

KEUZEMODULE *CYBERSECURITY*

WEERBAAR TEGEN CYBERCRIME

Module 1, Wat is cybersecurity en cybercrime?

Workshop 4, Risicoanalyse en -assessment



LEERUITKOMST MODULE 1

Je hebt een fundamenteel begrip van cybersecurity en bent met een risico-bewuste mentaliteit in staat om wet- en regelgeving, risicomanagement en het beheer van cybersecurity toe te passen in een organisatie, zodanig dat daarmee effectief wordt bijgedragen aan het beveiligingsbeleid en risicobeheer binnen organisaties.

Overzicht

Week 1: Risicodenken

- Workshop 1: De wereld van cybercrime
- Workshop 2: Risicodenken en -management
- Workshop 3: Governance van cybersecurity

Week 2: Risicoanalyse

- Workshop 4: Risicoanalyse en -assessment
- Workshop 5: Beveiligingsmaatregelen

Week 3: Challenge en afronding

WAT HEBBEN WE TOT NU TOE GEDAAN?

Governance

In de vorige workshop hebben we de rol en effectiviteit van cybersecurity governance en de functie van 'soft controls' daarin bekeken.

WAARMEE GA JE VANDAAG AAN DE SLAG?

Leeruitkomst workshop

- Je bedenkt en evaluateert voor verschillende casussen de consequenties en de bedreigingen, zodanig dat je de ernst van de initiële risico's inzichtelijk maakt.
- Je presenteert de resultaten op een gestructureerde wijze, zodanig dat de (cyber)risico's bij het management goed worden gecommuniceerd.

HACK-DRIEHOEK

Een hack kan alleen plaatsvinden op het moment dat aan alle drie de voorwaarden voldaan is. Dit kunnen we tevens gebruiken ter verdediging.



KWAADWILLEND

Bron: ENISA - European Union Agency For Cybersecurity

Wie zijn nou dit kwaadwillende die jouw systeem willen aanvallen?

*APT - Advanced Persistent Threat

Georganiseerde misdaad / cybercriminelen

Geld is het grootste en enige motief

Statelijke actoren (state sponsored actors / APT*)

Vaak militaire doelstellingen voor statelijk gewin, zoals spionage, politieke manipulatie, (industriële) sabotage, maatschappelijke ontwrichting (disruption and destruction).

Hacktivists

Hackers met activistische doelstelling. Statelijke actoren schuilen zich ook vaak achter activistische motieven om geen oorlog uit te lokken.

Script kiddies

Vaak eenlingen die mogelijkheden aan het verkennen zijn voor fun en opbouwen van vaardigheden. Kunnen al wel criminale activiteiten zijn.

Insider threats

Ontevreden medewerkers, omkoping van medewerkers, medewerkers met een kwaadwillende motivatie.

KROONJUWELEN

- Wat zijn kroonjuwelen?
- Wat zijn kroonjuwelen die bij Avans liggen?
- Wat zijn kroonjuwelen die bij jouw thuis liggen?
- Op welke manieren kunnen deze kroonjuwelen gestolen worden?

RISICO-ANALYSE

Om goed te begrijpen waar je moet beginnen en wat je moet doen, is een risicoanalyse van de cyberrisico's essentieel.

Vaak de basis van een security standaard of een verplichting vanuit wetgeving.



RISICOANALYSE

Een cyberrisicoanalyse is een structureel proces waarin de aanwezige cyberrisico's in kaart worden gebracht.

Alleen nadat deze risico's geïdentificeerd zijn, is het mogelijk om effectieve maatregelen te definiëren en te begrijpen. De eerste stap dus!

Risico's zijn onzekere gebeurtenissen in de toekomst die invloed kunnen hebben op jouw onderneming.

RISCOANALYSE STAPPENPLAN

1. Bepaal wat je wil beschermen (assetlijst)
2. Identificeer de risico's
3. Analyseer de gevonden risico's (risicoregister)
4. Besluit wat je gaat doen: accepteren, oplossen (of mitigeren), overdragen of stoppen.

WAT IS EEN RISICO?

Een risico is de **kans** dat een bepaalde **gebeurtenis** plaatsvindt met een bepaalde (negatieve) **impact**.

Risico = Kans x Impact (met Kans = Blootstelling x Waarschijnlijkheid)

Kans is de kans dat een kwetsbaarheid (blootstelling) aanwezig is plus de kans dat een kwaadwillende deze benut.

Impact is de ernst van het gevolg van verlies van vertrouwelijkheid, integriteit of beschikbaarheid van data of systeem door de kwaadwillende.

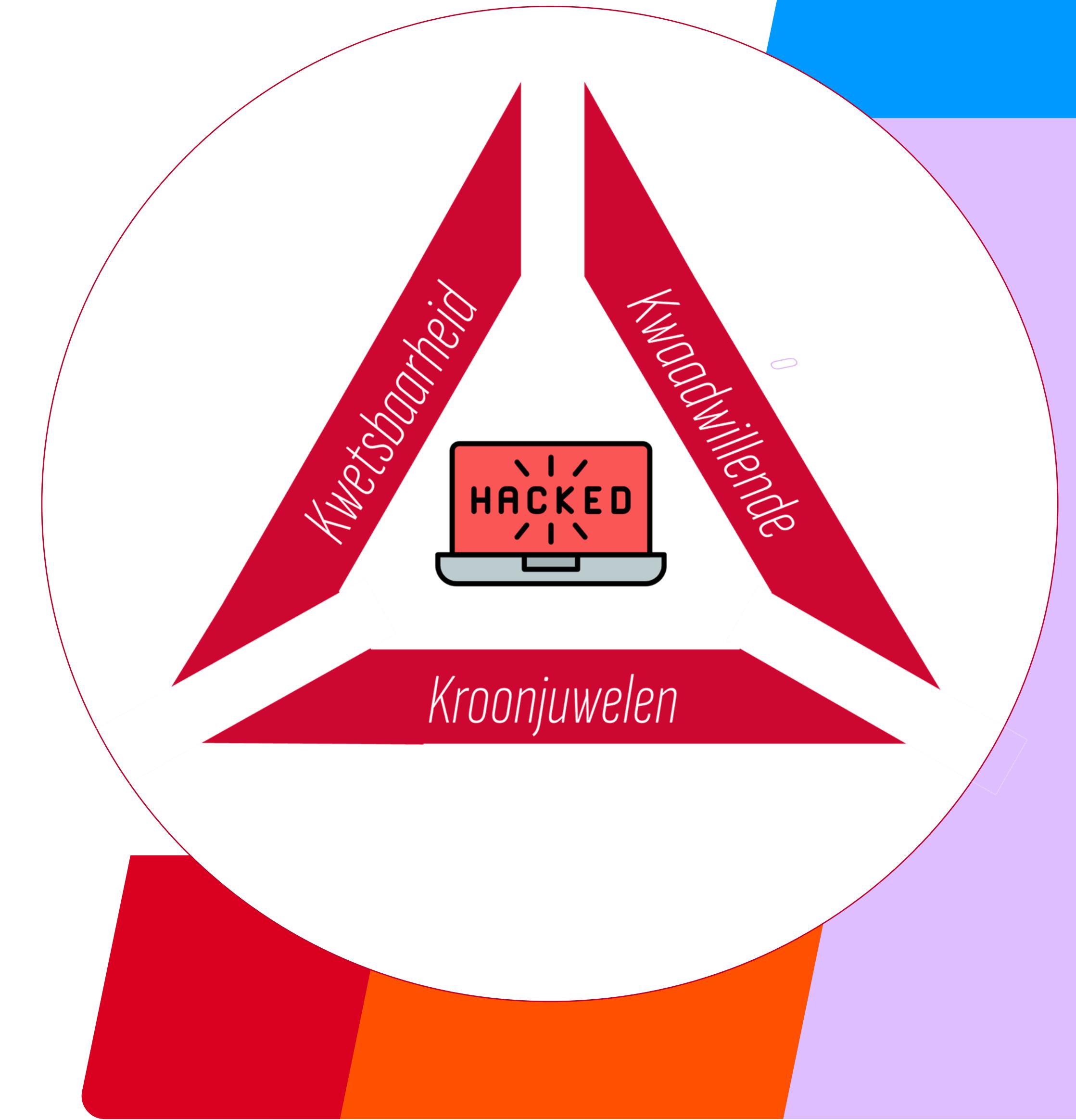
WAT IS EEN RISICOBRON?

Een risicobron (hazard) is een bron van gevaar.

Een gevaar is elke bron van potentiële schade, schade of nadelige gevolgen voor de gezondheid van iets of iemand. Denk aan gevaar voor de gezondheid, van verlies van eigendommen of apparatuur, of voor het milieu.

MET WELKE CYBER RISICO'S HEB JIJ TE MAKEN?

- Welke digitale risico's loop jij privé?
- Wat zijn de risicobronnen?
- Denk hierbij bijvoorbeeld aan je mobiele telefoon, spelcomputer, laptop of Raspberry Pi.



RISICOMATRIX

	Kans				
Impact	Zeer onwaarschijnlijk	onwaarschijnlijk	Mogelijk	Waarschijnlijk	Zeer waarschijnlijk
Onbelangrijk					
Minder ernstig					
Serieus					
Zeer serieus					
Catastrofaal					

Risico prima	Risico acceptabel	Risico te hoog	Risico niet aanvaardbaar
Voor dit risico hoeven geen (extra) maatregelen getroffen worden.	Alleen acceptabel als voor het risico reeds maatregelen zijn getroffen. Bij een initieel geel risico maatregelen treffen.	Risico kan niet worden geaccepteerd. Maatregelen moeten getroffen worden om deze verder te reduceren.	Voor dit risico moet direct maatregelen getroffen worden of het risico dient vermeden te worden als het lastig te mitigeren blijkt.

SECURITYMAATREGELEN (SECURITY CONTROLS)

	Kans				
Impact	Zeer onwaarschijnlijk	onwaarschijnlijk	Mogelijk	Waarschijnlijk	Zeer waarschijnlijk
Onbelangrijk					
Minder ernstig		X'			
Serieus					
Zeer serieus					
Catastrofaal			Kans verlagen		

Impact verlagen

X' X

Risico beheersing:

- Accepteren
- Oplossen (of mitigeren)
- Overdragen
- Ontwijken

Mitigeren:

- Kans reducerende maatregelen
- Impact reducerende maatregelen

RISICOMATRIX KANSEN IMPACT

- Hoe bepaal je de kans?
- Hoe bepaal je de impact?

		Kans				
Impact		Zeer onwaarschijnlijk	onwaarschijnlijk	Mogelijk	Waarschijnlijk	Zeer waarschijnlijk
Onbelangrijk						
Minder ernstig						
Serieus						
Zeer serieus						
Catastrofaal						

RISICOMATRIX IMPACT

- Financiële schade
- Schade aan personen en/of gezondheid
- Reputatieschade
- Schade aan omgeving
- ...

REAL EXAMPLE RISK MATRIX

VERTROUWELIJK – GEBRUIK DEZE NIET ZOMAAR ... MAG WEL ALS GOEDE INPUT!

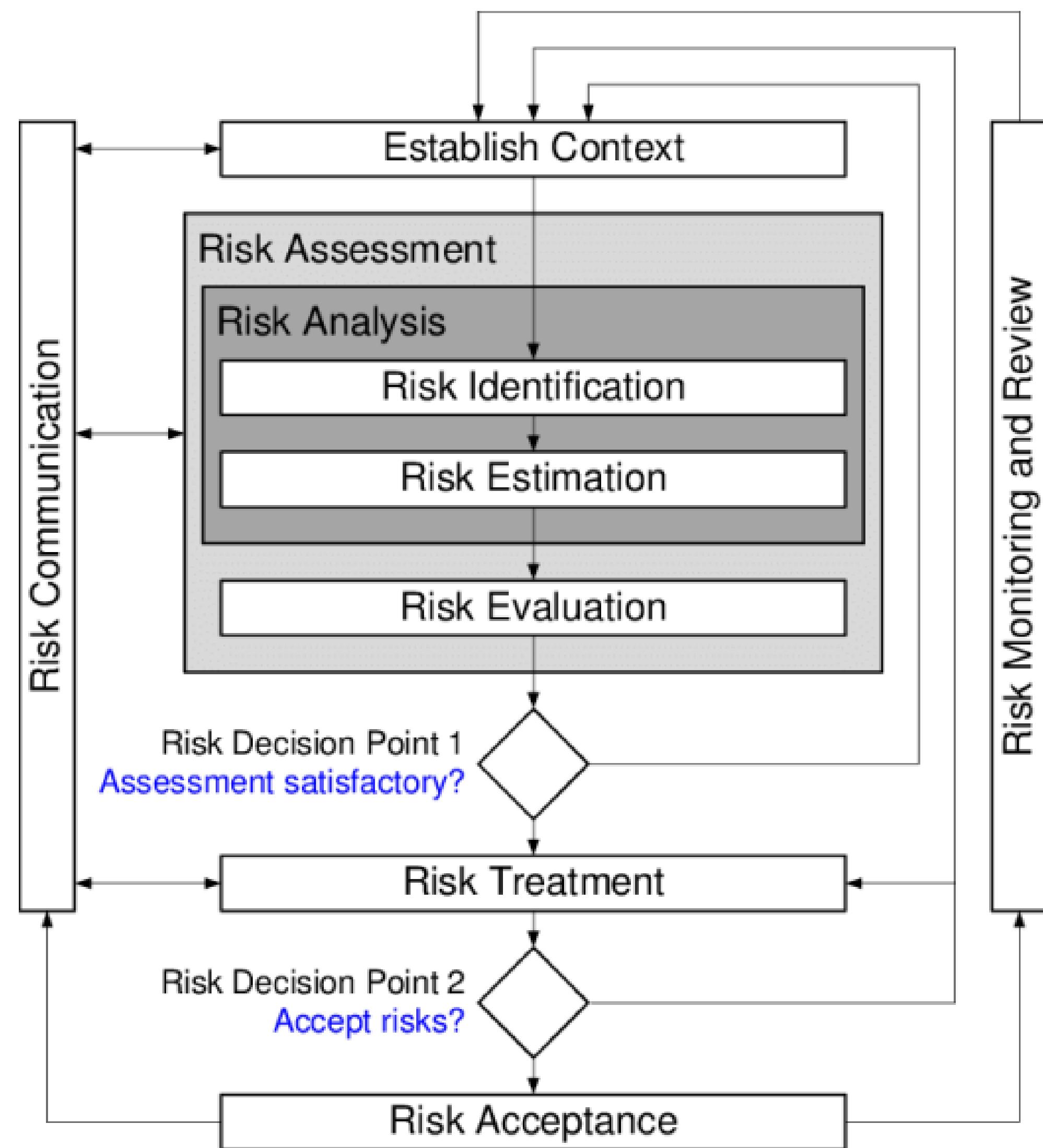
Category	Safety, Health & Wellbeing	Environment	Public Interest	Finance ¹⁾	OT Operational consequences	OT Data Security and OT Data Protection
1 Minor	First aid treatment	No or negligible impact on ecosystems or environmental standards.	No interest	< 10.000 Euro	OT security event, e.g. policy breach, with no immediate impact on operation.	Compromise of information otherwise available in the public domain. Data does not facilitate further exploitation.
2 Limited	Slight injury, medical treatment, temporary adapted work. Full recovery expected.	Minor impact that is mainly localised to the site or having short term impacts. No permit breach.	Local interest	> 10.000 till 100.000 Euro	OT security incident with limited impact on plant operation and no immediate impact on ability to generate.	Compromise of internal information. Data has limited or no security impact on further exploitation.
3 Serious	Serious injury with longer absence.	Moderate impact on local/regional ecosystem component(s) or a significant exceedance of environmental standards or permit breach.	Regional or cross-regional interest	>100.000 till 500.000 Euro	Readily recoverable OT Security incident impacting ability to generate.	Exploited data may, with additional steps, enable attackers to perform activities on the targeted systems and devices.
4 Very serious	Very serious permanent injury, disability	Major impact with medium-term impairment of ecosystem or major exceedance of environmental standards or permit breach with risk of permit being revoked by the regulator. Impact could also be outside the organisation/site.	Nationwide interest	>0,5 million till 10 million Euro ²⁾	Major OT security incident affecting generation output (not immediately recoverable) or report to national authorities is required.	Compromise of confidential information. Exploited data could, without needing to overcome further security controls, enable attackers to perform activities on critical targeted systems and devices.
5 Disastrous	One or more fatalities	Severe impact with long-term impairment of ecosystem or severe exceedance of environmental standards with potential for significant harm to human health or permit breach with permit being revoked by the regulator. Recovery and continued operation is not possible for an indefinite period of time.	International interest	> 10 million Euro	Major OT Security incident affecting safe operation of plant where this could endanger life. Recovery and continued operation is not possible for an indefinite period of time. Report to national authorities is required.	Compromise of (strictly) confidential information. Exploitation of combined data would fundamentally undermine security of affected systems and devices, enable actors to perform significant attacks with minimal effort.

SECURITY STANDAARDEN

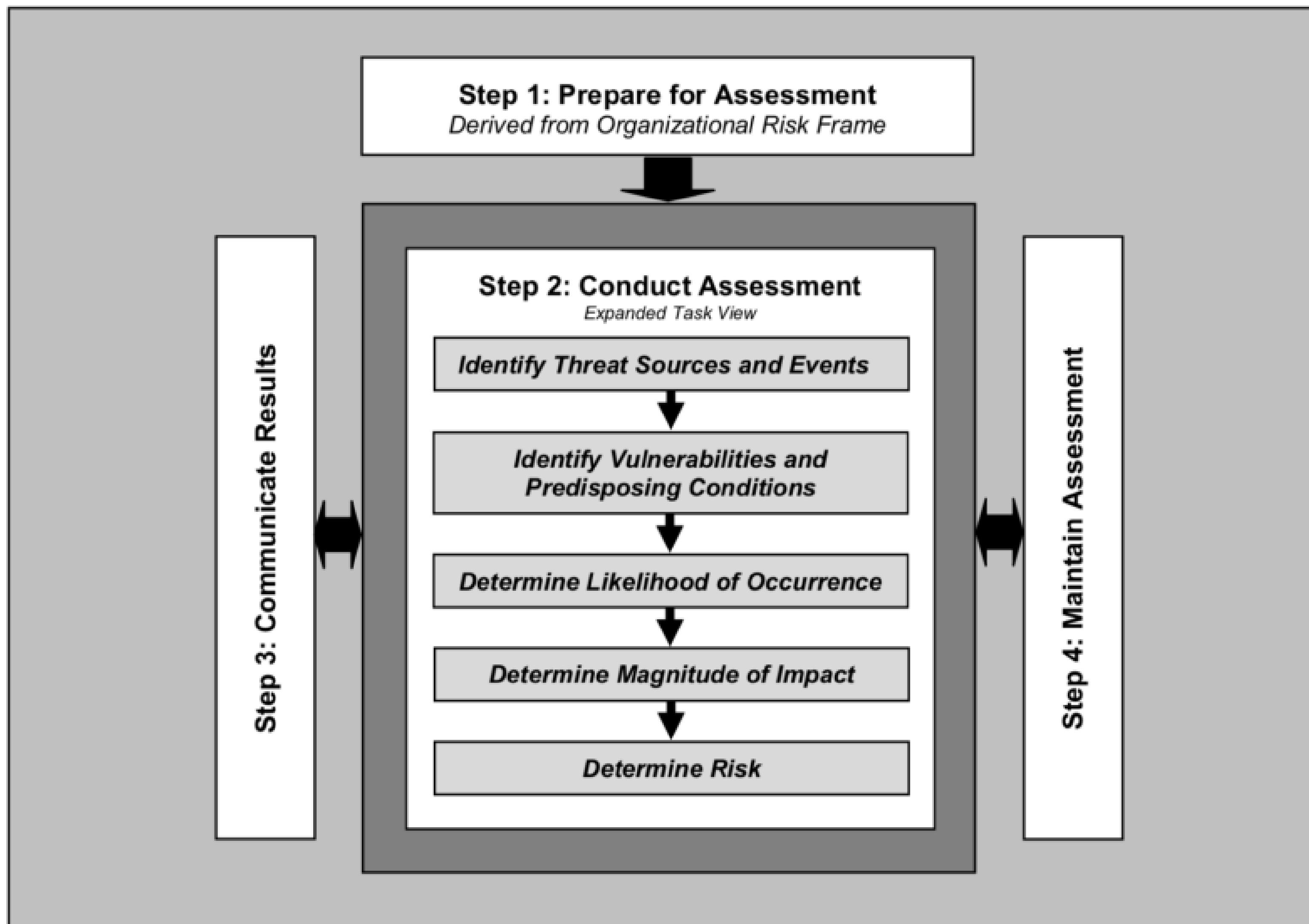
Wat vertellen de standaarden
op het gebied van
risicoanalyse?



ISO/IEC 27005 RISK MANAGEMENT PROCESS



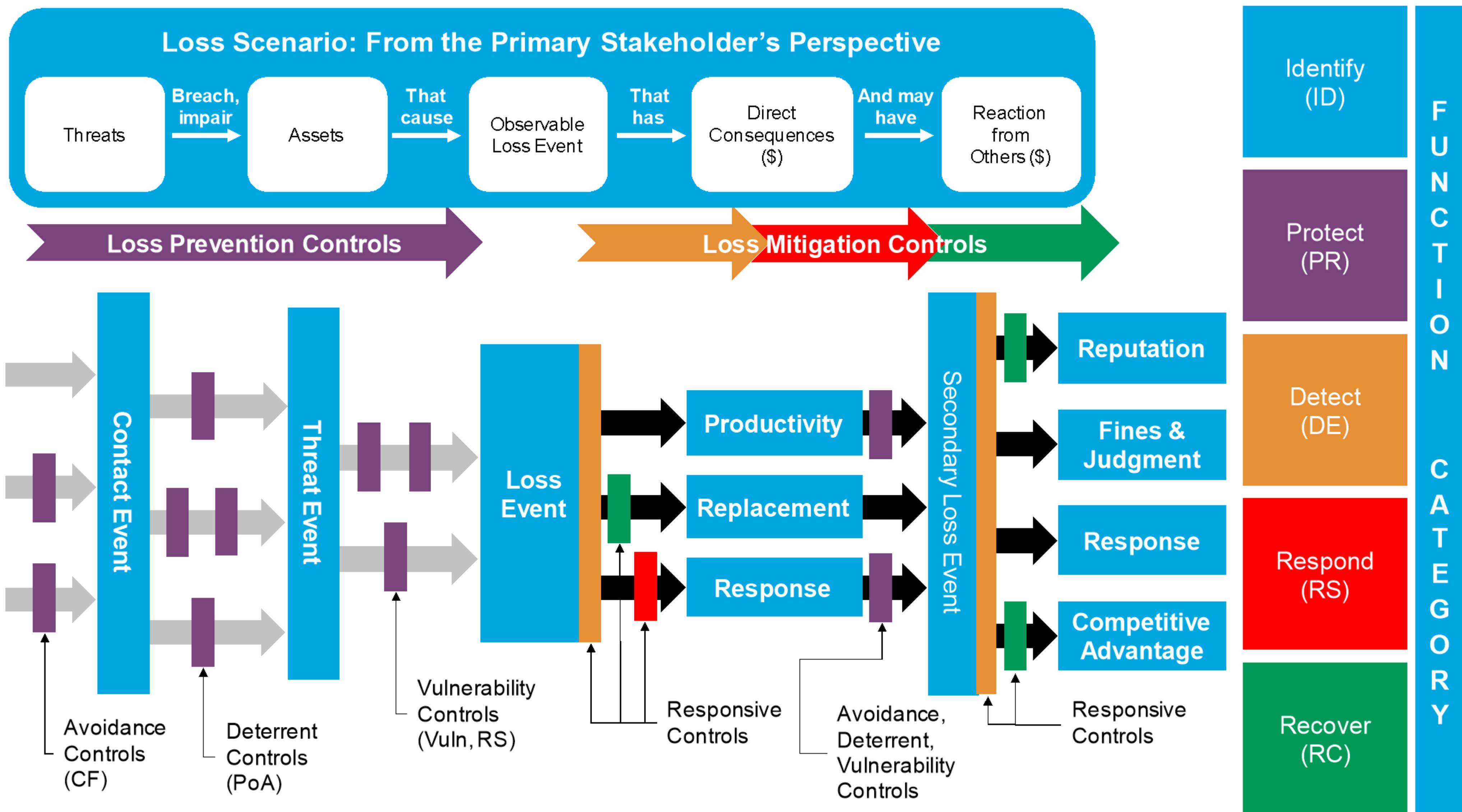
NIST SP-800-30 RISK ASSESSMENT PROCESS



IRAM2 RISK MANAGEMENT METHODOLOGY (ISF)



FAIR (OPENFAIR)



RISICO- ASSESSMENT

Methodiek om de risico's te identificeren en het bepalen van de grootte van het risico (kans x impact).



ISO27005



ID	Description	Position	Likelihood	Impact	Action	Owner	Review Date	Updated
H	Staff member leaks commercial in confidence company or customer information	20	Low	Severe	Terminate	David Kelly	25/01/2022	25/01/2021 17:50
I	Infrastructure critical supplier hosting service goes down	13	Very high	Minor	Tolerate: Residual risk	David Kelly	25/01/2022	25/01/2021 17:43
L	Hacking by normal users due to or allowed through: - inadequate IDAM controls	1	Very low	Insignificant	Tolerate: Residual risk	David Kelly	25/01/2022	25/01/2021 17:43
N	Hacking by outsiders due to or allowed through social engineering and phishing	1	Very low	Insignificant	Treat (Other)	David Kelly	25/01/2022	25/01/2021 17:44
O	Suppliers fail to protect our production data in line with our expectations *	19	Medium	Major	Tolerate: Residual risk	David Kelly	18/03/2021	09/06/2021 10:48

MAPGOOD-MODEL

- In kaart brengen van bedreigingen en risico's op het gebied van informatiebeveiliging om beveiligingsmaatregelen in kaart te brengen
- Verschillende invalshoeken om naar bedreigingen en risico's te kijken
- Belangrijk om elk component zo volledig mogelijk op hoofdniveau te beschrijven
- Verschil aangeven tussen eigen verantwoordelijkheid en uitbesteding aan externe partij (dienst)

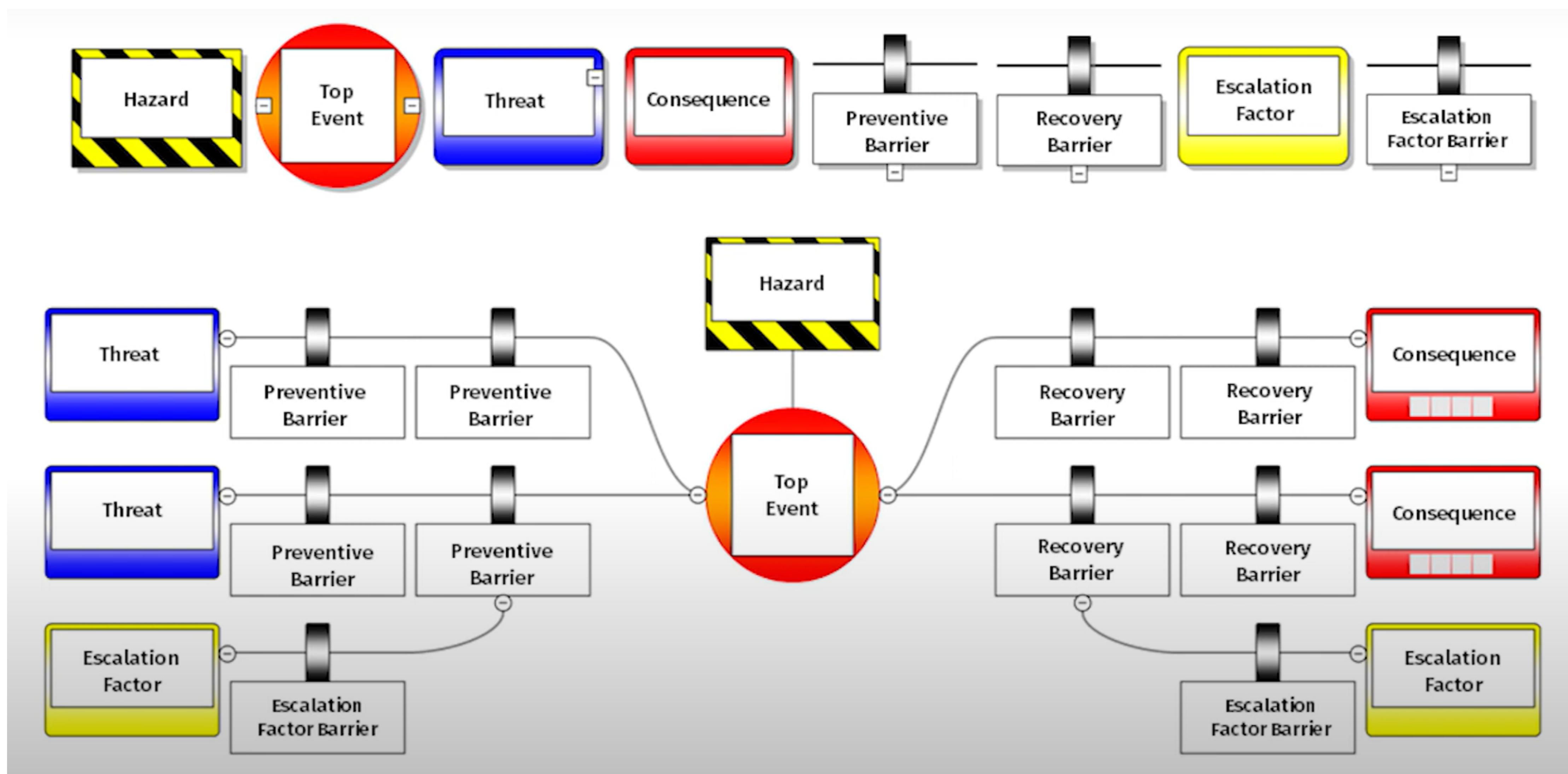
MAPGOOD-MODEL / INVALSHOEKEN

- **Mens** - mensen die nodig zijn om het informatiesysteem te beheren en gebruiken (directe/indirecte gebruikers en functioneel en technisch applicatiebeheer).
- **Apparatuur** - apparatuur die nodig is om het informatiesysteem te laten functioneren (webserver, applicatieserver, beheer van werkplekken, ...).
- **Programmatuur** - programmatuur waaruit het informatiesysteem bestaat.
- **Gegevens** - gegevens die door het systeem worden verwerkt.
- **Organisatie** - organisatie die nodig is om het informatiesysteem te laten functioneren (beheer-, gebruikers- en ontwikkelorganisaties).
- **Omgeving** - omgeving waarin het informatiesysteem functioneert (locatie, datacenter, werkplekken, ...).
- **Diensten** - externe diensten die nodig zijn om het systeem te laten functioneren (technisch systeembeheer, clouddiensten, infrastructuur, (onderhouds)contracten).

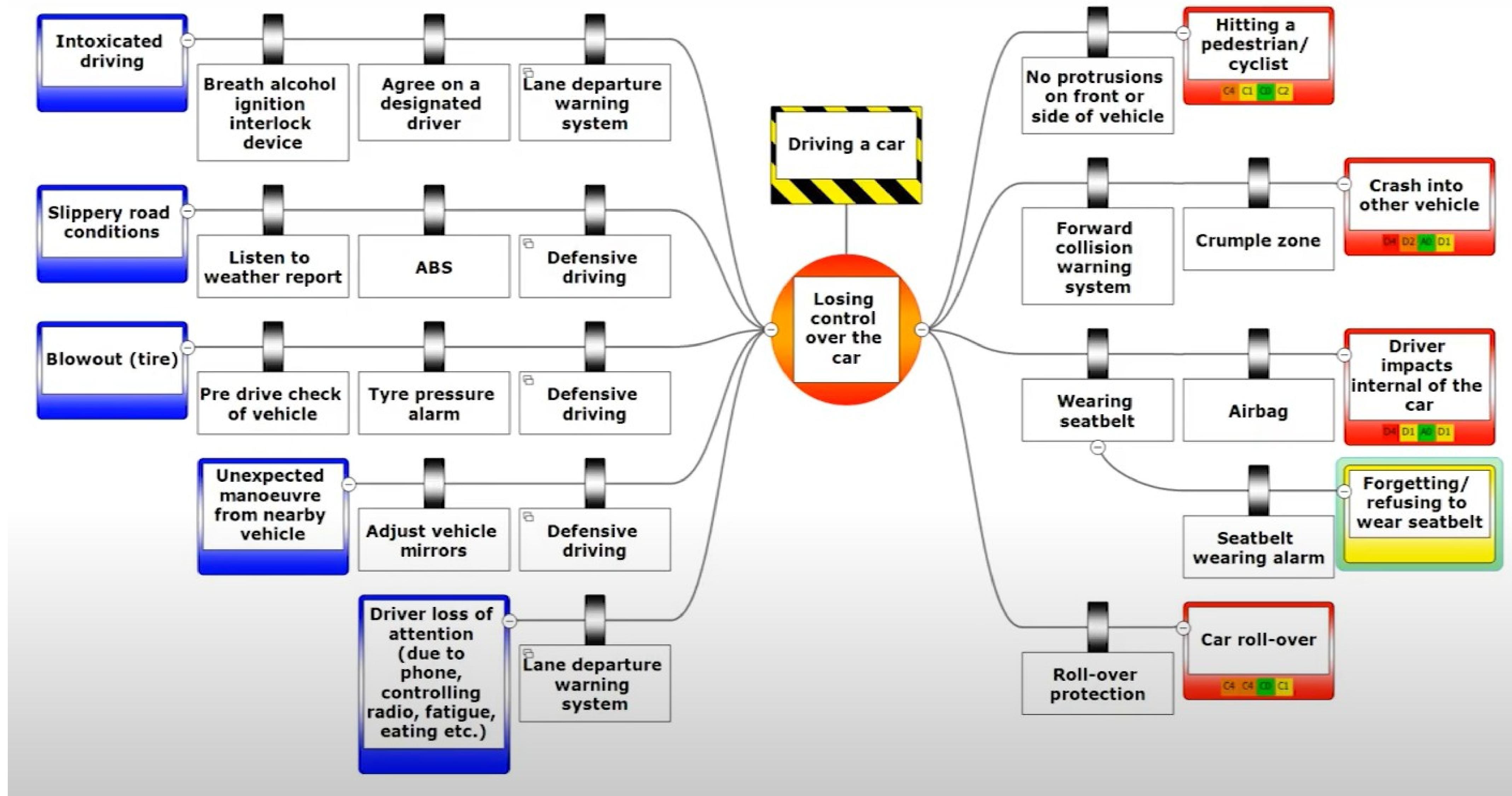
MAPGOOD-MODEL / PROCES

1. Elk component zo volledig mogelijk beschrijven
2. Inventariseren van de risico's en bedreigingen
3. Per onderdeel bepalen wat de kans op optreden is en welke impact daarbij hoort (vaststellen van het risico)
4. Bepalen hoe per vastgesteld risico wordt omgegaan om de dreigingen het hoofd te bieden:
 - **Vermijden** - Het risico vermijden door maatregelen te nemen
 - **Verminderen** - Het risico verminderen door alternatieve maatregelen te nemen
 - **Overdragen** - Overdragen van het risico aan een andere partij
 - **Accepteren** - Geen van eerder genoemde manieren lukt niet, zodoende accepteer je het risico en neem je geen maatregelen

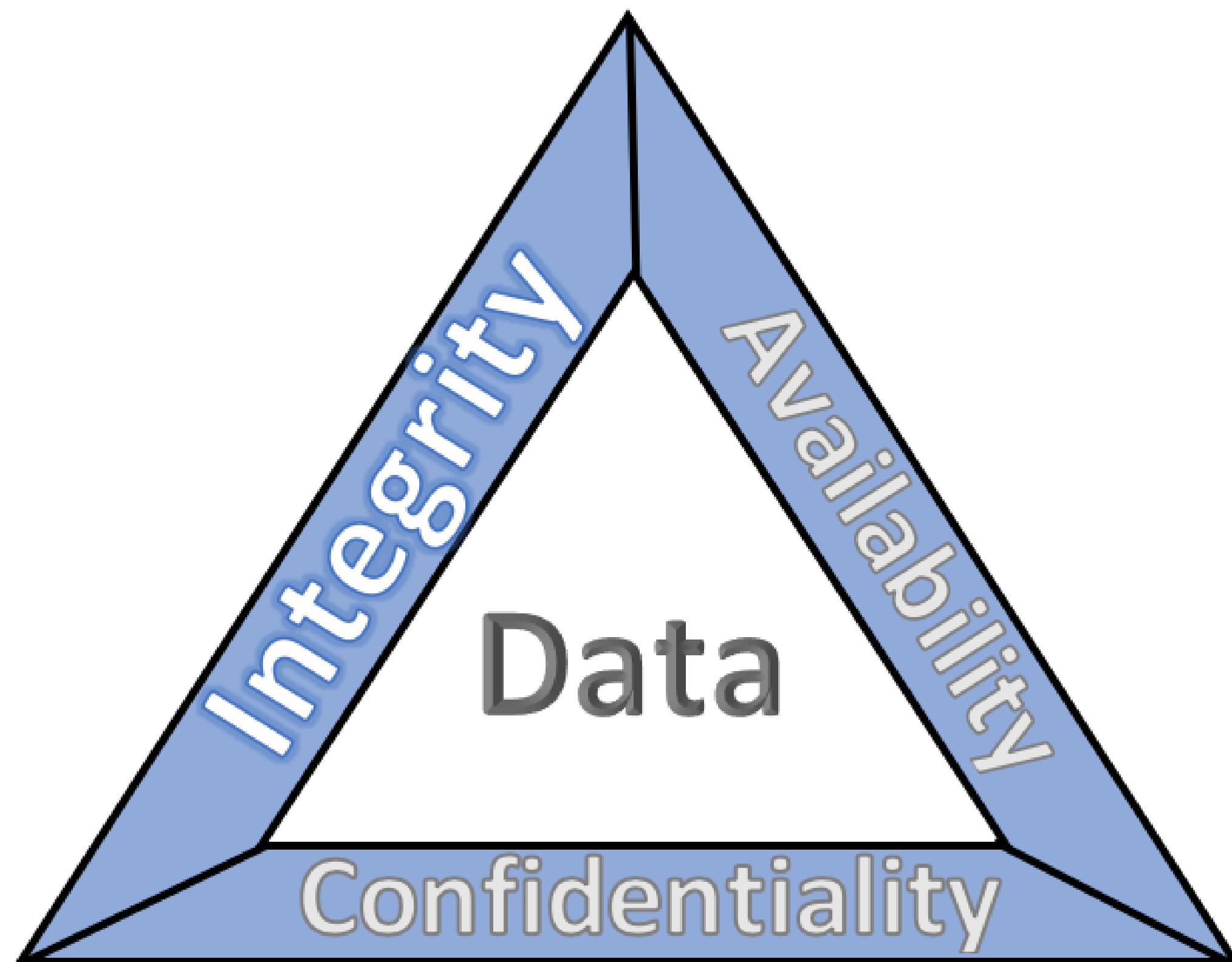
BOW-TIE



BOW-TIE



SECURITYDRIEHOEK MODEL

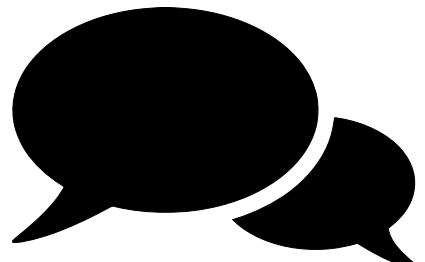


BOW-TIE EXAMPLE – YOUR LAPTOP

UNAUTHORIZED ACCESS

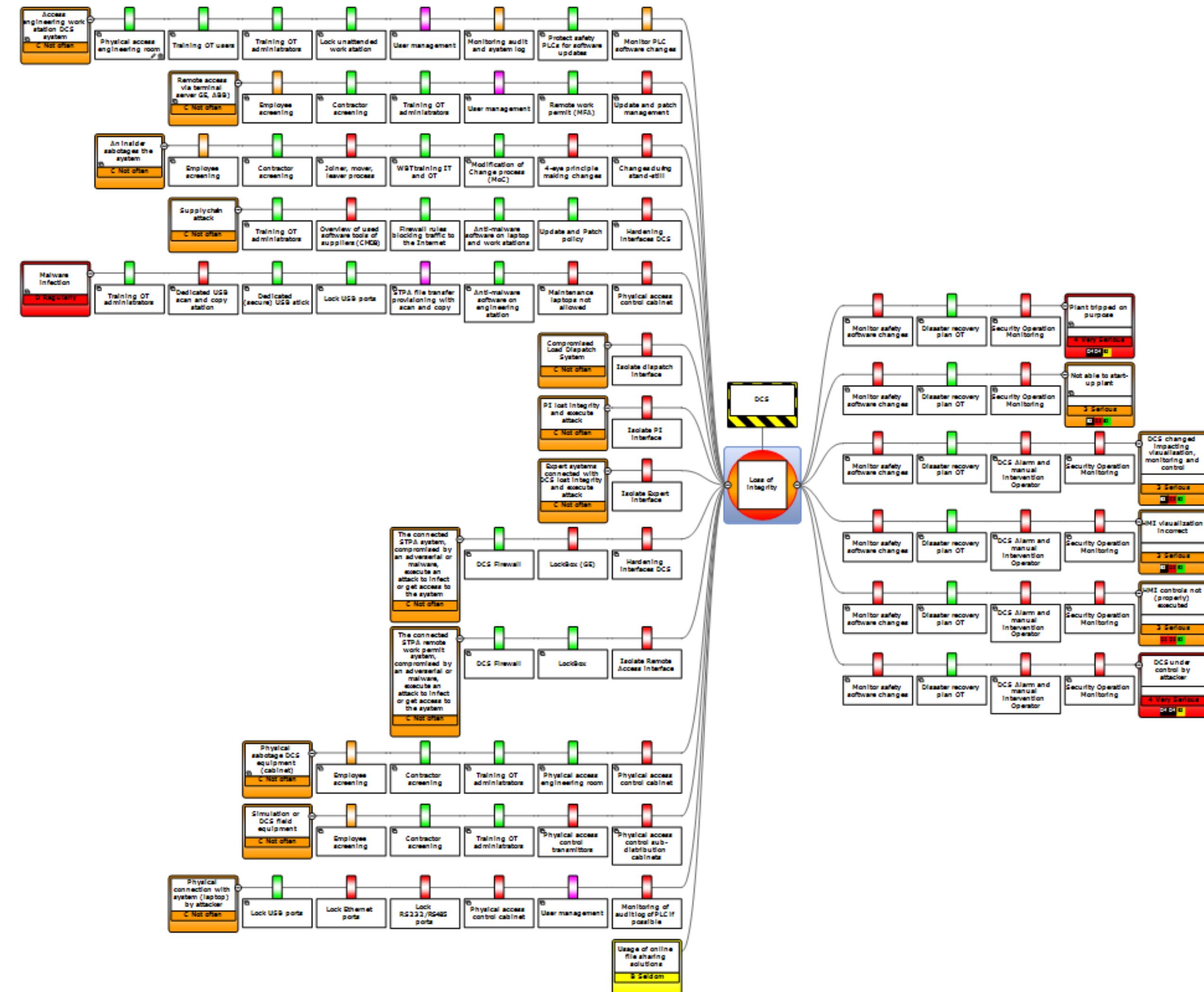


Loss of integrity, availability and
confidentiality



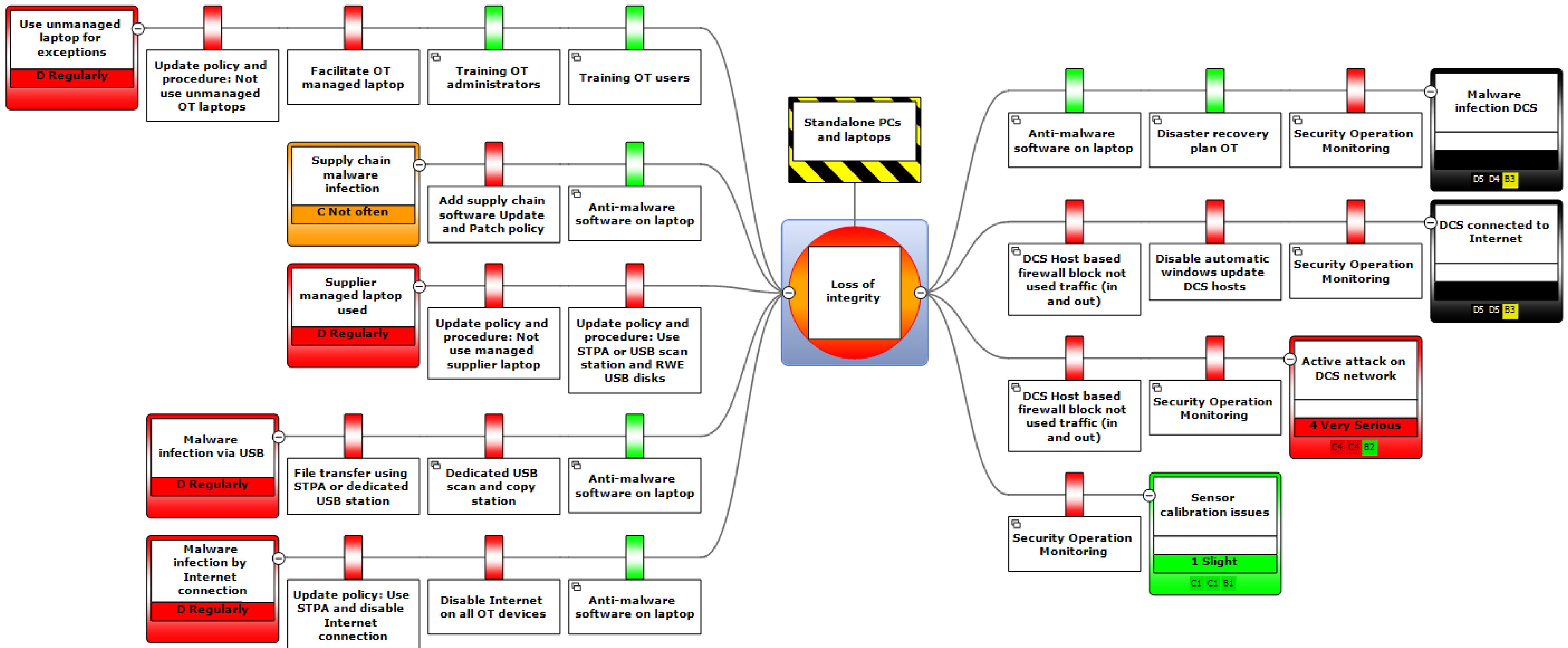
REAL EXAMPLE BOW-TIE FOR POWER STATION

VERTROUWELIJK



REAL EXAMPLE BOW-TIE

CONFIDENTIAL



IT VERSUS OT

Security vs Safety

Information Technology (IT) vs
Operational Technology (OT)

Jezelf hierin verdiepen is
onderdeel van de opdracht.

Stuxnet: <https://www.youtube.com/watch?v=7g0pi4J8auQ>
Generator attack: <https://www.youtube.com/watch?v=9pkDmvF8C2A>,
<https://www.youtube.com/watch?v=fJyWngDco3g>



SAMENVATTING

- Hack-driehoek: Kwetsbaarheid, Kwaadwillende en Kroonjuwelen
- Type kwaadwillende
- Risicoanalyse
- Risicobron
- Risicomatrix
- Risicoassessment
- IT versus OT

OPDRACHT

Je gaat met je projectgroep aan de slag met deze opdracht. Volgende workshop geven een aantal projectgroepen een presentatie van het resultaat aan de klas.





OPDRACHT A

Werk de volgende vragen uit met de projectgroep. Verdiep je in het onderwerp door bronnen te raadplegen. Je mag het werk verdelen, maar zorg dat je de kennis met elkaar deelt en discussies voert over het resultaat. Maak een plan van aanpak, want de tijd is beperkt! Leg het resultaat vast in je portfolio.

1. Zoek échte voorbeelden op het Internet (bijv. nieuwsbronnen en rapporten) van aanvallen van de verschillende typen kwaadwillenden.
2. Maak een risicomatrix waarbij je een eigen invulling maakt van de verschillende impact niveaus. Zorg dat je hier verschillende invalshoeken meeneemt.
3. Formuleer een antwoord op welke manier je de kans van risico's kan beoordelen. Werk dit uit aan de hand van een eigen gekozen voorbeeld.
4. Voer een literatuuronderzoek uit om een lijst van de meest bekende kwetsbaarheden (vulnerabilities) en bedreigingen (threats) op te stellen die je kan gebruiken tijdens een risicoassessment.

OPDRACHT B

!!Bedenk nu nog geen maatregelen!!

Werk alleen de consequenties en bedreigingen uit



Werk de volgende vragen uit met de projectgroep. Zorg dat je de kennis met elkaar deelt en discussies voert over het resultaat.

1. Verdiep jezelf in IT en OT en maak een presentatie waarin je goed laat zien wat de verschillen zijn en wat belangrijke aspecten zijn waar je op moet letten.
2. Zoek verschillende definities van wat IT systemen en wat OT systemen zijn. Beargumenteer welke je het beste te hanteren vindt en waarom. Kan je in één zin uitleggen wat het verschil is?
3. Verdiep je in de genoemde standaarden voor risicoanalyse. Maak een vergelijking en beargumenteer op welke wijze je de risicoanalyse en risicoassessment uit gaat voeren. Beschrijf op één A4 hoe je dit bij een bedrijf zou doen.
4. Verdiep je in de bow-tie methodiek en realiseer één bow-tie diagram op basis van een casus (zie volgende sheet), waarbij één top event "Loss of Control" wordt genomen. Hierbij neem je de driehoek mee: verlies van integriteit, vertrouwelijkheid en beschikbaarheid. Schrijf al de aannames op die je doet.

⁴⁴Let op: Dit resultaat is input voor de volgende opdracht!

OPDRACHT C

!!Bedenk nu nog geen maatregelen!!

Werk alleen de consequenties en bedreigingen uit



Je mag een eigen casus van een applicatie bedenken met de projectgroep om de bow-tie uit te voeren. Zorg dat je de casus zo goed mogelijk beschrijft. Je kan ook kiezen uit de volgende casussen A of B. **Werk deze casus dan wel verder uit met de groep.**

Maak een ontwerp van de applicatie en een assetlijst. Duik de standaarden in om ideeën te krijgen over bedreigingen. Ga gestructureerd te werk. Discussieer met elkaar en werk de volgende opdrachten uit:

1. Realiseer eerst een risico matrix die je gaat gebruiken.
2. Welke consequenties kunnen er voor de organisatie, gebruikers, klanten en/of maatschappij zijn als over deze applicatie de controle verliezen (denk aan integriteit, vertrouwelijkheid en beschikbaarheid). Maak een pakkende titel en beschrijf de consequentie. Bepaal met elkaar de impact van de consequenties.
3. Welke bedreigingen zijn er waardoor de controle van de applicatie verloren kan worden. Denk hierbij aan fysieke en digitale dreigingen. Maak een pakkende titel en beschrijf de bedreiging. Bepaal met elkaar de kans van deze bedreiging en onderbouw dat.
4. Reflecteer met elkaar of je de opdracht moeilijk of makkelijk vond en onderbouw dat. Zijn er verbetermogelijkheden?



CASUSA

Energiecentrale

Een energiecentrale heeft een regelsysteem van een bepaalde leverancier. Met deze software wordt de centrale bewaakt en bedient. Deze leverancier wil op afstand hulp kunnen bieden wanneer er problemen zijn. Deze remote toegang is gerealiseerd met een webportal waarbij de leverancier na het inloggen op een jumphost terecht komt. Via de jumphost kan de leverancier administratieve taken uitvoeren aan het systeem.

Maak drie bow-tie diagrammen voor deze remote toegang (hazard), waarbij je bekijkt dat deze applicatie de beschikbaarheid, integriteit of vertrouwelijkheid verliest (top events).

Zorg dat je de kansen en impact bepaald. Gebruik je risicomatrix en lijst van bekende kwetsbaarheden en bedreigingen. Maak een top 10 risico register.



CASUS B

Huisartsenpraktijk

Een huisartsenpraktijk gebruikt een elektronisch patiënten dossier systeem. Hierin staan de persoonlijke gegevens, afspraken, medicijnen en metingen van de patiënten van de praktijk. De systeem is beschikbaar via het Internet in een browser en wordt door een organisatie beheert.

Maak drie bow-tie diagrammen voor dit elektronisch patiënten dossier systeem (hazard), waarbij je bekijkt dat deze applicatie de beschikbaarheid, integriteit of vertrouwelijkheid verliest (top events).

Zorg dat je de kansen en impact bepaald. Gebruik je risicomatrix en lijst van bekende kwetsbaarheden en bedreigingen. Maak een top 10 risico register.

DEFINITIES

Or

love
ness;
beloved
or address
one;
gual person regards
or greeting
greetings;

KWETSBAARHEID (VULNERABILITY)

A **Vulnerability** is something open to attack or misuse that could lead to an undesirable outcome. If the vulnerability were to be exploited it could lead to an impact on a process or system. Vulnerabilities can be diverse and include technology (e.g., a software interface being vulnerable to invalid input), people (e.g., a business is vulnerable to a lack of human resources), legal (e.g., databases being vulnerable and linked to large legal fines if data is mishandled and exposed) etc.

[CyBok]

BEDREIGING (THREAT)

A **Threat** is an individual, event, or action that has the capability to exploit a vulnerability. Threats are also socio-technical and could include hackers, disgruntled or poorly trained employees, poorly designed software, a poorly articulated or understood operational process etc.

To give a concrete example that differentiates vulnerabilities from threats - a software interface has a vulnerability in that malicious input could cause the software to behave in an undesirable manner (e.g., delete tables from a database on the system), while the threat is an action or event that exploits the vulnerability (e.g., the hacker who introduces the malicious input to the system). [CyBok]

KANS (LIKELIHOOD)

Likelihood represents a measure capturing the degree of possibility that a threat will exploit a vulnerability, and therefore produce an undesirable outcome affecting the values at the core of the system. This can be a qualitative indicator (e.g., low, medium, high), or a quantitative value (e.g., a scale of 1-10 or a percentage). [CyBok]

GEVOLG (IMPACT)

Impact is the result of a threat exploiting a vulnerability, which has a negative effect on the success of the objectives for which we are assessing the risk. From a systems view this could be the failure to manufacture a new product on time, while from a component view it could be the failure of a specific manufacturing production component. [CyBok]

avans
hogeschool

BRONNEN



BRONNEN

1. Zie Bibliotheek op Brightspace
2. https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf
3. <https://www.informatiebeveiligingsdienst.nl/product/handreiking-diepgaande-risicoanalyse-methode-gemeenten/>
4. https://www.bio-overheid.nl/media/13kduksi/bio-versie-104zv_def.pdf
5. <https://www.wolterskluwer.com/en/expert-insights/managing-cyber-security-risks-using-bowties>