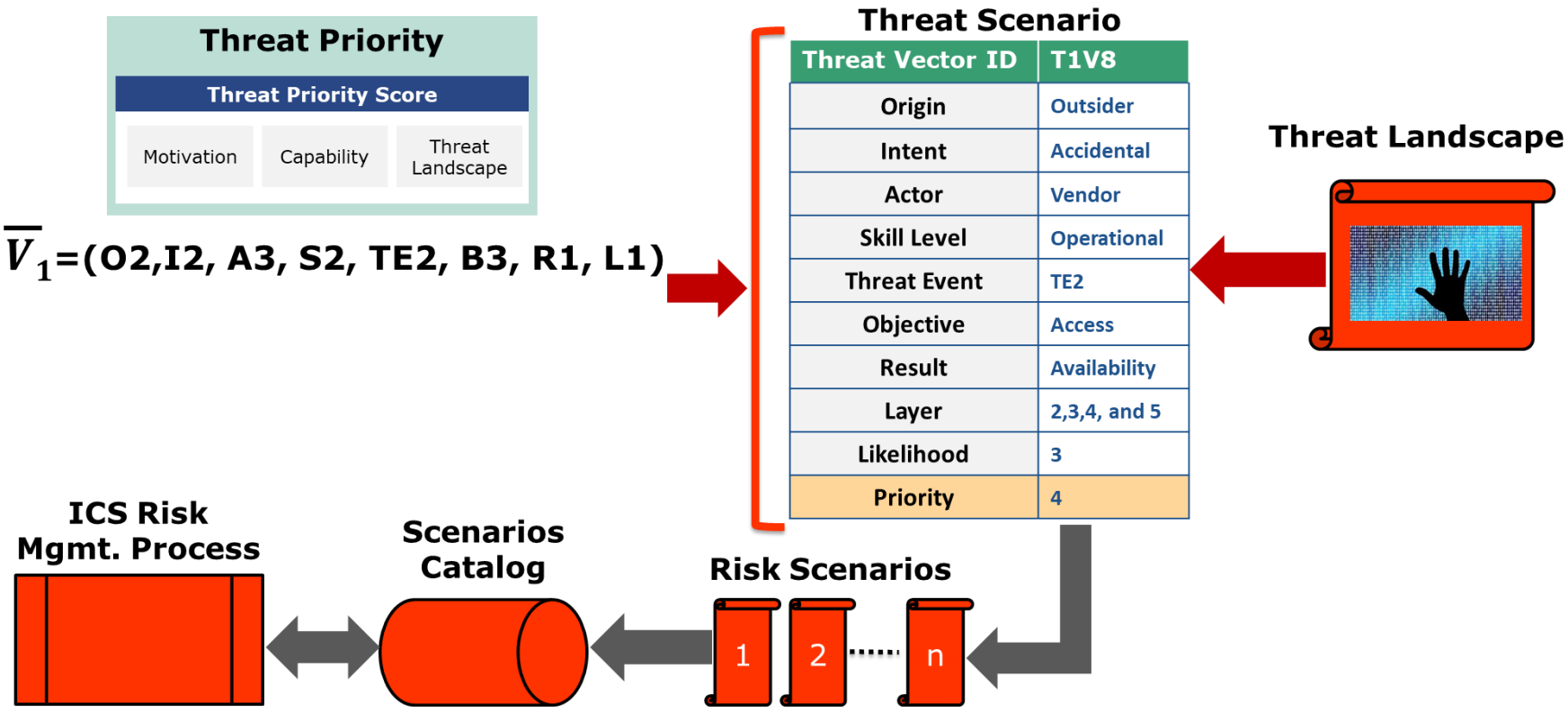
ICS Cybersecurity Threat Model



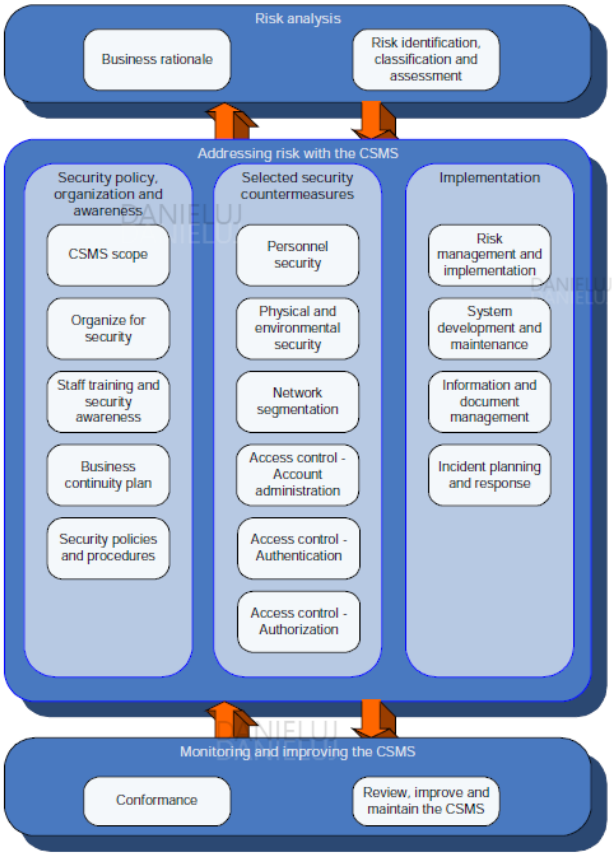
ICS Threat Modeling Elements



ICS Threat Vectors Driven Risk Assessment

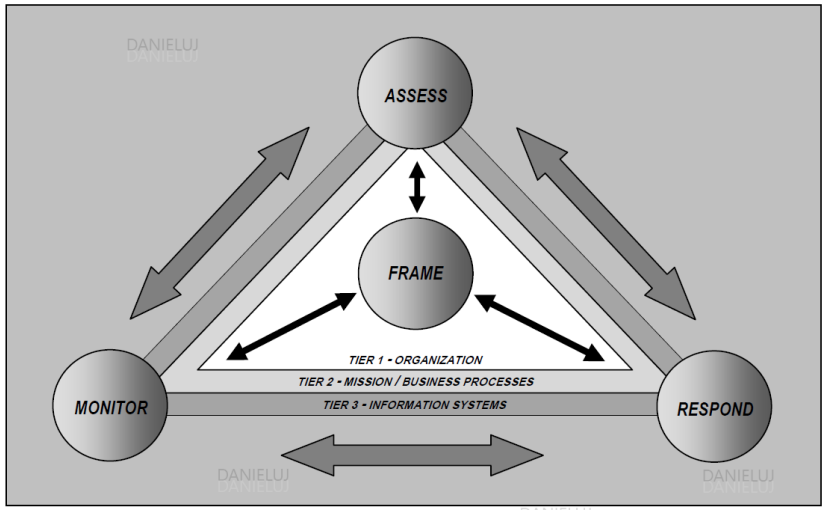


ICS Cyber Risk Assessment Process



Graphical view of elements of a cyber security management system

IEC 62443-2-1:2010(E) Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security Program, IEC, 2010.



Risk Management Process Applied Across the Tiers

NIST SP 800-39 Managing Information Security Risk, NIST, March 2019, [https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf].

Risk Calculation – High Level Approach

Threat Priority

Threat Priority Score

Motivation	Capability	Threat Landscape

Control Effectiveness

Control Effectiveness for likelihood Score

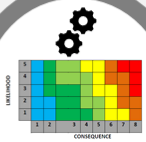
Number of effective controls applicable to likelihood and impact

Impact rating

Initial Impact rating

The maximum Impact ratings that the different operational impacts over the asset would have on the consequence categories defined in ERM

ERM



Risk Severity Rating Table

Risk Rating*

Impact Rating

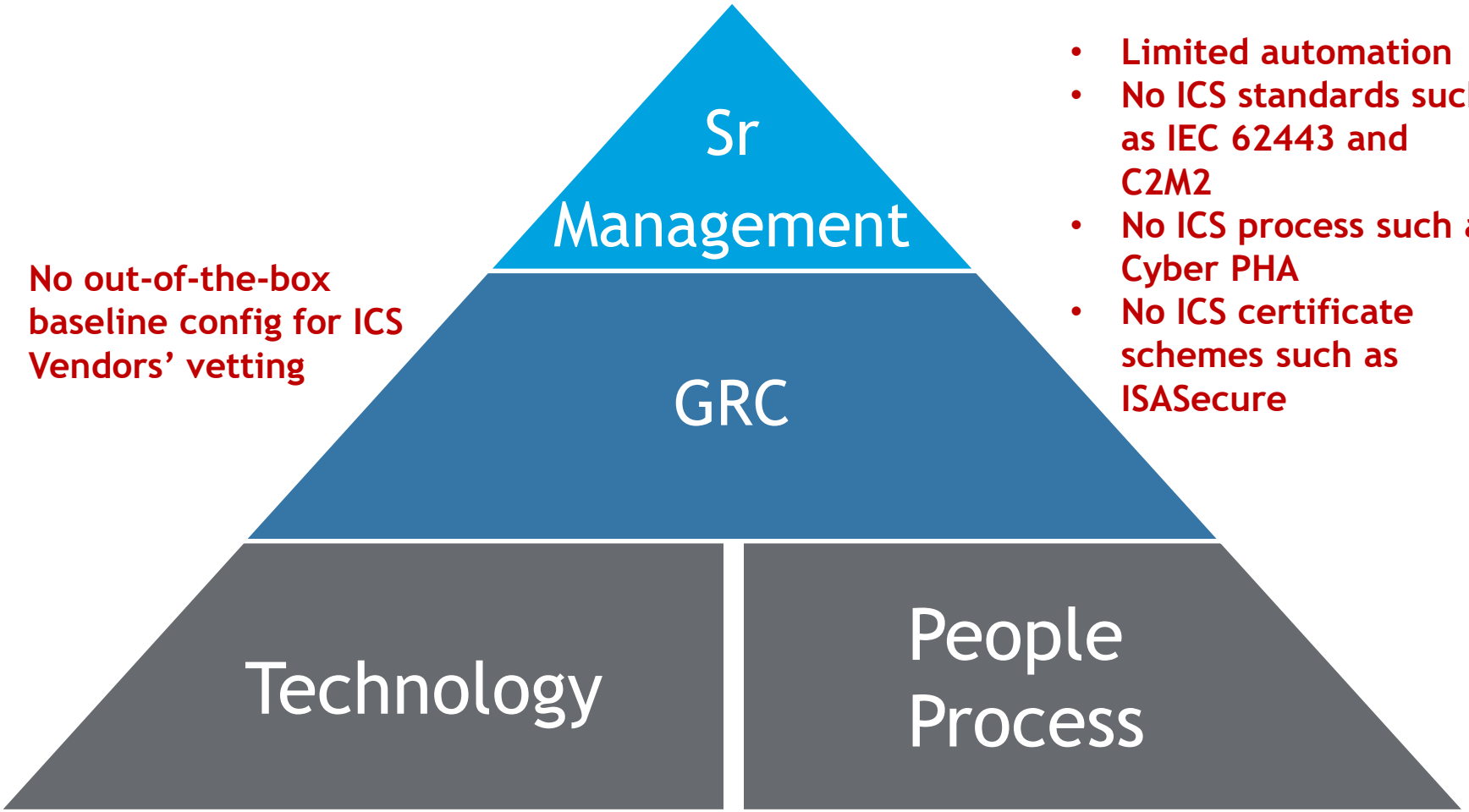
HSE Impact

ERM Impact Matrix and TSL

Consequence Category	Financial	Reputation	Regulations	Health	Business Interruption	Safety	Environment
Initial Impact Rating	Rating 6	Rating 4	*Not Applicable*	*Rating 2*	Rating 3	Rating 8	Rating 6
Target Security Level	Security Level 3	Security Level 2	*Not Applicable*	*Security Level 1*	Security Level 2	Security Level 4	Security Level 3

CyberPHA

Value Realization



- No out-of-the-box baseline config for ICS
- Vendors' vetting

- Limited automation
- No ICS standards such as IEC 62443 and C2M2
- No ICS process such as Cyber PHA
- No ICS certificate schemes such as ISASecure

أرامكو السعودية
saudi aramco

Future Value Maximization

Cybersecurity Big Data

AI Based Cybersecurity Risk Management


أرامكو السعودية
saudi aramco