RISIKOANALYSE

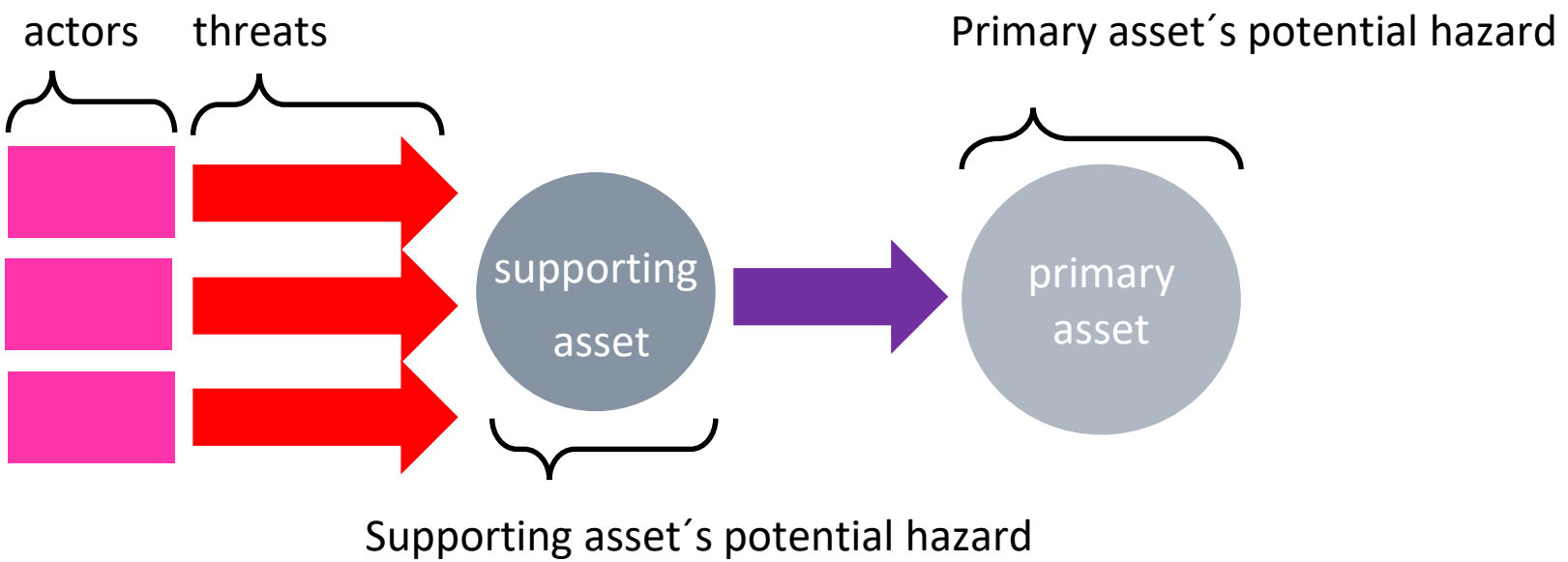
IDEEN, GEDANKEN, ANSÄTZE

PROZESSE ALS DREH- UND ANGELPUNKT

FMEA – SICHERHEIT ALS QUALITÄTSMERKMAL

Information Security Management

Risk Management – Basic: Actors, Threats, Hazards



Information Security Management
Risk Management – Risk identification

- Risk Identification in Risk Management consists of 6 steps,
  - asset identification,
  - threat identification,
  - weakness & vulnerability identification,
  - potential hazard analysis,
  - damage potential analysis,
  - relationship engineering

- As fine-grained proto-risk analysis may give better input for risk-estimation and risk-containment, the needed investment in effort may not justify the overall outcome as there is a high synergy in the measures of securing primary assets.

Information Security Management

Risk Management – Threat identification

Threats and potential hazards are typical likely to be in a direct relationship e.g., the threat of “Denial of Service” is in a relationship to the potential hazard of “Resource exhaustion” (and a weakness of “limited resources” or “insufficient interface monitoring”.

Typical Threats

Denial of Service: rendering a service "not usable" (within customers expectation).

Identity Theft: information assets that are used to identify an entity are stolen, enabling the thief to represent this entity.

Malicious Service Use/Misuse: The possibility that a well-meaning service is used in a bad-meaning use case.

Privilege Escalation: An entity gains unauthorized privileges (e.g., by exploiting an software or process fault).

Support of malicious activities: A state supporting (unintended or intended) malicious activities (e.g., backdoors, XSS)

Integration of infiltration and/or exfiltration channels: A state (theoretically) enabling data flows of malicious intent.

(intentional) (privileged) account misuse: A situation where an authorized user is performing malicious activities.

Integration of unmanaged component: A situation where unmanaged hard-/software is integrated into a techn. stack breaking compliance and endangering service performance.

Malware infection: Obvious

Operational errors: Nearly all activities are prone to operational errors (e.g., with devastating results)

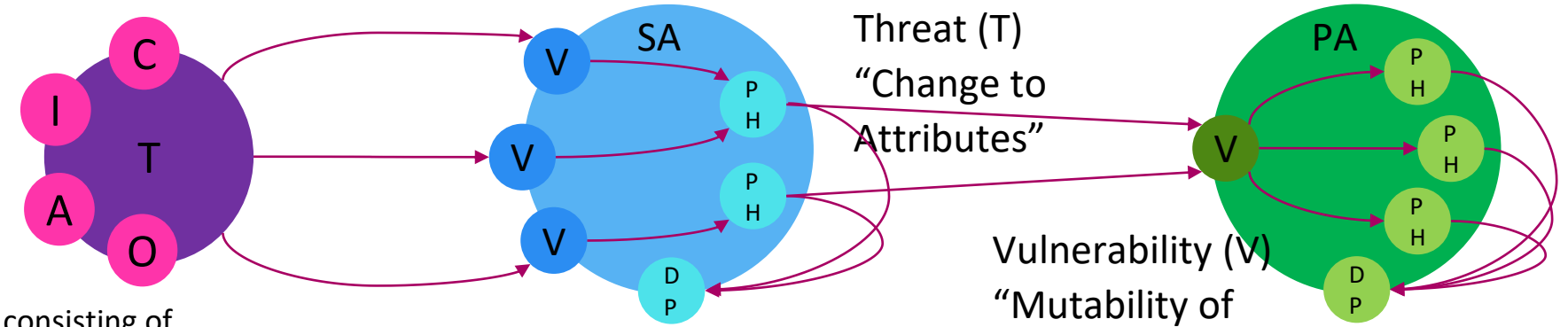
Information Security Management – OSC3

Basic Relationship Model

Threat (T) to Potential Hazard (PH) of Supporting Asset via Vulnerability (V)

Supporting Asset (SA) and inherent potential hazards (PH)

Primary Asset (PA) and inherent PH “Change to Attributes“



Threat consisting of
- Capability (C)
- Intend (I)
- Actor (A)
- Opportunity (O)
- Thread (T)

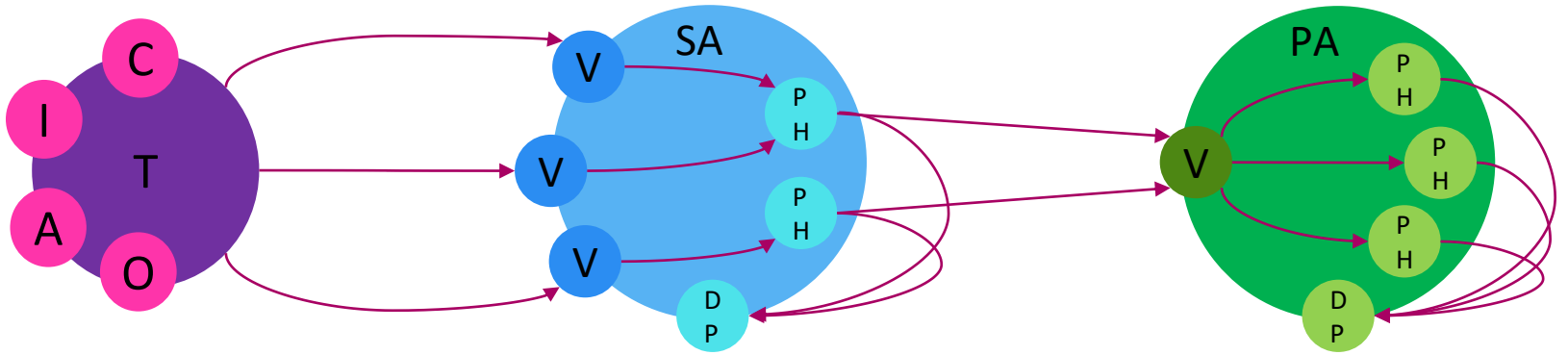
Diverse Vulnerabilities (V) of Supporting Asset

Damage Potential (V)

Vulnerability (V) “Mutability of Attributes”

Information Security Management – OSC3
Basic Relationship Model

Actor = A
Amplification Factor = AF
Capability = C
Damage Potential = DP
Forwarder = F
Immunity = IM
Intend = I
Opportunity = O
Primary Asset = PA
Potential Hazard = PH
Resistor = R
Resistance Factor = RF
Supporting Asset = SA
Threat = T
Vulnerability, Weakness = V



Information Security Management

Risk Management – Potential Hazards in primary Assets

Classical information security typically handles 3 potential hazards that are directly attached to information and it´s nature.

This 3 primary potential hazards are

- Loss of availability
- Loss of integrity
- Loss of confidentiality (or information authority)*

Other, related to a primary assets natures, might be relevant in your use cases:

- Loss of indisputability (Nicht-Abstreibarkeit)
- Loss of reliability / trustability (Verlässlichkeit)
- Loss of confirmability (Nachvollziehbarkeit)

*When the confidentiality is lost, the point is not the loss in confidentiality but of control and authority.

Information Security Management – OSC3
Supporting Asset „Car“ – Un-entangled

- Inherent Potential Hazard
  - Deprecation
    - Aging
    - Laws and Regulations
    - Deflation
  - Loss
    - Theft
    - Destruction

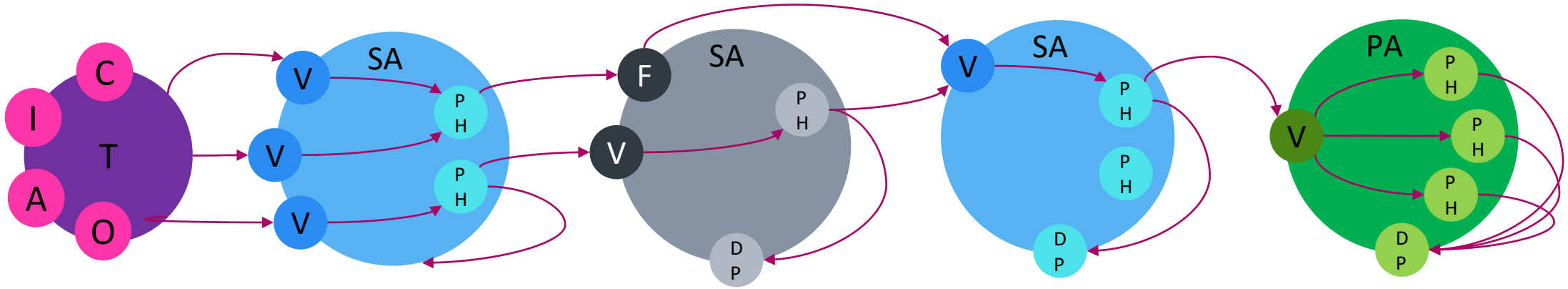
- Vulnerabilities
  - Unsatisfactory material quality e.g., Corrosion
    - Aging
  - Changing of acceptance criteria e.g., Emission Regulations
    - Laws and Regulations
  - Changing of monetary value e.g., change of currency system
    - Deflation
  - Physical accessible, it´s a material thing
    - Theft
    - Destruction

- Damage Potential
  - Deprecation
    - partial loss of invest
  - Loss
    - total loss of invest

Analyzing un-entangled assets is relatively easy, vulnerabilities and damage potential are transparent.

Information Security Management – OSC3

Action Chain Neutral Objects – Environment I

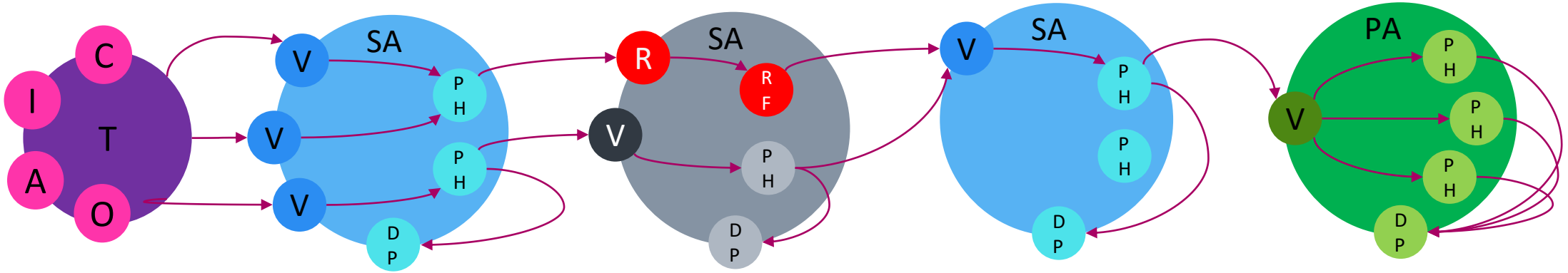


F – Forwarder:

To reduce the effort in modelling a special shortcut is introduced.
Forwarders are neutral elements in respect of the action chain.
This shortcuts are used if an intermediate supporting assets behaves neutral in one or more aspects of the action chain, e.g., a network cable behaves neutral in the action chain of business logic exploitation, but a physical network cable does not behave neutral in other aspects in regards of security and safety e.g., it enables wiretapping or could probably break, get lost, get enflamed, mis-patched etc...

Information Security Management – OSC3

Action Chain – Resistors – Environment II

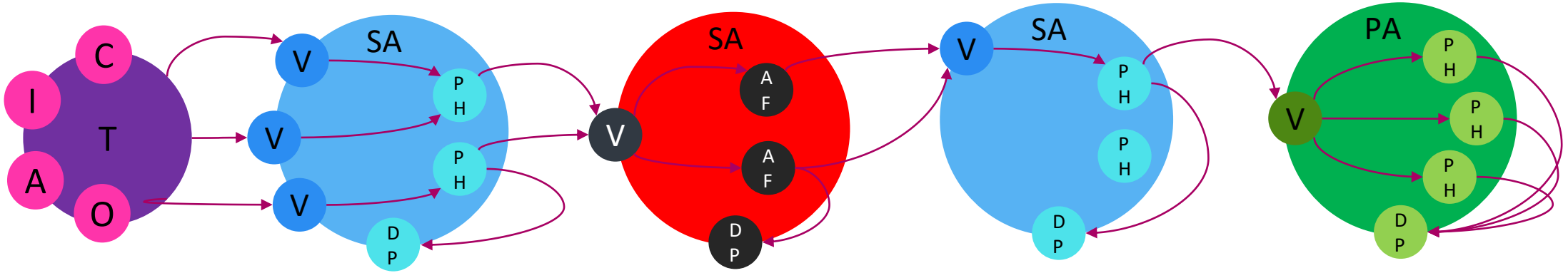


R – Resistors: The term resistors is carefully chosen. These are elements that fulfill no other purpose in reflection of the process or procedure than to reduce the amount of opportunities specific to one or more vulnerabilities supported by the action chain. A firewall for example reduces the amount of opportunities connected to arbitrary service access in downstream assets, an anti-malware solution reduces the amount of opportunities of deploying and executing malware on the downstream assets. Resistors increase the resistivity of a processing chain. They typically cannot eliminate the specific vulnerability completely and typically introduce further vulnerabilities (and complexity) into the processing chain and are typically driven and operated by an external pseudo-parallel-process. In some situations it is possible to cancel out vulnerabilities and resistors with each other to reduce effort, e.g., if supporting assets bring asset native internal resistors.

They introduce the “Resistance Factor” (RF), which enables the illustration of the gain in resistivity in the model and can be mathematically integrated. This is necessary because some resistors are of a high RF (reliability) like firewalls others of a low RF like anti-malware and 1-factor-authentication.

Information Security Management – OSC3

Action Chain – Amplifier – Environment III



A – Amplifier: Typically, Risk-Amplifiers are not explicitly used, but in the form of vulnerabilities of supporting assets containing them. Yet, it can be of interest to explicitly name (and blame) them. I use them to demonstrate the impact of unneeded entangled assets. What are real-world examples of risk amplifiers? In the perspective of IT a classic example of a risk amplifier are privileged accounts another example in regards of IT are software-components like Flash Player, Java Runtimes, Interpreter and Compilers. Based on this examples it becomes obvious what amplifiers are, components, often below the radar, that, by their nature, not only enable – like vulnerabilities - but amplify a proto-risk. As an example, consider a component which comes with an outdated java-runtime environment and running a vulnerable server process, that enables attackers to get restricted limited system access with guest privileges. The risk is amplified by the java-re, because it has a vulnerability enabling local users to escalate their privileges to superuser. Another example a multi-purpose server does not only contain primary data assets of one process but of many and due to its entanglement in not 1 but many processes, the exposure to users is increased.

Information Security Management

Risk Management – Process

ISO/IEC 27005:2011 at least gives the hint that there are at least 2 types of assets to observe. This are the supporting assets, assets like staff, computers, buildings and primary assets like information/data.

But what about processes?

It is necessary to understand that a process is (like information and its attributes) a concept.

A process is describing a *state machine*.

Processes and programs are very similar. That's obvious. Those processes or procedure chains are therefore likely to contain the very similar vulnerabilities by their nature in **regards of logic, process flow, data handling, error accumulation, side channel information leakage, queueing and caching, timing, false assumptions** etc. etc.

Information Security Management

Risk Management – Special Asset - Process

ISO/IEC 27005:2011 at least gives the hint that there are at least 2 types of assets to observe. This are the supporting assets, assets like staff, computers, buildings and primary assets like information/data. But what about processes?

The process perspective is very interesting. It is necessary to understand that a process is (like information) a concept. A process is describing a *state machine*. It is planned and designed as an state machine of the type finite state machine, but in the practical application of a process in the scope of IT it is mostly not possible to foresee or describe any possible input points, inputs, any possible states and therefore any possible action and outcomes. This unpredictable behavior of processes is strengthened by the application of (pseudo-)parallelism e.g., introduced by scaling of processes through parallelization / instancing of processes or running other processes entangling identical assets.

Processes and programs are very similar. That's obvious. Those processes or procedure chains are therefore likely to contain the very similar vulnerabilities by their nature in **regards of logic, process flow, data handling, error accumulation, side channel information leakage, queueing and caching, timing, false assumptions** etc. etc.

Information Security Management
Risk Management – Process Example

Private Transportation, a process well-known in detail to most of us, is a good example for a process.

It is well documented. It is mature. It is to some degree working, it has its hazards and risks, involved people are mostly qualified, it is resilient (which means bending the rules can be tolerated to some degree by the process), it is under monitoring and control and to optimize it, you need to have a deep understand on demand, opportunities and risks.

Not only all kinds of process errors, hazards and risks can be observed on a daily base, but also more complex scenarios like in-flexibility, parallelism (think of road construction, logistic, public transportation and their mass-instancing), load behavior and external factors like asset management, rules of physic are to be considered.

Information Security Management – OSC3

Example - Special Asset - Process

Why are Processes and their Scope, Assets and Impact is important.

Authentication is a major thing in the internet, credit card-based information are often used to authenticate users.

This resulted in a nice hack. While Big-Seller-A asks for credit card-number to authenticate like
“Please, enter the credit card number for your card **********1234” another Big-Seller-B
asks for “Please, tell us the last 4 digits of credit card to recover your account.”

Guess what happens, a clever guy, obtained exposed email-addresses from Big-Seller-A,
with this email-addresses he obtained the last 4 Digits of the account´s owner credit card from Big-Seller-A,
went to Big-Seller-B and pwned the account.

That´s basically why process design and scope is of utter most importance.

Information Security Management

Risk Management – Potential Hazards of Processes

Some potential hazards might not be relevant in the defined context of information security but in the extended context of information security management, in which processes and management processes are of some relevance.

Some of this process related potential hazards are:

Failure of process

A situation resulting in a failure of process defined as rendering the defined target(s) of a process as unachievable.
In the specified context this is a typical threat in the continuous improvement process.

Violation of law and/or regulations

A situation resulting in breaking of the law and/or organizational regulations (e.g., GPDR, Code of Conduct, Compliance)

Loss of attributability, traceability, comprehensibility

A situation resulting in a loss of attributability, traceability, comprehensibility (e.g., loss of quality related records, loss of a document´s change history)

Missing reproducibility

A situation resulting in a loss of reproducibility of a certain state (e.g., due to missing records, documentations).

Loss of time in a time critical processes

A situation in which a loss of time is resulting in advancing damage (e.g. incident process).

Information Security Management
Risk Management – Special Asset – Process II

A service from the process perspective is a probably multi-instance capable process loop.

This perspective introduces a further dimension of dependencies and inheritance to the process.
As a process is typically not designed to run once but be repeated, attributes changes and states obtained (in regards of security attributes) might be passed on to further instances/iteration of the process, down- and upstream processes and processes of higher order.

There are ephemeral states, which are terminated once the process (chain) has finished, persistent state changes, and state changes that are private, local or global to all instances/iterations of a process.

Ephemeral states are states which's influence on in the processing chain is contained within that specific instance/iteration of the process (chain). Further or parallel instances of the same process are not affected by this state change, downstream processes might be influenced by this state change depending of the nature of the state change which influence is either private, local or global.

Process private state changes are not passed on to downstream processes and further iterations. (e.g., poisoning the soup)

Process local state changes are passed on to downstream processes and possibly following iterations of the of same procedure, (if they are not ephemeral (reset) in the scope of any higher layer of processes) persistent, they influence called procedures of lower layers if not privately/locally (or globally) overwritten by the processes of lower layers). (e.g., poisoning the village well)

Process global state changes are not only affecting the local process and its children, but the global process chain (downstream and upstream procedures of the following iterations) of any order passing on possibly undesired states or state changes to entangled procedure calls and primary assets. (e.g., poisoning the ground water)

This can be easier analyzed than explained by data flow diagrams and asset dependency mappings, which make this things obvious.

Information Security Management – OSC3

Pseudo-Parallelism of Processes

The pseudo-parallelism of processes entangling (partially) the same supporting assets and possibly primary assets and the pseudo-parallelism of instances of the same process entangling (partially) the same assets comes with opportunities and risks. A typical threat to a pseudo- parallelized process is the threat “of calling arbitrary processes or procedures of processes with the possibility of entangling arbitrary assets” – scenarios like this are complicating things drastically, especially because we are not trained to think parallel but serial in causal chains.

In a well-designed not instantiable serialized processes the entangled primary and supporting assets and the target states of this assets is easy to assume, by pseudo-parallelism the number of possible overall process states is exponential growing by every instance and only limited by limiting the volume of instances.

Parallelism removes or mitigated some risks typical to serial processes, like the threat “of slow operation on provided interfaces by an accessor/user/client” or more generic “misuse of interface”, which is linked to a vulnerability like “ overgenerous/overforgiving interface” and a hazard potential of “exhaustion of processing capacities” which triggers the hazard potential of the process “blocking of critical process resource” or more generic “Denial of Service” by the process vulnerability “procedure limited to serial processing” in a serial-process.

Information Security Management
Value of Supporting Assets

Supporting Assets have a value, which originates from the effort invested to generate them, the opportunities they generate and their state.

Supporting assets are to be protected to prevent the loss of invested effort and opportunities to protect the processes this supporting assets are embedded in and to protect the entangled primary assets.

The goal of protecting supporting assets is to keep an supporting assets in a desired state, the asset´s target state. Obviously, it is necessary to know the target state of a SA to protect it. Changes to the state of a supporting asset have an impact on the state of entangled primary asset as supporting assets inherit states to entangled primary assets.

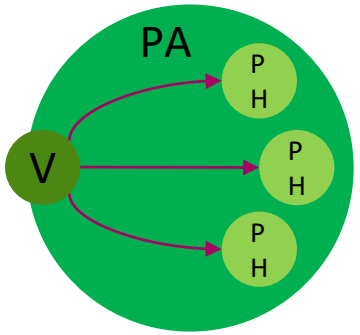
Information Security Management – OSC3

Pseudo-Parallelism of Processes II

- Today in IT there are typically at least 3 processes always potentially parallelized.
  - Work-Process
  - Supporting Process e.g.,
    - Change
    - Incident

- While the production process can be tightly controllable and restrictive, the change process and especially the incident process are not. This is simply because assets entangled in this processes like staff need to be outfitted with a broad range of opportunities to work effective in regards of their process targets. This opportunities are integrated by exhausting permission and powerful tools.
- To reduce downtime in the production this processes are used in parallel to the production process.
- The production process is majorly endangered by this other processes.

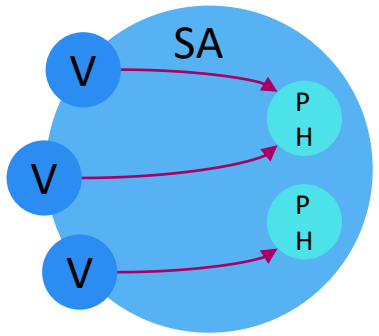
Information Security Management – OSC3
Relationship model – Standardizing PA-HPs



Standardizing primary assets, their vulnerabilities and their potential hazard is pretty easy and already widely applied.

The inherent potential hazard of PAs simply is an undesired change of the state of an assigned attribute. Assign whatever you like, you want blue data? Hm…ok. The potential hazard than is “Change of data color” and the vulnerability still is “Mutability of (the) Attribute (Color)”. (Yeah, I know data has no color, just demonstrating how simple this concept is.)

Information Security Management – OSC3
Relationship model – Standardizing SA-HPs



Standardizing supporting assets, their vulnerabilities and their potential hazard (PH) is a necessity to setup reusable models.

In IT we typically see 3 types of supporting assets, people, places and IT-Components. Computers and People are both transporting, storing and processing data alias primary assets. Therefore both share a subset of inherent potential hazards related vulnerabilities in both.

Both for example share the PH to “elevation of privilege(s)”, “an (unintentional) support of malicious activities” and both can be “manipulated to assume a certain state is given”. The related vulnerabilities could be descript as “credulousness” or “erroneous input validation” for example.
They are both supporting assets and are prone to PHs like “ a loss of availability” or “loss of integrity”, in regards of intentional black boxes “loss of confidentiality” can be a potential hazard, too.

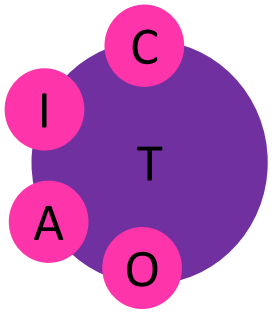
By this examples it is becoming obvious that the standardization of PH is possible and furthermore that there is a synergy even in diverged supporting assets. Additionally, that the identification of PHs is supportive to vulnerability (or weakness) identification.

Information Security Management
Risk Management – Threat catalogs

Thankfully many somewhat clever people already identified threats related to supporting and primary information security assets. There are threat-catalogues available for all kinds of technology stacks, web-application, agency IT, data-center… some are extremely detailed other strongly aggregated.

- BSI released 6 exhausting Gefährdungskataloge
- National Institute of Standards & Technology (NIST) released SP 800-30
- ENISA released ENISA Threat Taxonomy
- International Organization for Standardization (ISO) released ISO/IEC 27005

Information Security Management
Risk Management – Threat Standardization



T consisting of
- Capability (C)
- Intend (I)
- Actor (A)
- Opportunity (O)

Many aspects of threats are unknown, random and manifold.

This aspects are not helpful, even worse, working with inherent false assumption will always have a negative impact on the accuracy of the holistic risk management process, with the outcome of wrong strategic decisions.

Actors: We know they are there. People, logical and physical effects.

Opportunities: We might be able to determine some.

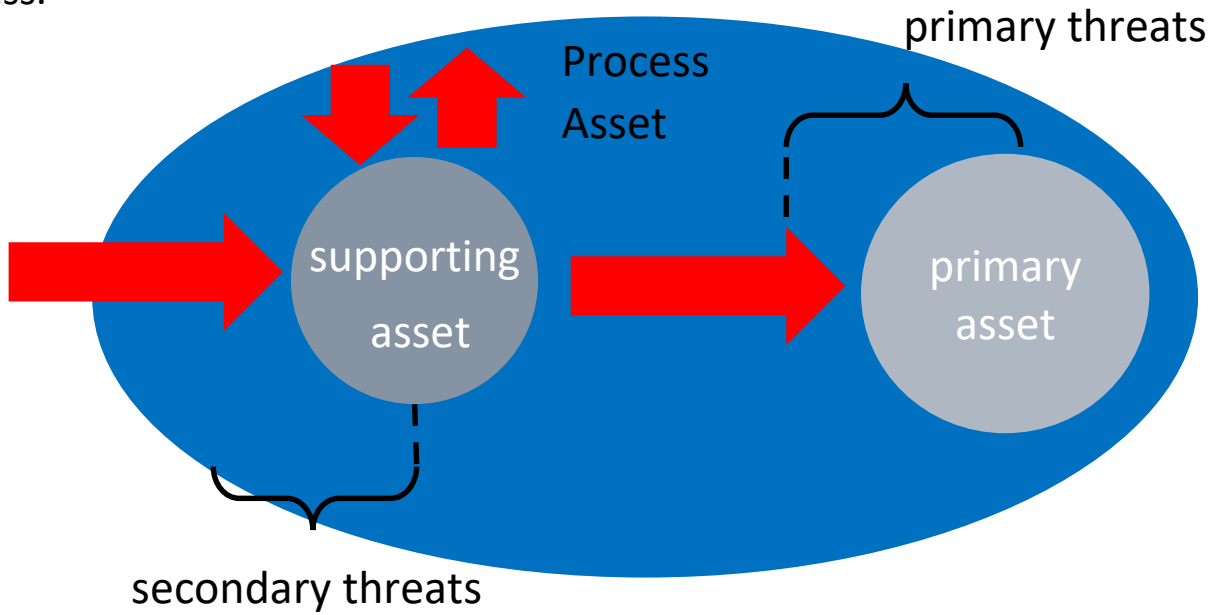
Intend: It´s an overall false assumption to speak of intends.
Physical effects and Errors have no intend.

Capability: There are is a basic set and potential necessary to exploit a vulnerability in regard of threat actors but again physical effects and errors does not need a capability.

The needed potential in capability is an aspect often referred and while this can be agreed upon, the quantitative volume of entities who obtained this potential remains uncertain. I personally would tend to reduce the whole threat actor discussion to an absolute minimum.

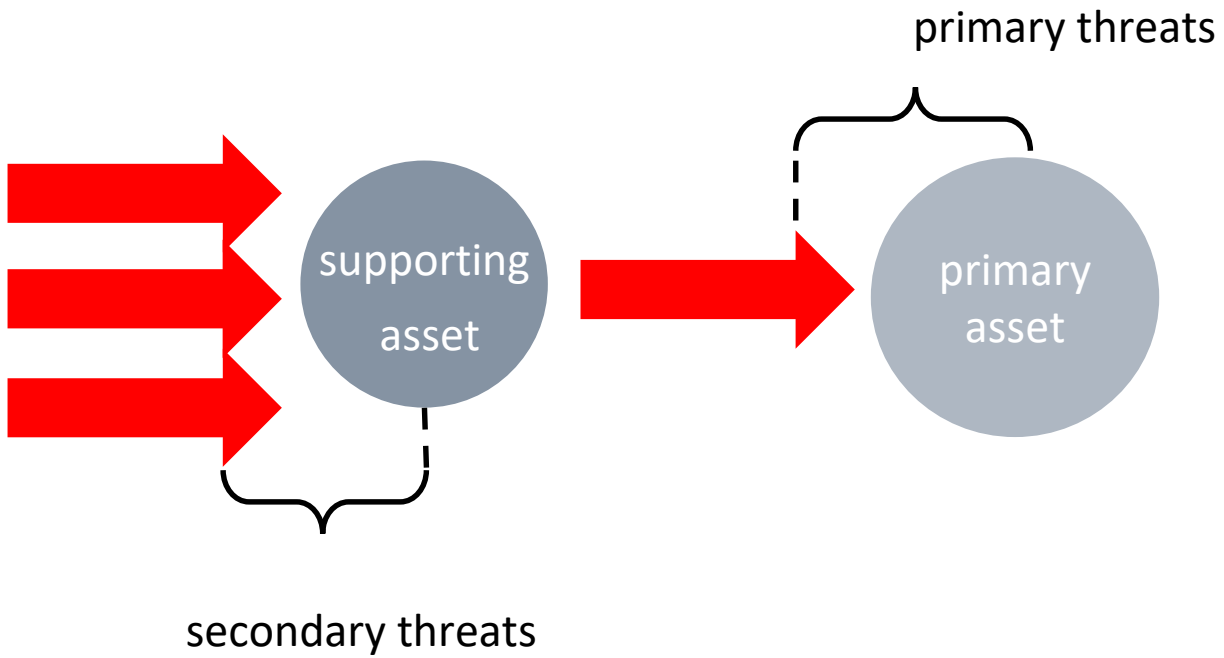
Information Security Management
Risk Management – Threat identification

- Threat identification in consideration of the underlying process and its embedded assets.
- The process asset itself is capable of countering specific threats to secondary assets.
- The process by itself is introducing the inherent threat of a “Loss of Capability” to perform.
- This threat is exploitable by inherent weaknesses of the process itself but only by vulnerabilities in supporting assets associated with the process.



Information Security Management
Risk Management – Threat identification

- Threat identification based on the threat´s intermediate targets, vulnerabilities in supporting or process assets, in combination with threats to primary targets in relation to a primary asset´s vulnerabilities is providing a model asset orientated model fine-grained enough to successfully identify potential threats.



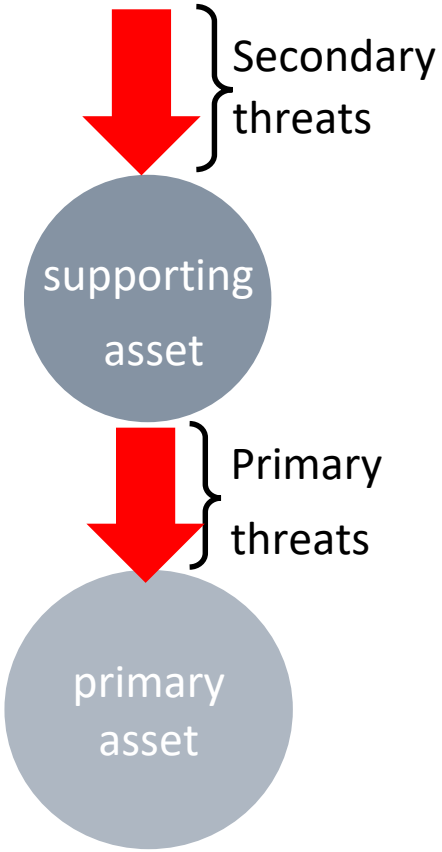
Information Security Management
Risk Management – Threat identification

Secondary threats describing threats that are threatening the triggering of hazard potentials by exploiting vulnerabilities of supporting or process assets.

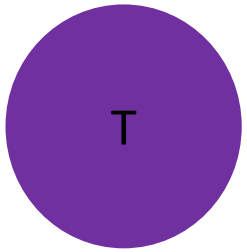
While primary threats are inherent to primary assets vulnerabilities, secondary threats on a usable level of abstraction are not always given by the abstract nature (inherent) of the supporting assets.

On a very high level all of this threats could be addressed as “undesirable utilization of weaknesses in entities (e.g., process logic, staff, hard-, software)”.

All this secondary threats have one thing in common, they enable the primary asset inherent hazard potentials to affect primary assets.



Information Security Management
Risk Management – Threat Standardization



Threats can be grouped, categorized, normalized and finally standardized. A grouping can be performed based on (intermediate) target vulnerabilities, target (intermediate) potential hazard or based on the type of associated assets and furthermore.

Most efficient is the grouping by a threat´s nature, which will enable the analyst to highly aggregate threats. Reducing details and granularity of threats will increase the efficiency.

Risk Management is not made for breaking down threats to unique events.

-> See Microsoft STRIDE – which is in my opinion not detailed enough

Information Security Management

Hazard Identification – Examples: What we have so far.

- Primary Hazards
  - Loss of Availability
  - Loss of Integrity
  - Loss of Confidentiality
    - Loss of Control

- Attribution related Hazards
  - Loss of indisputability
  - Loss of reliability / trustability
  - Loss of confirmability
  - Loss of timeliness
  - Loss of accuracy

- Secondary Hazards
  - Un-sanctioned/malicious asset state deviation (Process, SA) (Loss of Integrity)
  - Loss of Control (SA, PA, Process)
  - Denial of Service (Process, SA)
    - Temp. Loss of Capacity (Proc, SA)
    - Temp. Loss of Capabillity (Proc, SA)
  - Support of malicious activities (Process, SA)
  - Malicious Service Use/Misuse (Process, SA)
  - (intentional) (privileged) account misuse; (Process, SA)
  - Privilege escalation (Process, SA)
  - Integration of unmanaged components (Process) (Loss of Integrity)
  - Integration of infiltration and/or exfiltration Channels (Process, SA) (Loss of Integrity)
  - Operational errors (Process, SA)
  - Persistent undetected vulnerabilities/weaknesses (Process, SA)
  - (intentional) (privileged) account misuse (Process, SA)
  - Identity theft (Process, SA)
  - Malware infection (SA)
  - Loss of Capacity (Process, SA)

- Management process related Hazards
  - Loss of Capability
  - Failure of process
  - Violation of law and/or regulations
  - Loss of attributability, traceability, comprehensibility,
  - Missing reproducibility
  - Loss of time in (time) critical processes (timelyness)
  - Qualification gaps

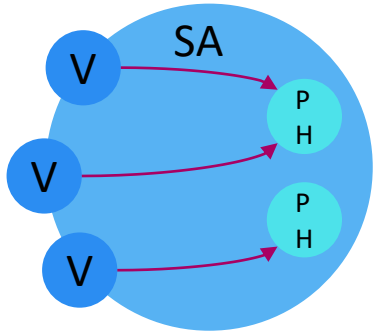
Information Security Management
Risk Identification – Process-Level

- While the threat to a process and its procedures stays the same during the runtime of the process, the vulnerability and the inherent hazards of the process, it is partially inhering from the entangled (supporting) assets, is associated with the state of the process.
- Every procedures (or tasks) within the process has an specific set of embedded supporting assets (staff, applications) which are vulnerable to very specific threats only during specific points in time during the procedures runtime, typically (but not limited to) the state of input intake, of the individual procedure is associated with hazards.
- Typical process related hazards arising from its vulnerability to the unsanctioned call of execution of a specific procedures, a state where an action/ procedure is executed without legitimation and/or at a point in time where the process is in a state where the execution of the called procedure is not necessary or undesired to achieve a defined process target.
- As processes consume limited resource, processes bear the hazard of capacity overload, they are vulnerable to resource exhaustion. A state where essential resources of the process are no longer able to fulfill the execution of tasks to achieve the defined process target within the designated time frame. (real time processing)
- Some Observations:

  Most vulnerabilities inherent to programs are also inherent to processes for obvious reason.
  Scaling concepts like “increasing workload potential” and “parallelization” has an major impact on the threat landscape.
  There is a close to infinite amount of threats existing, detailing must be limited to just fulfill the specific risk m. process requirements.
  Vulnerabilities can be mapped to states of processes and procedures.
  Hazards are inherent to assets. Related Vulnerabilities can be mitigated or avoided by processes.
  States are of procedures/processes are vulnerable to state specific threats.
  Many but not all vulnerabilities of process states originates from the entangled data and supporting assets.
  The undesired execution of procedures is a vulnerability inherent to processes.
  Intentionally or unintentionally misconfiguration of processes is a threat to processes.

Information Security Management – OSC3

Relationship model – Standardizing Vulnerabilities



If you find more than, 20 native vulnerabilities per asset type, you have a better imagination capacity than me or you might do something wrong (e.g., scoping).

Identifying and standardizing vulnerabilities in supporting assets is a little more complicated, deriving basic vulnerabilities based on PHs is the first step, but the relationship between vulnerabilities and the potential hazard are usually not 1:1, it typically is N:1 or 1:N.
A well-designed scoping of supporting assets is of major importance. It´s heavily recommend to cut supporting assets into chewable pieces (e.g., Server into Hardware, OS, Application, Network) by still maintaining a full coverage.
After an initial set of SAs have been descripted, this probably will become more and more easy and self-completing. Keep in mind, we do not talk about “vulnerabilities“ in a closer but wider sense, not specific bugs or backdoors, but weaknesses.

Typical vulnerabilities of processes are authentication, authorization, logic, state and state change related and some vulnerabilities arise in processes pseudo-parallelism, like race conditions, concurrence, resource competition, resource blocking, and other are effects to occur only under certain process workload pattern like bottlenecks. Integrity and Confidentiality of a process can be compromised and related to BCM a process can become unavailable, e.g., by termination of process critical assets (where *terminate-ability* of course is an inherited vulnerability of a supporting asset.).

Typical vulnerabilities of supporting assets are related to faulty authorization, authentication, false assumptions, input validation related, design errors, technical errors in supporting assets…

Information Security Management – OSC3

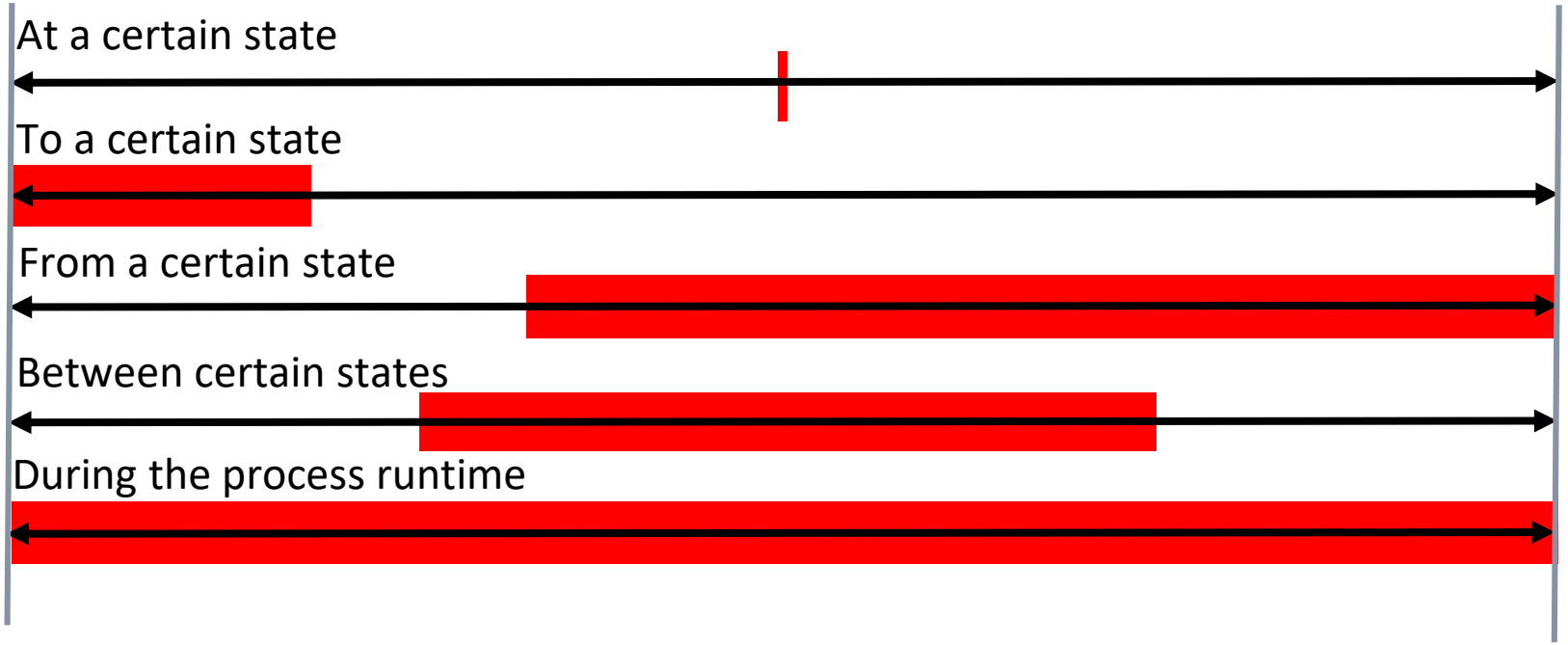
Vulnerabilities

- Vulnerabilities of primary assets are related and limited to the attribution of the primary asset which is introducing potential hazards to the primary assets. This vulnerabilities are of the mutability of the associated attributes.
- There are two types of vulnerabilities given by the nature of the asset and vulnerabilities introduced to supporting assets by error or decision. (Philosophical spoken, nothing men-made can be perfect so one could argue that faultiness is inherent in supporting assets.) Vulnerabilities of a supporting assets are not limited to the number of inherent potential hazards of the related supporting asset.
- Vulnerability to process assets consist of vulnerabilities which are inherited from the associated supporting assets, primary assets and vulnerabilities introduced by the process itself.

Information Security Management – OSC3

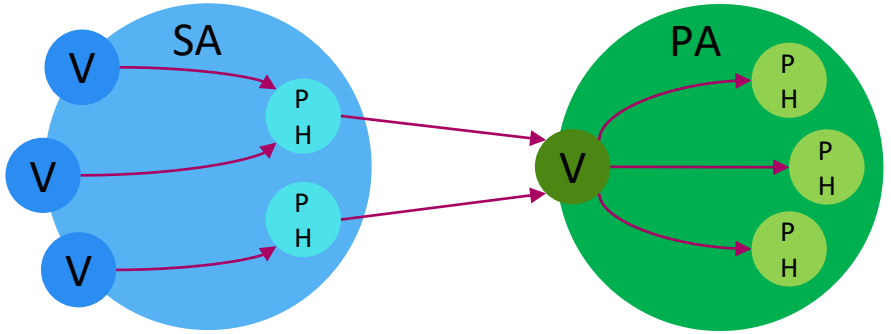
Vulnerabilities during the Process-Runtime - Environment II

The existence of vulnerabilities of assets is coupled with the occurrence of potential hazards in process- and supporting assets. The process enters and exits vulnerable states during its runtime.



Information Security Management – OSC3

Relationship model – Damage Potential



Damage potential of an event is descripted as a potential loss or a potential loss of losing the opportunity to reach a defined target.

The loss might be related to the value of the asset, the loss generated by the loss of opportunity, and the subsequent damage arising from the occurrence of the event in addition to the costs of incident handling.

damage potential

- Value
- Effort
- Invest

+

damage potential

- Value
- Effort
- Invest
- Attribution related damage potential

+

Subsequent damage potential

- …

+

Incident handling costs

- Handling costs
- Recovery effort
- Business impact

Information Security Management
Risk Management - Damage Potential

- The estimation of a risk related impact, typically the loss of money due to the occurrence of an event incl. recovery and restore procedures, customer communication, incident management etc. is no longer easy to calculate, while IT supported processes where widely setup monolithic with sharp process and technologic boundaries since the very beginning of IT, services nowadays become ever smaller and specialized parts with entanglement not in a single but dozens or possibly hundreds of processes with horizontal, vertical dependencies on other decentralized services, even loops are possible. The direct impact, a service outage of several minutes fixed with low effort, may accumulated to days of outages in dependent services and processes. Therefore it is necessary to design processes with respect of the risks of their components and resilient in the reflection of the service delivery chain.

Information Security Management – OSC3

Resolving Dependencies - Pseudo-Parallelism of Processes III

- As mentioned before the web of dependencies of process and assets is problematic in classic risk management. By proto-risk identification through the introduced asset centric entity relationship model, it´s generated automatically as a side effect.
- Nodes can be identified by the relationships of assets. By analyzing the relationships the entanglement in procedures and processes multi-dimensional dependencies maps can be generated, easing identification of not only dependencies but also the criticality of assets in regards of the business-process.
- Identifying risks and proto-risks of every stage in multi-process domains for free.

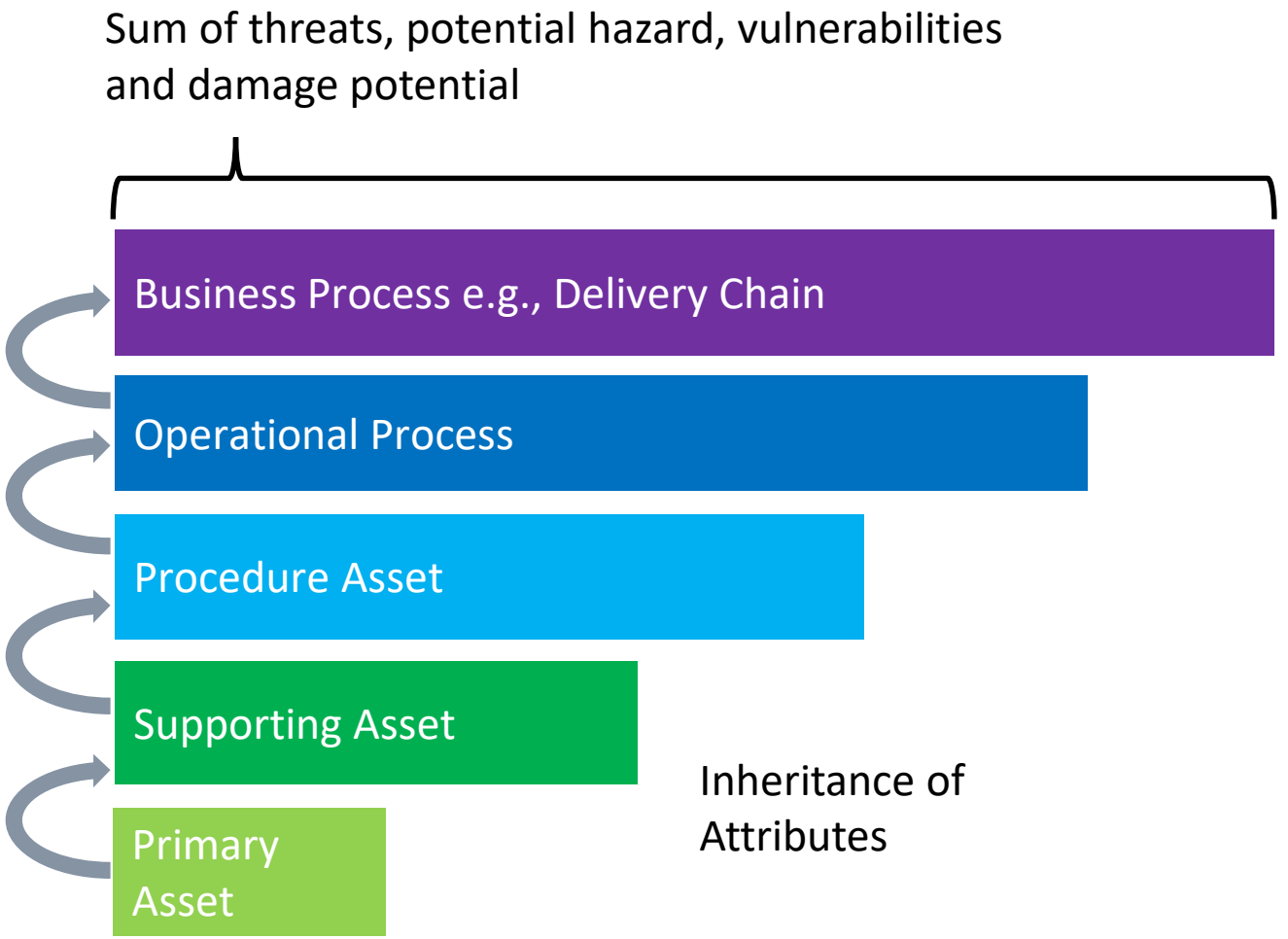
Information Security Management – OSC3

How to identify risks.

Holistic identification of valid risks has to be performed by the top-down-methodology to be efficient.

The sum volume of the invest and the value added by the value chain as the total value of the entangled primary assets and the damage potential is only known on the level of the business process.

All assets, potential hazards, threats and vulnerabilities must be identified.



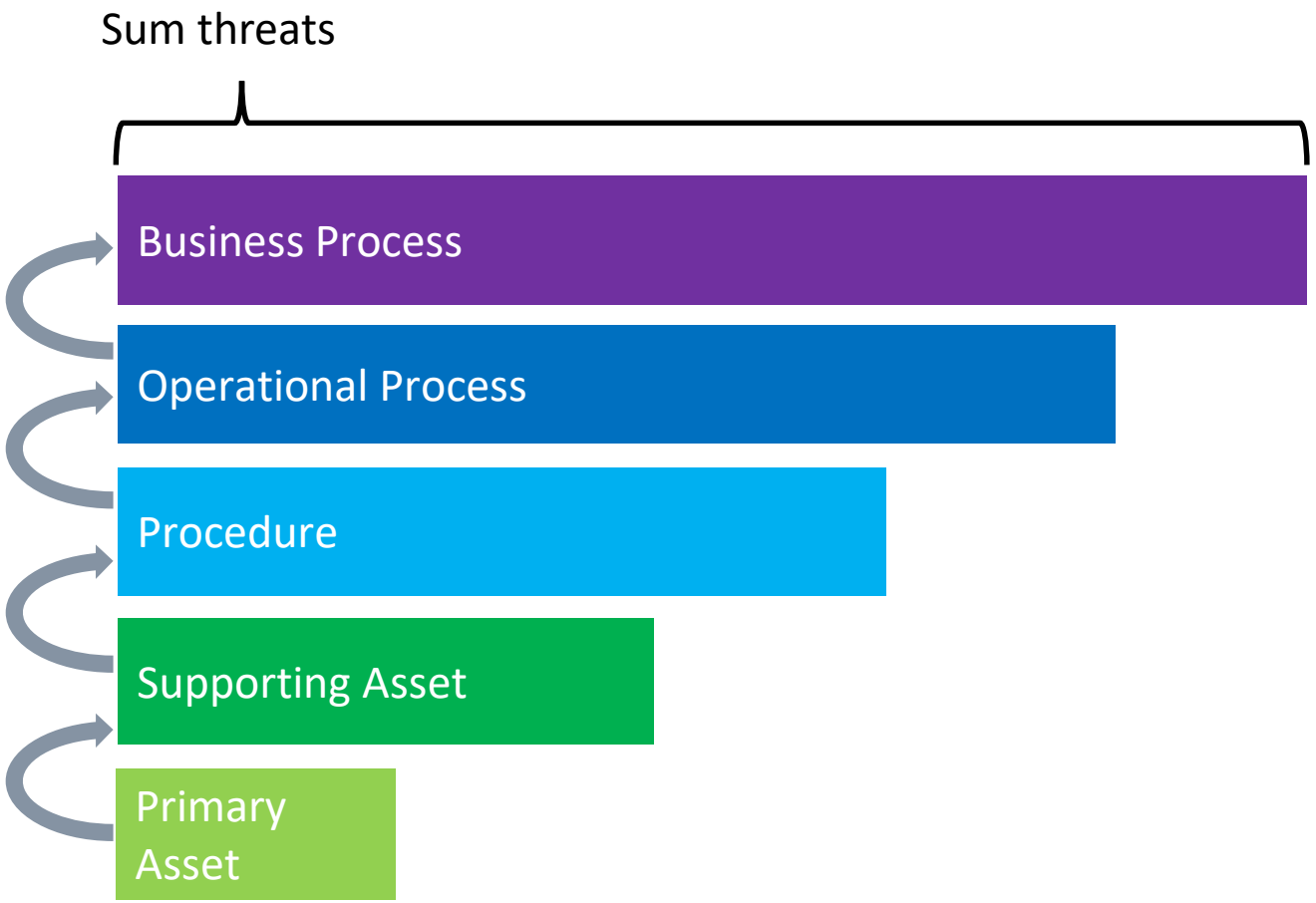
Information Security Management – OSC3

How to identify risks.

By obtaining the
- potential hazards
- vulnerabilities
the holistic identification of valid threats is enabled.

With the completion of the threat analysis, the valid risk scenarios become obvious, this is an important part of the necessary input for the risk analysis.

By consuming the parameter of the value chain and the input from the qualitative or quantitative risk analysis the risk analysis can be completed by application of the damage potential.

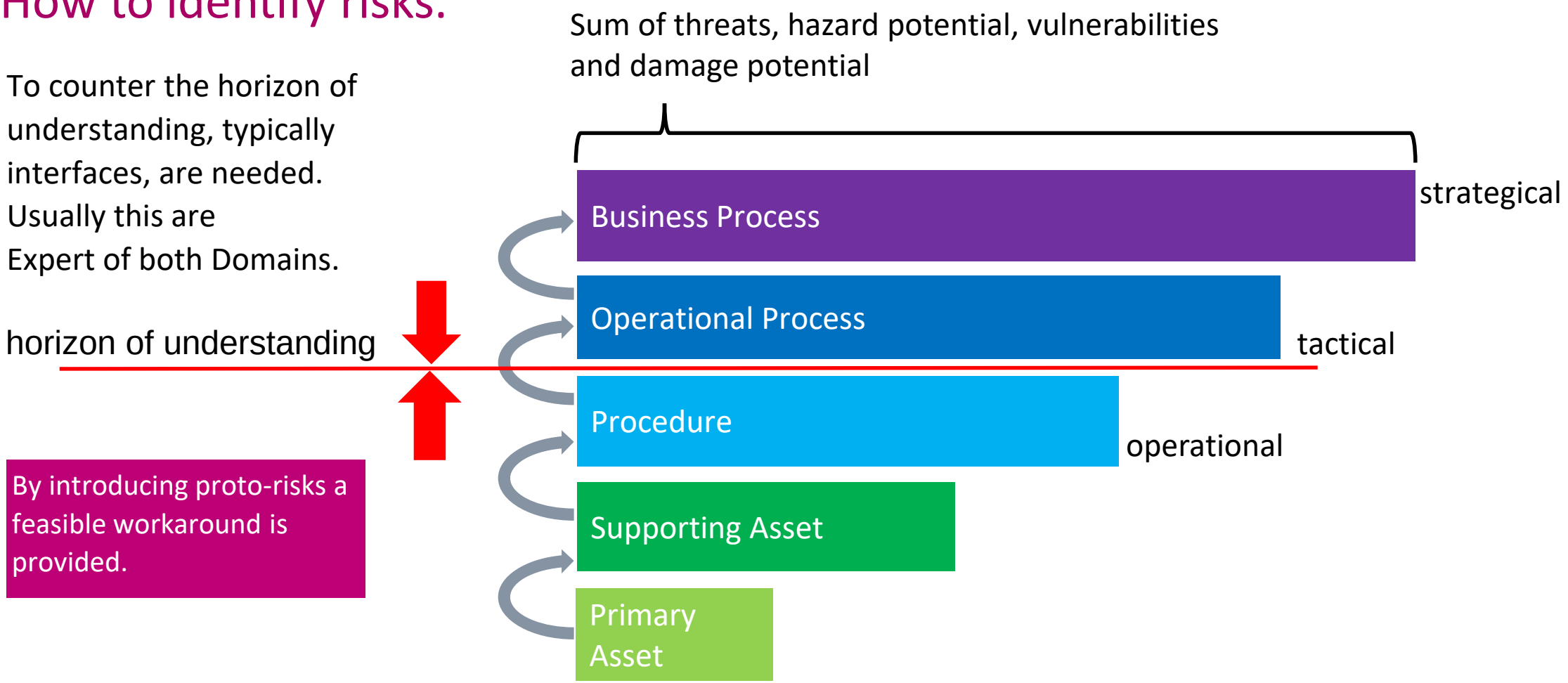


Information Security Management – OSC3

How to identify risks.

To counter the horizon of understanding, typically interfaces, are needed.
Usually this are
Expert of both Domains.

By introducing proto-risks a feasible workaround is provided.

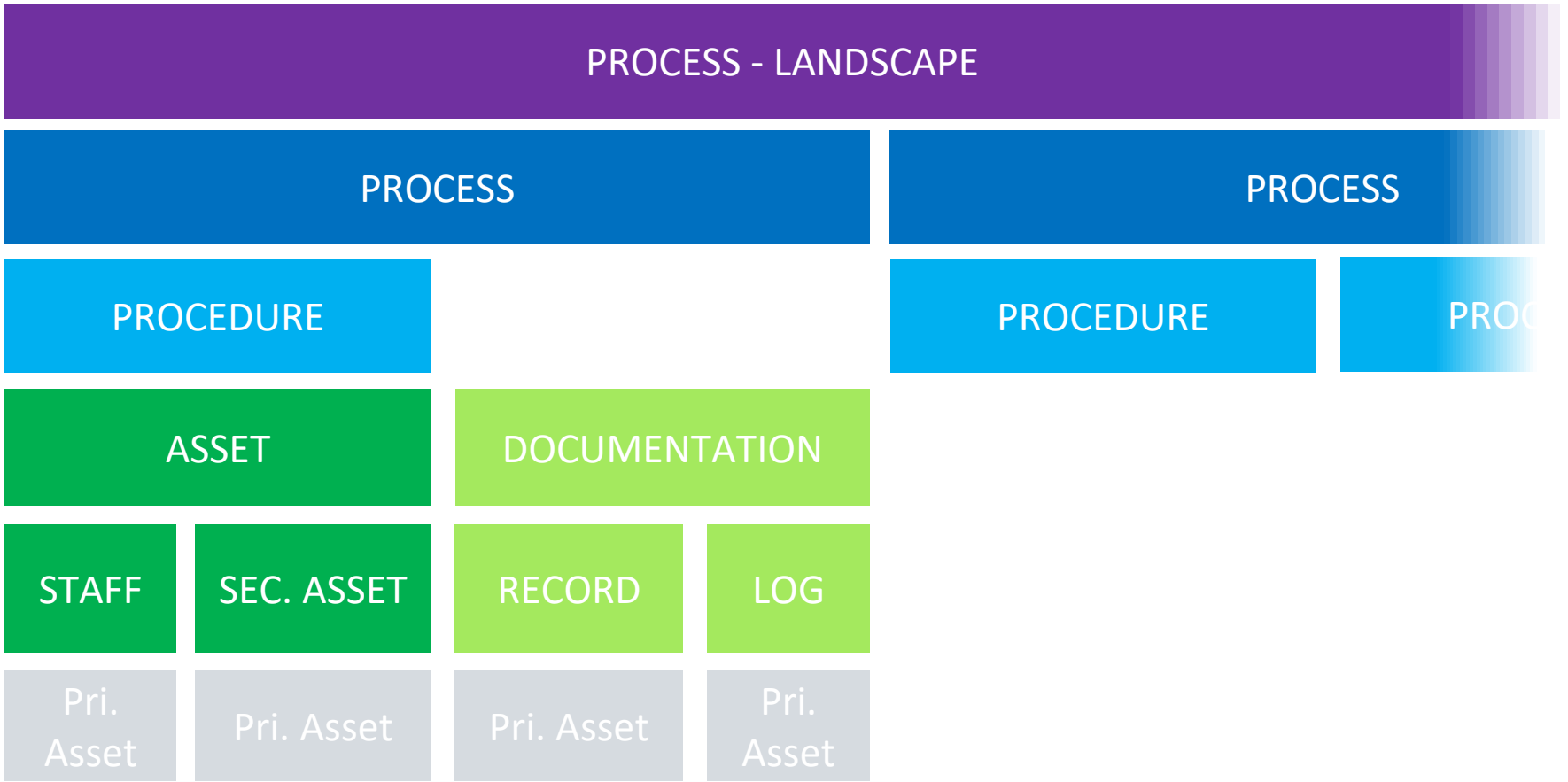


BOSCH

Information Security Management
Concepts of Proto-Risks

- As it is not always possible or necessary to analysis a risks, e.g., due to the immanent „Horizon of Understanding“, proto-risks are introduced. This proto-risks are results from incomplete risk analysis, a proto-risk contains only partial information regarding a classic risk e.g., missing a damage potential analysis from the perspective of the business process, or missing the aspects of the threat analysis, like quantitative or qualitative threat analysis. It´s not a *full qualified* risk.
- Using the term „proto-risks“ instead of „risks“ should make it transparent to the consumer, that we talk about a (possibly use case or stage sufficient but) incomplete model of risks, to reduce false assumption in regards of the proto-risk in question.
- Any risk not identified by a transparent and reproducible approved methodology from at least the perspective of the business process may be considered as a proto-risk.
- Regarding the top-down-analysis model one could use stages or levels e.g., a risk analyzed in the perspective of the procedure-level could be called a „level-3-proto-risk“.
  (Ok, I confess, love this wording, It´s totally Scifi.)
- This staging-procedure has 3 major pros, first of all by staging the risk analysis, domain experts operating the risk analysis process in regards of their domain, risk analysis can be parallelized and a max. of transparency is created, easing understanding and management drastically.

Information Security Management
Risk Identification - Level



BOSCH

Information Security Management

FMEA - Einführung

FMEA – Failure Mode Effect Analysis ist ein lange erprobtes und im Bereich Produkt-Sicherheit umfangreich eingesetztes Verfahren zur Qualitätssicherung. Der Einsatz von FMEA in den Bereichen Risikoanalyse und insbesondere Folgenabschätzung in der Informationssicherheit hingegen ist kaum verbreitet. Ausgangspunkte hier ist der Defekt, von dem ausgehend mögliche Folgeschäden betrachtet werden und mögliche Maßnahmen abgeleitet werden.

Ursächlich hierfür dürfte die Fokussierung von ISO 27001 und BSI auf stark vereinfachten Methoden der Risikoanalyse sein, die sich stark auf unterstützende Assets, wie Server, Software und Netze, fokussiert. Dieser Ansatz wird zumeist kombiniert mit Mitteln wie Delphi-Analyse und Brainstorming. Diese Methoden liefern meiner Ansicht nach allerdings ein nicht-reproduzierbares und in den seltensten Fällen nachvollziehbares Ergebnis, welches stark von individuellen Sichtweisen und dem technischem Niveau der Teilnehmer beeinflusst wird.

Durch die lange Historie der FMEA kann diese Methode als sehr ausgereift angesehen werden.
Bedingt durch diese Historie gibt es mit Auditoren und Revisoren keine Methodik-Diskussionen.
Ein weiterer Vorteil der Nutzungsbreite ist, das Vorhandensein von unterstützenden Werkzeugen (**oft kostenlos**).

https://www.controlling-wiki.com/de/index.php/Risikoanalyse_FMEA

https://www.uni-ulm.de/fileadmin/website_uni_ulm/iui/datenschutz/VL2013-2c.pdf

http://www.iso27001security.com/html/risk_mgmt.html

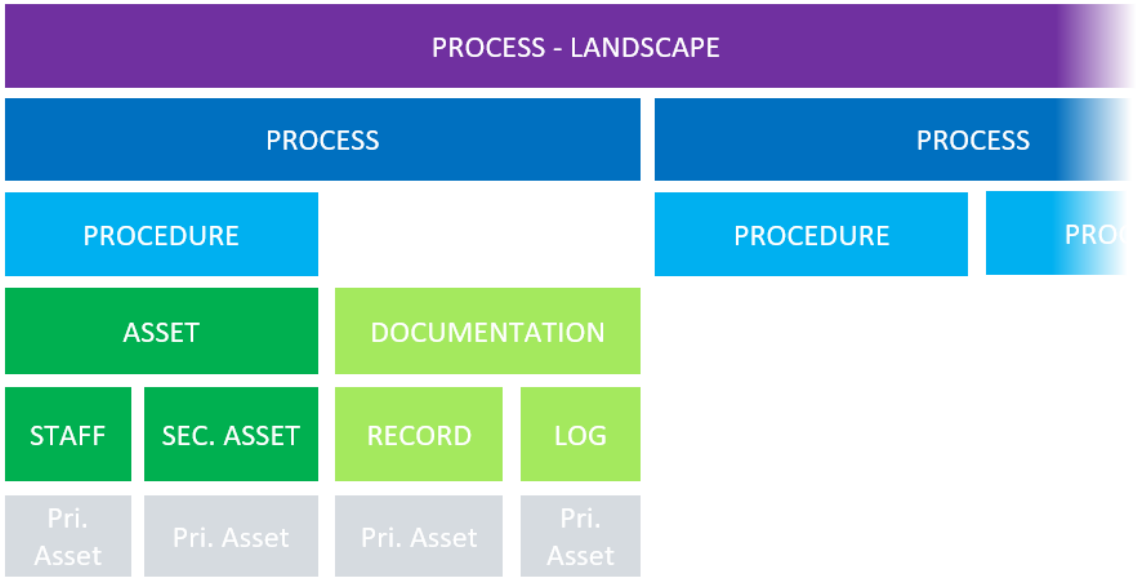
http://www.iso27001security.com/ISO27k_FMEA_spreadsheet_1v1.xlsx

BOSCH

Information Security Management

Risk Assessment – FMEA Interview - Praktisches Vorgehen

Ausgangssituation ist eine ausreichend detailliertes und vollständiges Prozess- oder Architektur-Dokumentation, welche neben primären und unterstützenden Assets auch externe Abhängigkeiten und Schnittstellen einschließt.



Die Tiefe des Detaillierungsgrads richtet sich nach dem Ziel der Analyse. Die Bandbreite kann von der Prozessebene bis hin zum Transistor reichen.

Gezielt wird nach der Häufigkeit (1-10), der Wahrscheinlichkeit einer Erkennung (1-10), den Folgen, von möglichen Fehlern (z.B. Verlust von Daten und Funktionen), die damit verbundenen Schadenspotential (Bedeutung 1-10) und möglichen Ursachen sowie kompensierenden Maßnahmen gefragt werden.

BOSCH

Information Security Management

Risk Assessment – FMEA Interview - Praktisches Vorgehen

Im Interview zwischen FMEA-Experten und technischen Experten erfolgt eine ggf. Tool-gestützte Modellierung des Services.
Dies kann sowohl für die Prozess-Domain als auch den Systemverbund, dessen Daten, Schnittstellen und Komponenten durchgeführt werden.

Während dieser Modellierung ist es die Aufgabe des FMEA-Experte Fragen zur Kritikalität von Komponenten (z.B. Arbeitsabläufen oder Datenquellen und Schnittstellen) zu stellen und den technischen Experten um eine Folgenabschätzung im Falle eines Defektes (z.B. Datenverlust, Funktionsverlust) zu bitten, sowie mögliche Ursachen hierfür (z.B. unzureichende Zugriffskontrolle) und (geplante/umgesetzte) Maßnahmen (strikte Rechteverwaltung) zu erfragen.

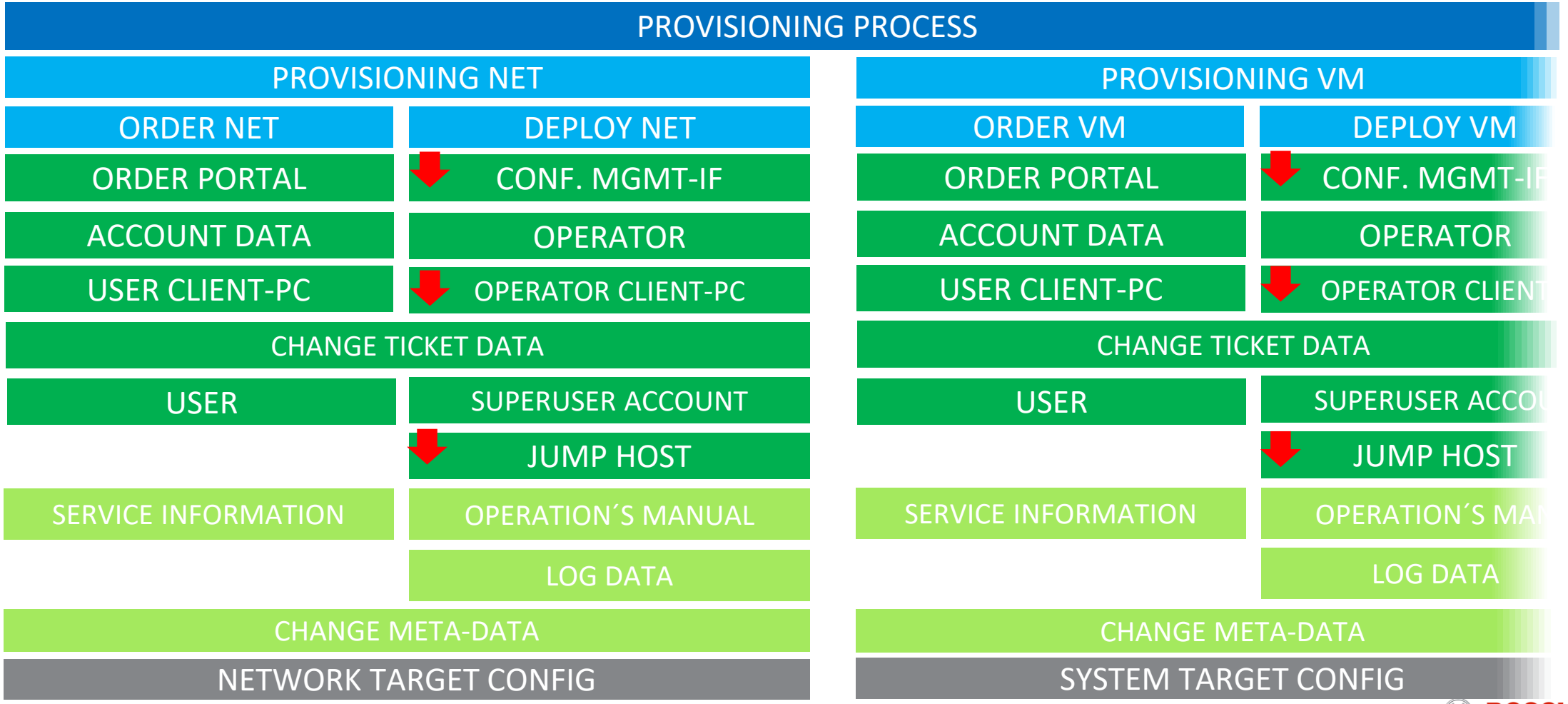
Bei umfangreichen Prozessen und Architekturen wird der Fokus zunächst auf die kritischsten Komponenten gelegt.
Zur Identifikation dieser kritischen Komponenten kann die Risikokennzahl (RKZ als Produkt aus Häufigkeit (1-10), Wahrscheinlichkeit (1-10) und Schadenspotential (1-10)), herangezogen werden.

Ursachen, können mittels dem 5-Why-Verfahren zur Rootcause-Analyse, ermittelt werden.

Modellierungswerkzeuge standardisieren typischerweise Komponenten, Ursachen und Folgen,
es ist im höchsten Maße empfohlen dieses Vorgehen zu übernehmen,
z.B. so wie ich hier Threats (Bedrohungen), Vulnerabilities/Weaknesses (Schwächen) und Potential Hazards (Gefährdungspotenziale) demonstriert habe.

Information Security Management

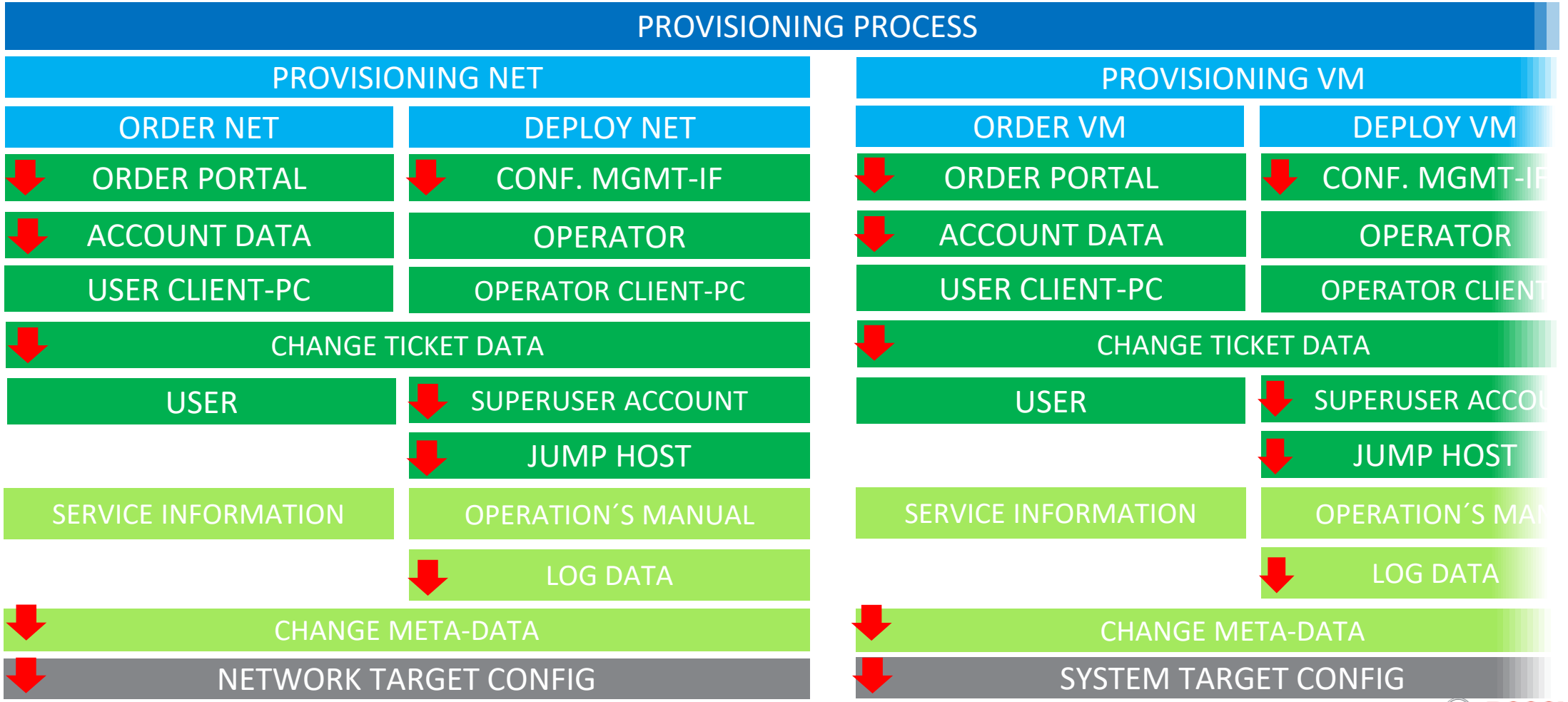
Risk Identification – Asset based focus



BOSCH

Information Security Management

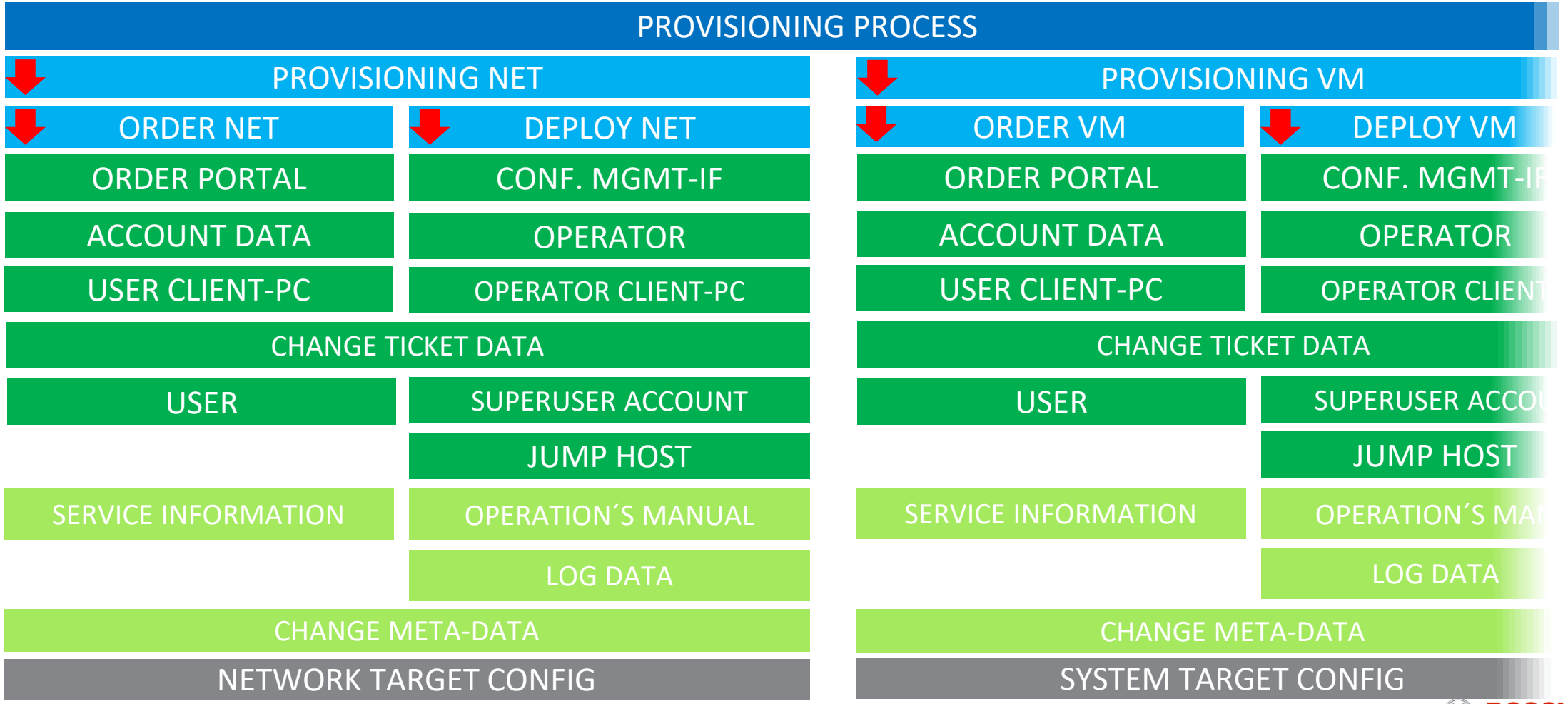
Risk Identification – DSGVO Focus



BOSCH

Information Security Management

Risk Identification – Process based focus

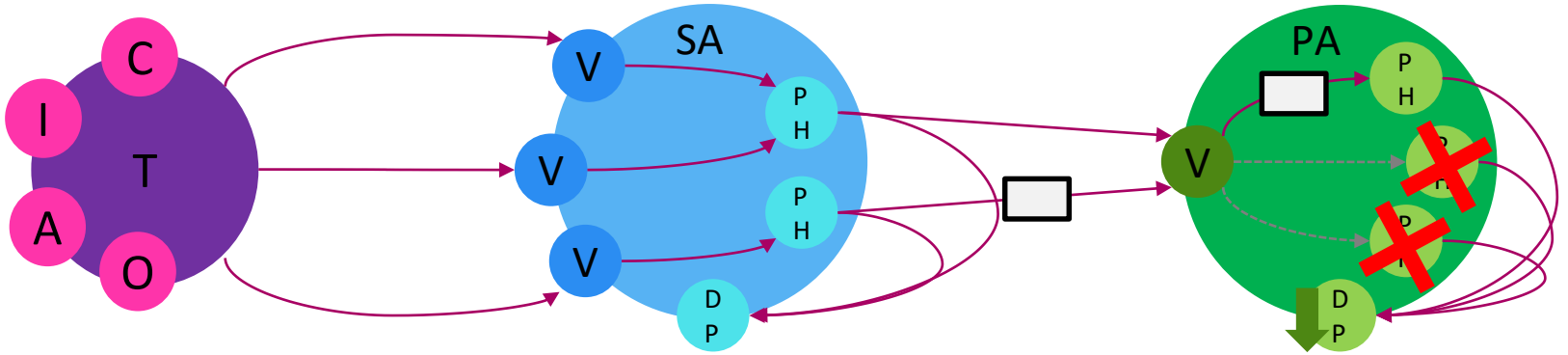


Information Security Management – OSC3

Asset-centric Information Security – Environment V

Information security key-functions:

Reduce value, disablement of information, voiding information and adding resilience on primary assets.



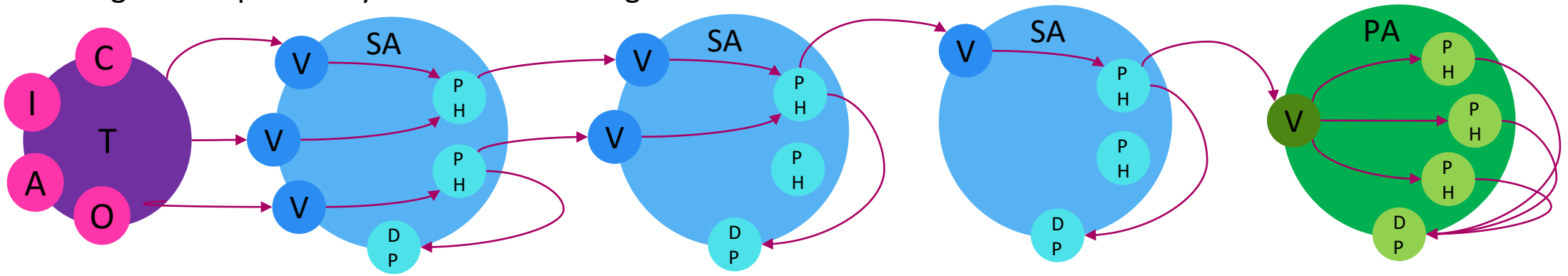
1. Reducing exposure of data by reducing process entanglement, enforcing restricted access, 4-eyes-principle, providing working copies of master data instead master data only.
2. Reduce impact on availability by adding resilience in storage e.g. adding data location resources, offsite/offline backups copies, auto-versioning object storage etc.
3. Remove value from data objects by cyphering contained information.
4. Making data objects inherent integer by lowering the possibility to apply changes to data e.g., by ciphering information contained in data objects.

Information Security Management – OSC3

Asset-centric Information Security – Environment VI

Information security key-functions:

Reducing data exposure by architectural design

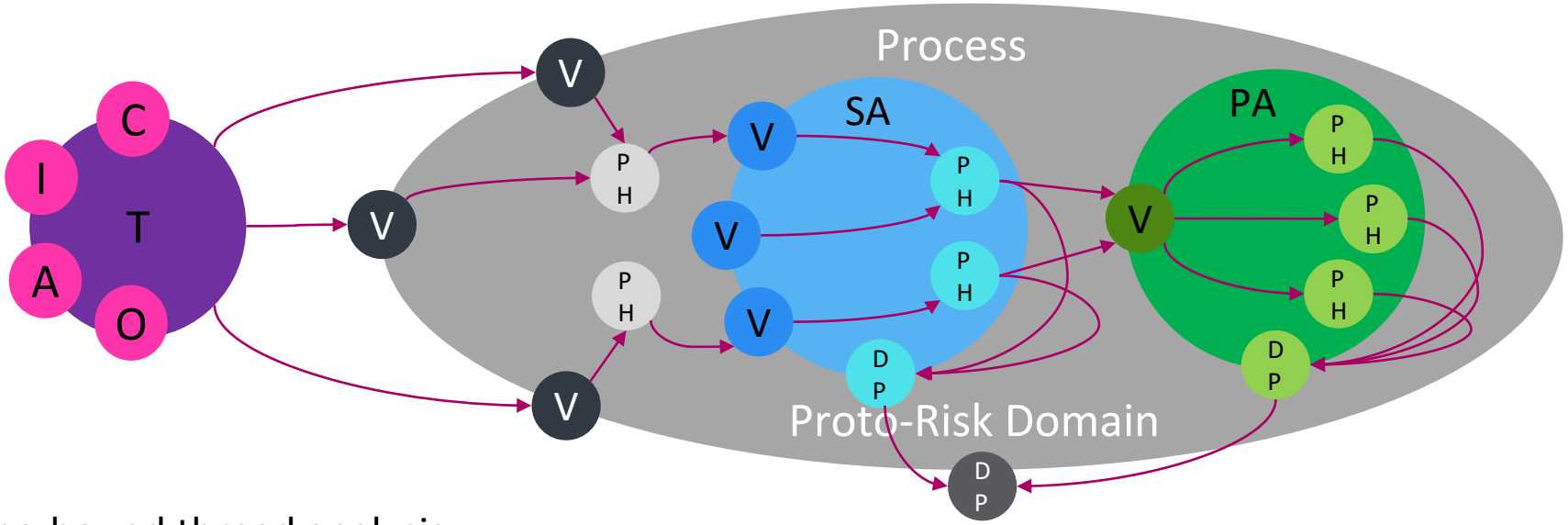


Removing data from highly exposed assets, like webservers, is a practice commonly known as 3-Tier-Principle, where the functionalities “presenter”, “logic” and “data store” are separated from each other.

1. Tier 1: The presenter is fully exposed but is of low value, easy replaceable and holds no data.
2. Tier 2: The logic-engine (code) is only accessed by the presenter, it holds the logic of the application.
3. Tier 3: The data store is only accessible by the logic-engine, it holds the data.

Information Security Management – OSC3

Information Security – Risk Estimation – Environment VII



1. Scope-bound thread analysis
2. Scope-bound potential hazard + vulnerability analysis
3. Scope-bound damage potential analysis
4. Scope-bound proto-risk analysis
   T * (SA DP + PA DP + PR DP) = domain-specific proto-risk

Information Security Management – OSC3
Perspectives & Conclusions

- There is a close to infinite amount of threats existing, detailing must be limited to just fulfill the risk m. process requirements.
  The risk can only be pre-qualified in operational- and tactical-processes at least in the regards of overall damage potential of qualitative risk analysis.
  Staged risk analysis is a solution to the immanent problems of risk analysis, where risk event and risk impact occur in separate knowledge domains.
  With the introduction of scoping and staging of risk-data, competence is aggregated, errors reduced and transparency of risk quality is massively gained.
  The risk can only be quantitative analyzed by obtaining the knowledge of the processes the regarding assets are entangled in.
- As the relationship between vulnerability and potential hazard can be 1:N. More than one potential hazard can become effective, this has a major impact of the damage potential, it could be N times higher than the classically estimated risk.
- States of procedures/processes are vulnerable to state specific threats.
  The impact of a risk is by its nature typically manifold, damage potential is hold by supporting assets, primary assets and processes.
  There is a correlation between process phase and damage potential. Damage potential is typically increasing over process runtime.
  Most vulnerabilities inherent to programs are also inherent to processes for obvious reason.
  Vulnerabilities can be mapped to states of processes and procedures e.g., by flow or timeline.

- Business Processes are designed to cover many threats and counter many proto-risks related to the process and entangled assets.
  It´s of essential importance to identify parallelism of processes to identify the holistic effect of proto-risks.
  Dependencies and interplay between processes and the entanglement of assets is becoming obvious starting from the analysis of the second process.
  Changes to processes and their effects on the associated risk can be instantly mapped.
  Processes introducing process domain native vulnerabilities, e.g., in regards of logic, data flow, interfaces, error accumulation, side channel information leakage, queueing and caching, timing and false assumptions.
  The undesired call for execution of procedures is a vulnerability inherent to processes.
  Intentionally or unintentionally misconfiguration of processes is a threat to processes. (Well known, in the domain of product acquisition (by manipulating requirements) or risk evaluation (by manipulating asset value).)
  To identify the risk, it is of major importance to identify the lifespan and scope of affected asset states therefore it´s of essential importance to identify the heritage of states and data.
  Asset attributes (e.g., states), when once affect by a risk (impact), carry the related compromise with them, passing them onwards on the time line and process flow.
  Scaling concepts like “increasing workload potential” and “parallelization” has an major impact on the risk landscape.
  Potential Hazards are inherent to assets. Related Vulnerabilities can be mitigated or avoided by processes.
  The vulnerability of process states are in a relationship with entangled primary assets.