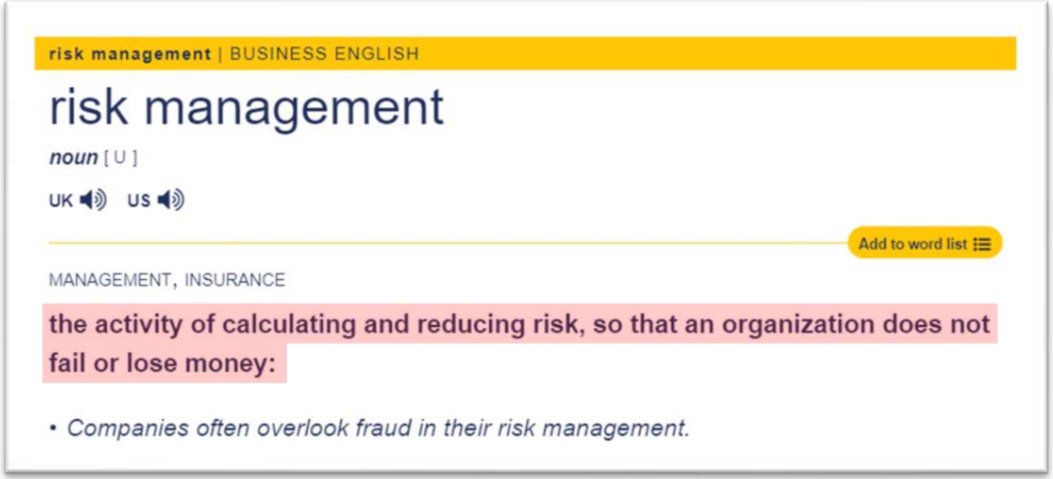
OT security at Enexis

Using bowties for the management of digital risks

Philip Westbroek
OT security officer | risk manager

23 April 2024

ENEXIS



risk management | BUSINESS ENGLISH

risk management

noun [U]

MANAGEMENT, INSURANCE

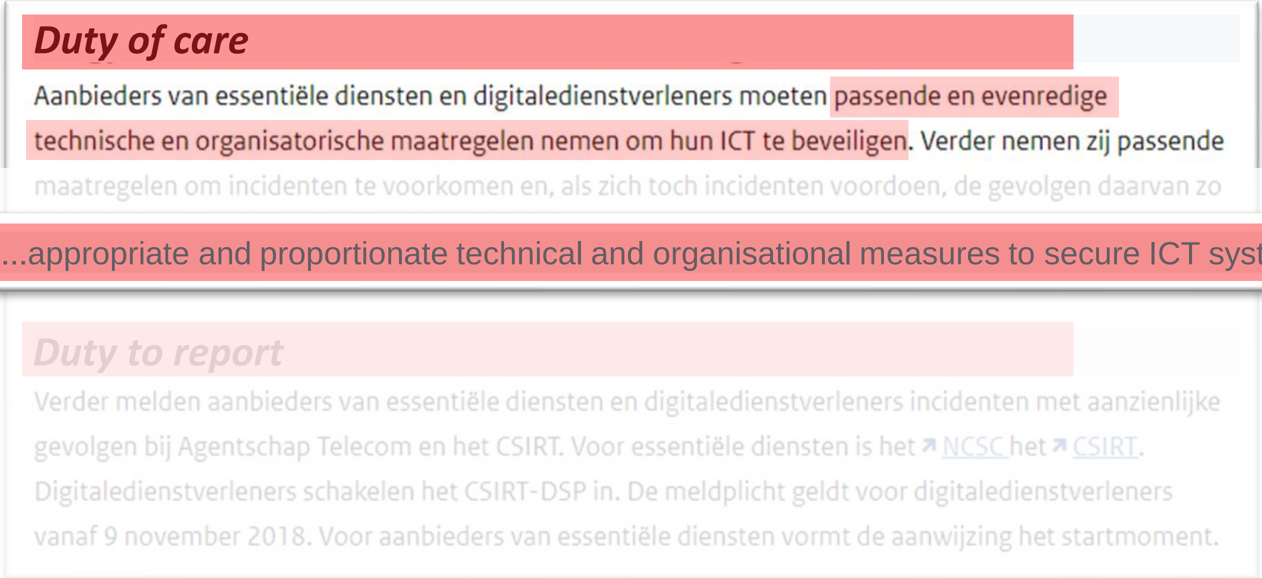
the activity of calculating and reducing risk, so that an organization does not fail or lose money:

- *Companies often overlook fraud in their risk management.*

'Wet beveiliging netwerk- en informatiesystemen' - Wbni

Dutch implementation of the EU NIS directive

Dutch Authority for Digital Infrastructure
Ministry of Economic Affairs and Climate Policy



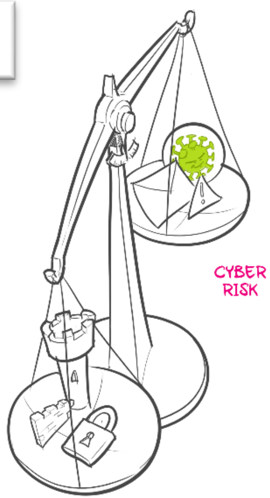
Duty of care

Aanbieders van essentiële diensten en digitaledienstverleners moeten passende en evenredige technische en organisatorische maatregelen nemen om hun ICT te beveiligen. Verder nemen zij passende maatregelen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo

...appropriate and proportionate technical and organisational measures to secure ICT systems.

Duty to report

Verder melden aanbieders van essentiële diensten en digitaledienstverleners incidenten met aanzienlijke gevolgen bij Agentschap Telecom en het CSIRT. Voor essentiële diensten is het ↗ NCSC het ↗ CSIRT. Digitaledienstverleners schakelen het CSIRT-DSP in. De meldplicht geldt voor digitaledienstverleners vanaf 9 november 2018. Voor aanbieders van essentiële diensten vormt de aanwijzing het startmoment.



How do I know what is appropriate and proportionate ?

This is what risk management is all about

- The answer to that question depends on a number of factors, e.g.:
  - Which industry you are active in;
  - What is your own risk appetite;
  - Commercial vs. regulated industry;
  - With digital risks: are you evaluating IT or OT systems;
  - What is your resilience against attacks;
  - What is the importance of the processes, systems etc. you are investigating during your risk assessment.

vs.

- The costs of mitigating controls should not outweigh the potential impact of a risk:
  - This doesn't just apply to financial costs;
  - Find the balance between digital security, physical security, costs, user friendliness etc.

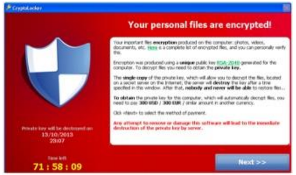
Risk appetite formalised by the board of directors

A company's risk appetite is typically documented in a risk matrix

- Risk needs to be quantified where possible:
  - Risk = **Threat * Vulnerability * Impact**

*

*



CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click <Next> to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
13/10/2013
23:07

Time left
71 : 58 : 09

  - The number of threats and vulnerabilities defines the likelihood that something goes wrong;
  - Most companies use the following risk equation: Risk = **Likelihood * Impact**;
  - In this example, the values could vary from 1 (low) to 3 (high), thus resulting in a risk level of 1 to 9;
  - Risks can have a financial impact, but might also affect company values like safety or reliability;
  - Most important is to have a consistent, repeatable approach to quantifying risk;
  - The exact value of individual risks is less important, as long as they can be compared to each-other.

			Likelihood	
		Low (1)	Medium (2)	High (3)
Impact	High (3)	Low (3)	Medium (6)	High (9)
	Medium (2)	Low (2)	Medium (4)	Medium (6)
	Low (1)	Low (1)	Low (2)	Low (3)

- A risk matrix defines the framework for risk mitigation decisions:
  - When to accept, reduce, transfer or avoid the risk;
  - A company's risk appetite is documented in the risk matrix; e.g. which risk levels can be accepted.

Risk appetite formalised by the board of directors

The Enexis Netbeheer risk matrix

Likelihood

Low → High

Impact: High ↑ Low

Impact	Nearly impossible	Exceptional	Seldom	Incidental	Yearly	Monthly	Daily
Very serious	L	M	H	ZH	O	O	O
Serious	V	L	M	H	ZH	O	O
Significant	V	V	L	M	H	ZH	O
Moderate	V	V	V	L	M	H	ZH
Limited	V	V	V	V	L	M	H

Risk level

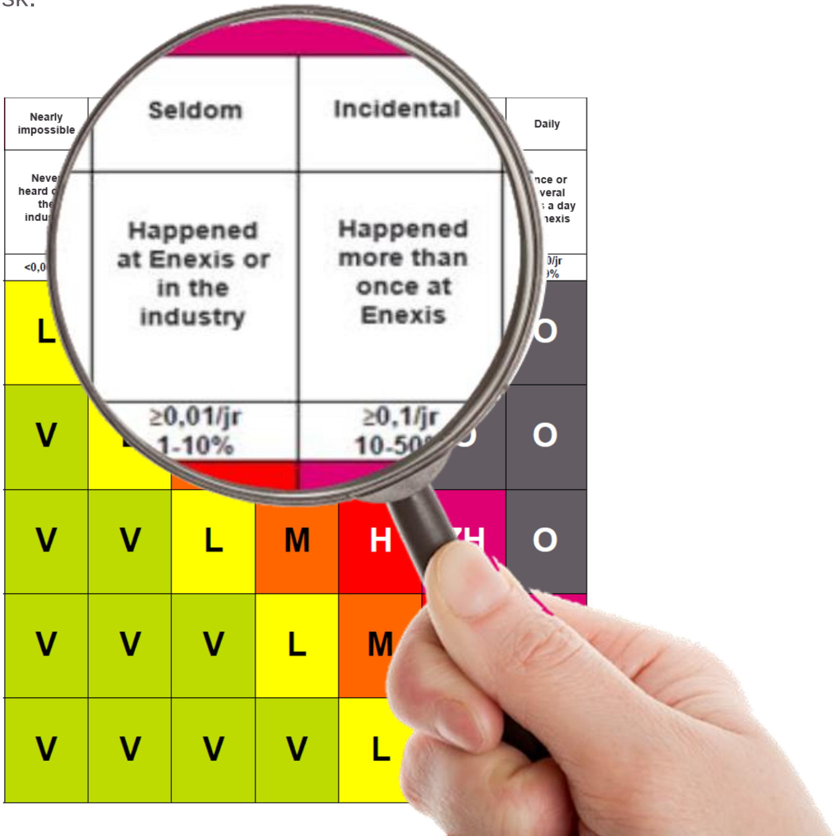
O	Unacceptable
ZH	Very High
H	High
M	Medium
L	Low
V	Negligible

Risk appetite formalised by the board of directors

The Enexis Netbeheer risk matrix

One example of a company value that might be affected by a risk.

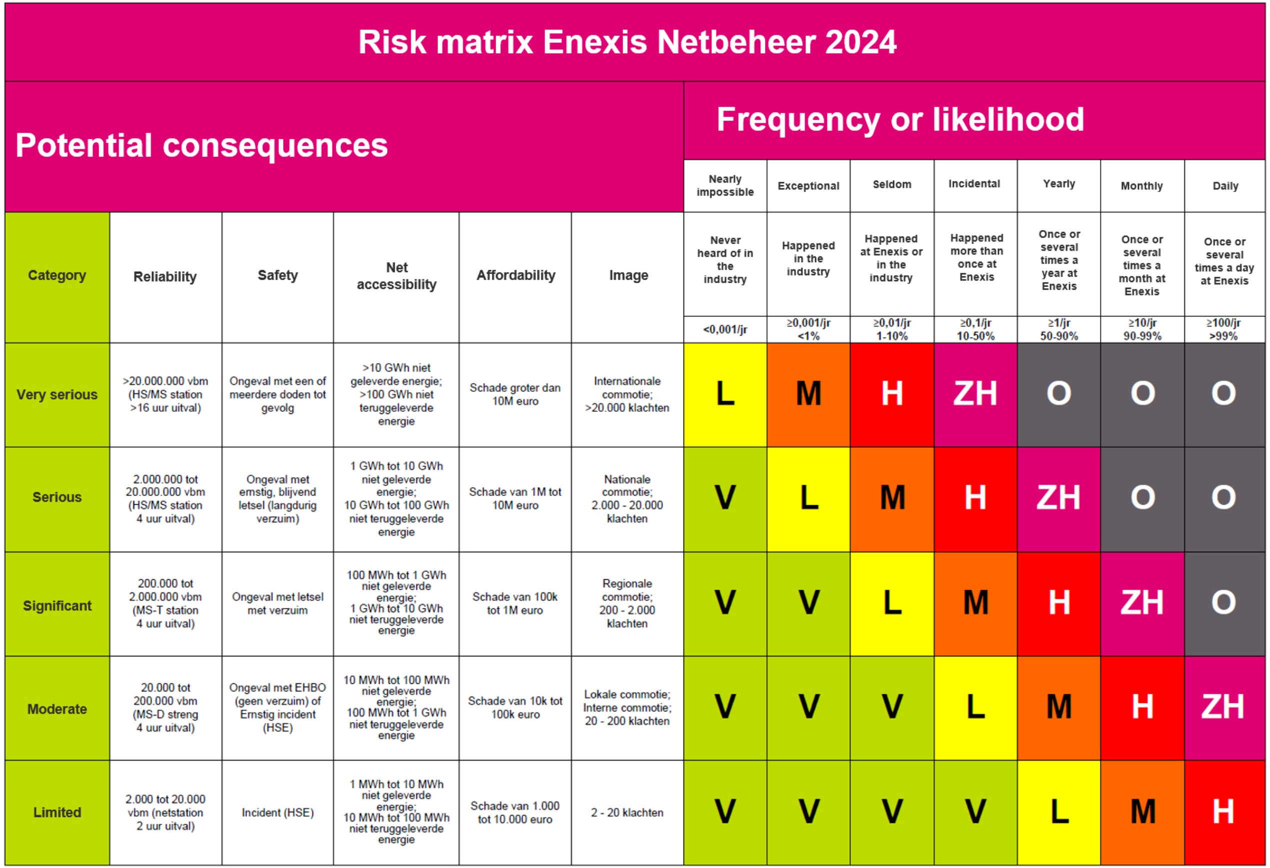
	Affordability	Nearly impossible						Daily
		Neve heard o the indu						nce or veral a day nexis
		<0,0						0/jr 0%
Very serious	Schade groter dan 10M euro	L						O
Serious	Schade van 1M tot 10M euro	V	L				O	O
Significant	Schade van 100k tot 1M euro	V	V	L	M	H	VH	O
Moderate	Schade van 10k tot 100k euro	V	V	V	L	M		
Limited	Schade van 1.000 tot 10.000 euro	V	V	V	V	L		



Seldom	Incidental
Happened at Enexis or in the industry	Happened more than once at Enexis
≥0,01/jr 1-10%	≥0,1/jr 10-50%

Risk appetite formalised by the board of directors

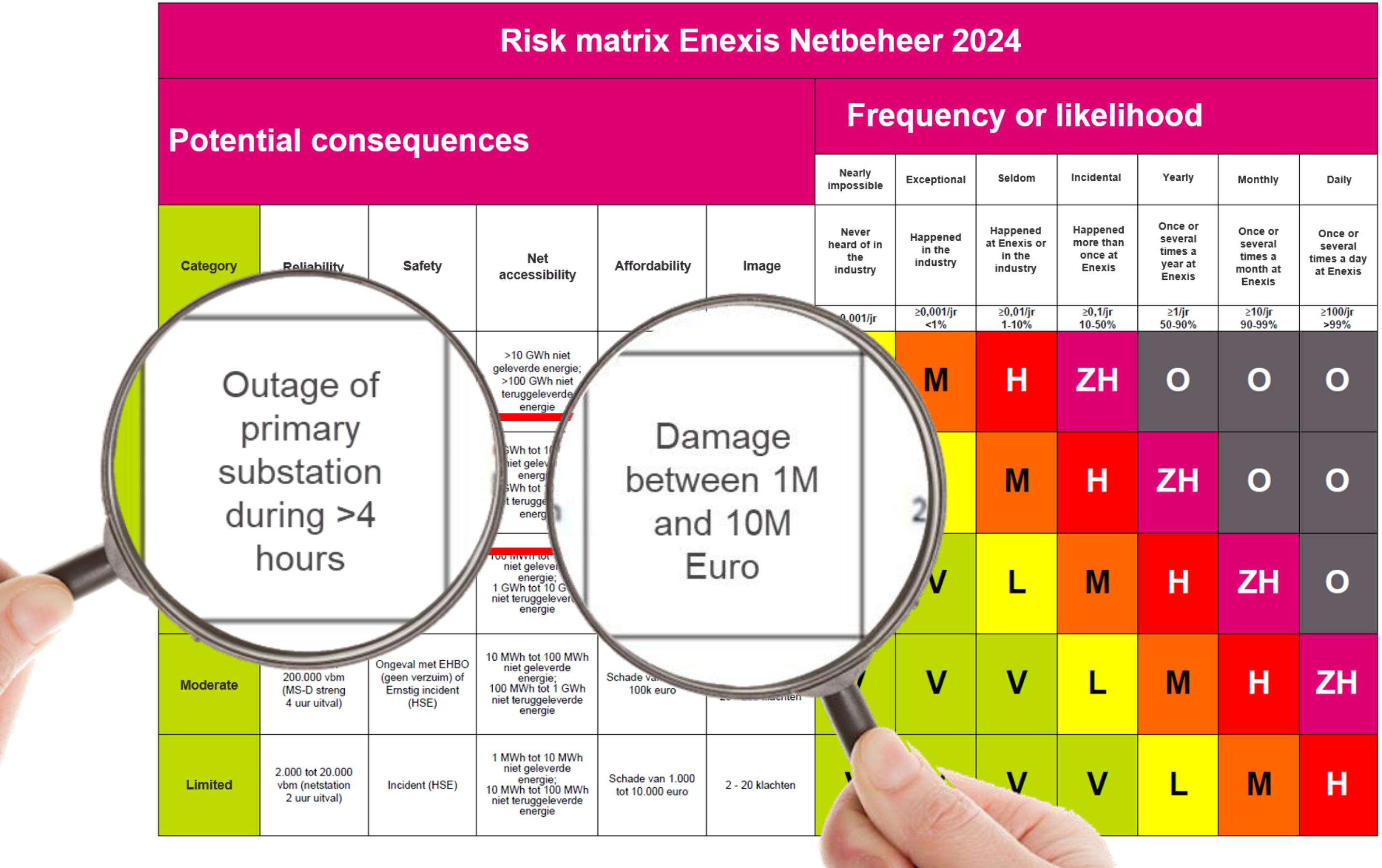
The Enexis Netbeheer risk matrix



Risk matrix Enexis Netbeheer 2024												
Potential consequences						Frequency or likelihood						
						Nearly impossible	Exceptional	Seldom	Incidental	Yearly	Monthly	Daily
Category	Reliability	Safety	Net accessibility	Affordability	Image	Never heard of in the industry	Happened in the industry	Happened at Enexis or in the industry	Happened more than once at Enexis	Once or several times a year at Enexis	Once or several times a month at Enexis	Once or several times a day at Enexis
						<0,001/jr	≥0,001/jr <1%	≥0,01/jr 1-10%	≥0,1/jr 10-50%	≥1/jr 50-90%	≥10/jr 90-99%	≥100/jr >99%
Very serious	>20.000.000 vbm (HS/MS station >16 uur uitval)	Ongeval met een of meerdere doden tot gevolg	>10 GWh niet geleverde energie; >100 GWh niet teruggeleverde energie	Schade groter dan 10M euro	Internationale commotie; >20.000 klachten	L	M	H	ZH	O	O	O
Serious	2.000.000 tot 20.000.000 vbm (HS/MS station 4 uur uitval)	Ongeval met ernstig, blijvend letsel (langdurig verzuim)	1 GWh tot 10 GWh niet geleverde energie; 10 GWh tot 100 GWh niet teruggeleverde energie	Schade van 1M tot 10M euro	Nationale commotie; 2.000 - 20.000 klachten	V	L	M	H	ZH	O	O
Significant	200.000 tot 2.000.000 vbm (MS-T station 4 uur uitval)	Ongeval met letsel met verzuim	100 MWh tot 1 GWh niet geleverde energie; 1 GWh tot 10 GWh niet teruggeleverde energie	Schade van 100k tot 1M euro	Regionale commotie; 200 - 2.000 klachten	V	V	L	M	H	ZH	O
Moderate	20.000 tot 200.000 vbm (MS-D streng 4 uur uitval)	Ongeval met EHBO (geen verzuim) of Ernstig incident (HSE)	10 MWh tot 100 MWh niet geleverde energie; 100 MWh tot 1 GWh niet teruggeleverde energie	Schade van 10k tot 100k euro	Lokale commotie; Interne commotie; 20 - 200 klachten	V	V	V	L	M	H	ZH
Limited	2.000 tot 20.000 vbm (netstation 2 uur uitval)	Incident (HSE)	1 MWh tot 10 MWh niet geleverde energie; 10 MWh tot 100 MWh niet teruggeleverde energie	Schade van 1.000 tot 10.000 euro	2 - 20 klachten	V	V	V	V	L	M	H

Risk appetite formalised by the board of directors

Easy to compare risks that affect different company values



Risk matrix Enexis Netbeheer 2024

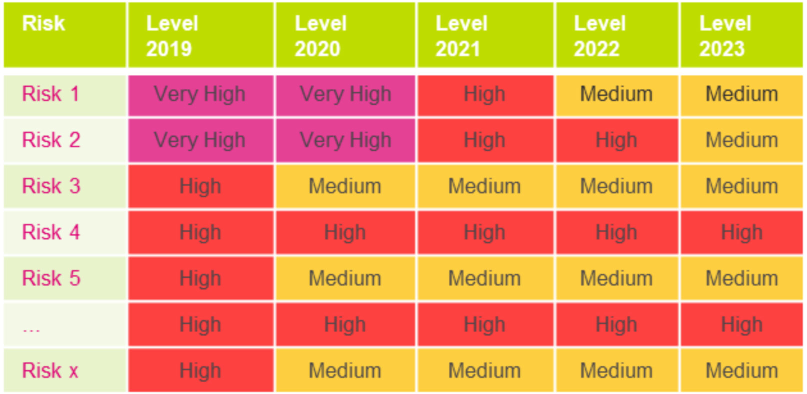
Potential consequences						Frequency or likelihood						
						Nearly impossible	Exceptional	Seldom	Incidental	Yearly	Monthly	Daily
Category	Reliability	Safety	Net accessibility	Affordability	Image	Never heard of in the industry	Happened in the industry	Happened at Enexis or in the industry	Happened more than once at Enexis	Once or several times a year at Enexis	Once or several times a month at Enexis	Once or several times a day at Enexis
						0.001/jr	≥0,001/jr <1%	≥0,01/jr 1-10%	≥0,1/jr 10-50%	≥1/jr 50-90%	≥10/jr 90-99%	≥100/jr >99%
			>10 GWh niet geleverde energie; >100 GWh niet teruggeleverde energie				M	H	ZH	O	O	O
	Outage of primary substation during >4 hours		GWh tot 1 niet gelev energ GWh tot t terugge energ	Damage between 1M and 10M Euro	2			M	H	ZH	O	O
			niet gelever energie; 1 GWh tot 10 G niet teruggelever energie				V	L	M	H	ZH	O
Moderate	200.000 vbm (MS-D streng 4 uur uitval)	Ongeval met EHBO (geen verzuim) of Ernstig incident (HSE)	10 MWh tot 100 MWh niet geleverde energie; 100 MWh tot 1 GWh niet teruggeleverde energie	Schade va 100k euro	klachten	V	V	V	L	M	H	ZH
Limited	2.000 tot 20.000 vbm (netstation 2 uur uitval)	Incident (HSE)	1 MWh tot 10 MWh niet geleverde energie; 10 MWh tot 100 MWh niet teruggeleverde energie	Schade van 1.000 tot 10.000 euro	2 - 20 klachten	V		V	V	L	M	H

All items on the same row are valued equally

Using the risk matrix

A risk matrix defines the framework for risk mitigation decisions

- The risk matrix is used during risk assessments to determine the risk level
- After identifying and quantifying risks, companies should:
  - have a an overview of all (or at least the most important) risks;
  - be able to prioritise these risks;
  - be able to decide on budget assignment for risk mitigation.
- Important to periodically update risk assessments and report on risk mitigation progress:



Risk	Level 2019	Level 2020	Level 2021	Level 2022	Level 2023
Risk 1	Very High	Very High	High	Medium	Medium
Risk 2	Very High	Very High	High	High	Medium
Risk 3	High	Medium	Medium	Medium	Medium
Risk 4	High	High	High	High	High
Risk 5	High	Medium	Medium	Medium	Medium
…	High	High	High	High	High
Risk x	High	Medium	Medium	Medium	Medium

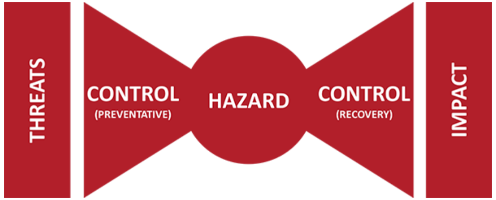
Digital risk management challenges

- Some typical challenges during risk assessments and risk management in general:
  - Deciding who to involve in risk assessments;
  - How to objectively quantify risks;
  - Explaining digital security risks to other people than security nerds, especially budget owners;
  - Trying to be perfect and 100% complete too quickly;
  - Identifying threats, threat actors and vulnerabilities;
  - Deciding which threat scenarios are realistic and which are not (avoid FUD and 'James Bond scenarios');
  - The potential impact of digital (mainly OT security) risks can be much higher than conventional risks;
  - Determining the likelihood part of the risk equation;
  - Assigning responsibility of the identified risks;
  - Finding the right balance between **A)** digital security and **B)** physical security, user friendliness, costs etc;
  - Deciding which risk mitigating controls to implement and who is responsible for this;
  - Monitoring the effectiveness of controls (intrinsic and actual).

Digital risk management challenges

Our best decision so far: using the existing Enexis risk management approach

- Many different risk management frameworks, for example:
  - ISO 31000 and 27005;
  - COSO Enterprise Risk Management;
  - NIST Risk Management Framework (RMF) and SP 800-30;
  - Information Security Forum (ISF)'s Information Risk Assesment Methodology (IRAM) model.
- In our experience, it is important to align digital and 'conventional' risk management:
  - This helps explaining the result of risk assessments to your colleagues;
  - Easier to compare the outcome of risk assessments for different topics;
  - Easier to assign budget for risk mitigation based on the amount of risk reduction per invested Euro.
- At Enexis, we use the 'bowtie method' to document risks



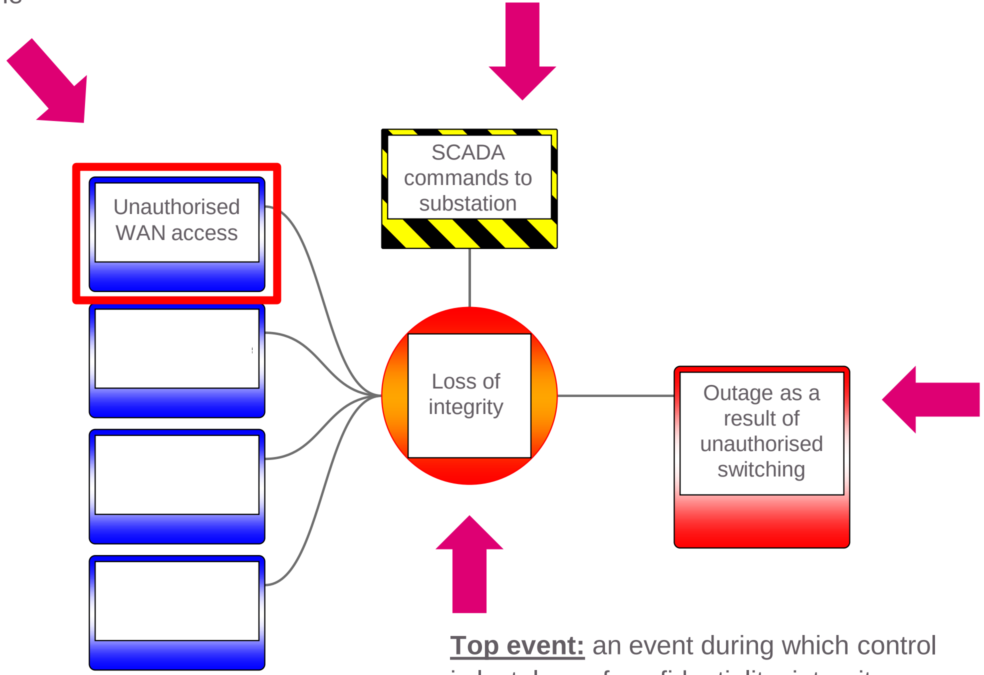
Source: https://www.risklens.com/infographics/what-is-a-bow-tie

The Enexis risk management process

Use of bowties - introduction

Hazard: an activity that an organisation executes, but that could cause damage if control is lost.

Threats: events that can lead to the top event, in case of digital risks these are typically actions by attackers.



SCADA commands to substation
Unauthorised WAN access
Loss of integrity
Outage as a result of unauthorised switching

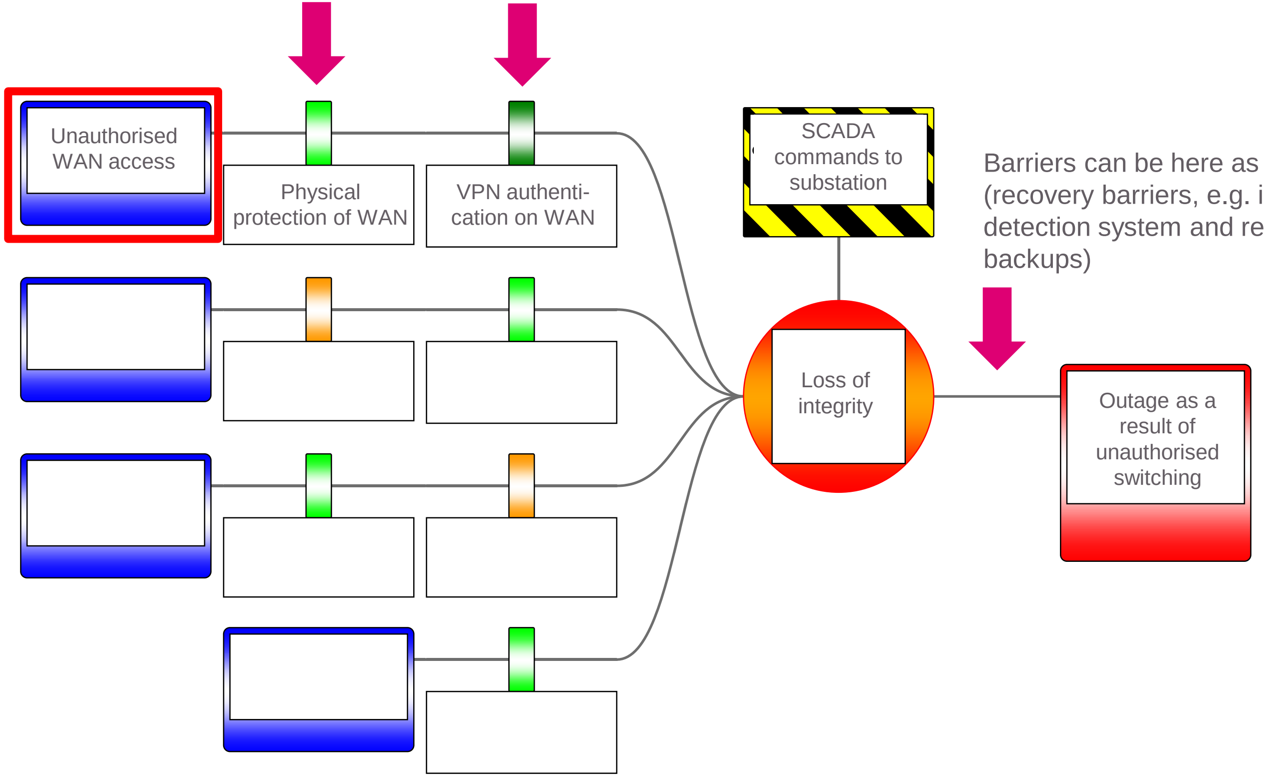
Consequences: the negative effects of the top event (related to our company's core values).

Top event: an event during which control is lost: loss of confidentiality, integrity or availability in case of digital security risks.

The Enexis risk management process

Use of bowties - barriers

Control barriers are measures that are taken to minimise the likelihood of a top event occurring.
The colour is an indication of the quality of the measure (intrinsic quality and/or current condition).



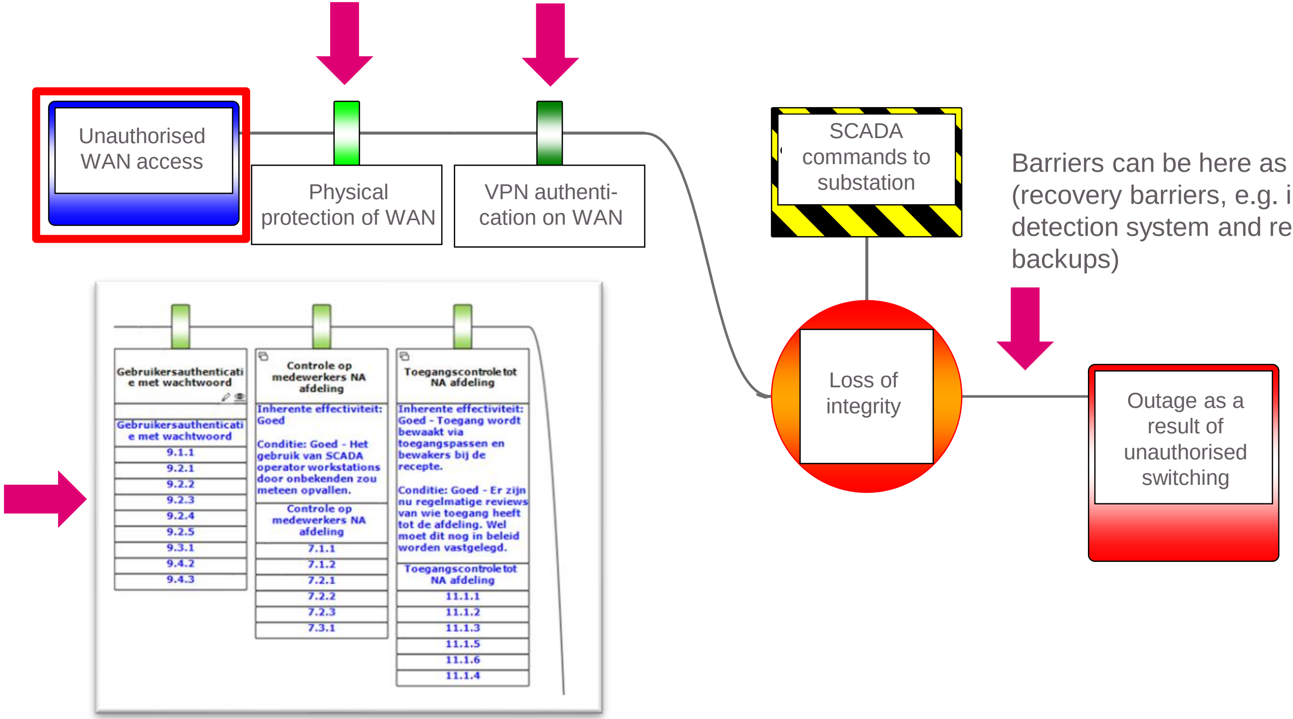
Unauthorised WAN access
Physical protection of WAN
VPN authentication on WAN
SCADA commands to substation
Loss of integrity
Outage as a result of unauthorised switching

Barriers can be here as well (recovery barriers, e.g. intrusion detection system and restoring backups)

The Enexis risk management process

Use of bowties - barriers

Control barriers are measures that are taken to minimise the likelihood of a top event occurring.
The colour is an indication of the quality of the measure (intrinsic quality and/or current condition).



Unauthorised WAN access

Physical protection of WAN

VPN authenti-cation on WAN

SCADA commands to substation

Loss of integrity

Outage as a result of unauthorised switching

Barriers can be here as well (recovery barriers, e.g. intrusion detection system and restoring backups)

Annex A references.

Gebruikersauthenticatie met wachtwoord

Gebruikersauthenticatie met wachtwoord

9.1.1

9.2.1

9.2.2

9.2.3

9.2.4

9.2.5

9.3.1

9.4.2

9.4.3

Controle op medewerkers NA afdeling

Inherente effectiviteit: Goed

Conditie: Goed - Het gebruik van SCADA operator workstations door onbekenden zou meteen opvallen.

Controle op medewerkers NA afdeling

7.1.1

7.1.2

7.2.1

7.2.2

7.2.3

7.3.1

Toegangscontrole tot NA afdeling

Inherente effectiviteit: Goed - Toegang wordt bewaakt via toegangspassen en bewakers bij de recepte.

Conditie: Goed - Er zijn nu regelmatige reviews van wie toegang heeft tot de afdeling. Wel moet dit nog in beleid worden vastgelegd.

Toegangscontrole tot NA afdeling

11.1.1

11.1.2

11.1.3

11.1.5

11.1.6

11.1.4

The Enexis risk management process

Selecting barriers to implement

- Based on IEC 62443-3-3 and ISO 27001
- Control barriers (left in bowtie):
  - Between threat and top event.
- Recovery barriers (right in bowtie):
  - Between top event and consequence.

IEC 62443-3-3

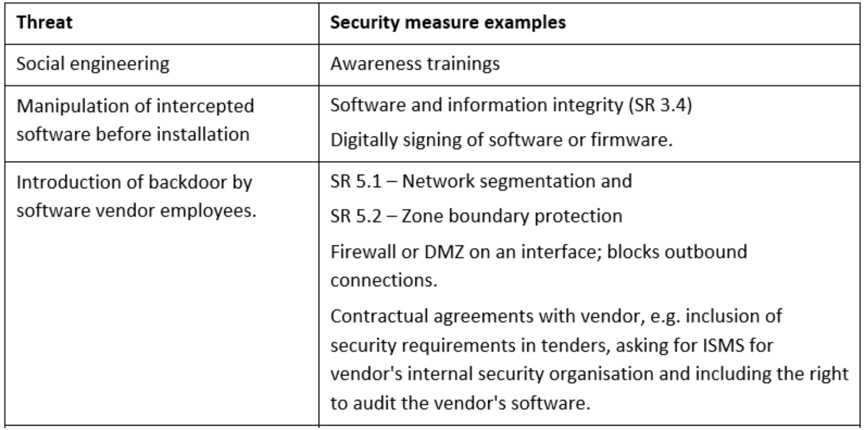
Edition 1.0 2013-08

IEC

INTERNATIONAL STANDARD

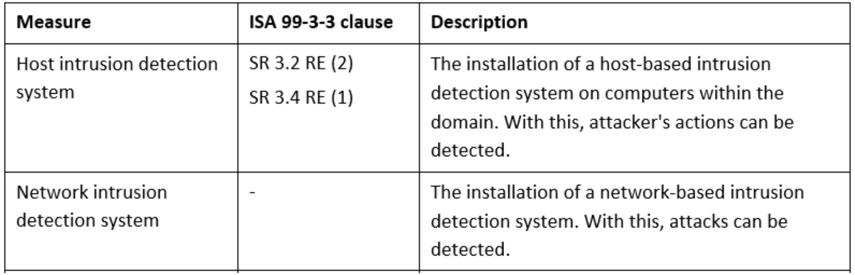
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

Control barriers:



Threat	Security measure examples
Social engineering	Awareness trainings
Manipulation of intercepted software before installation	Software and information integrity (SR 3.4) Digitally signing of software or firmware.
Introduction of backdoor by software vendor employees.	SR 5.1 – Network segmentation and SR 5.2 – Zone boundary protection Firewall or DMZ on an interface; blocks outbound connections. Contractual agreements with vendor, e.g. inclusion of security requirements in tenders, asking for ISMS for vendor's internal security organisation and including the right to audit the vendor's software.

Recovery barriers:



Measure	ISA 99-3-3 clause	Description
Host intrusion detection system	SR 3.2 RE (2) SR 3.4 RE (1)	The installation of a host-based intrusion detection system on computers within the domain. With this, attacker's actions can be detected.
Network intrusion detection system	-	The installation of a network-based intrusion detection system. With this, attacks can be detected.

CGE
Risk Management Solutions
Making risk understandable

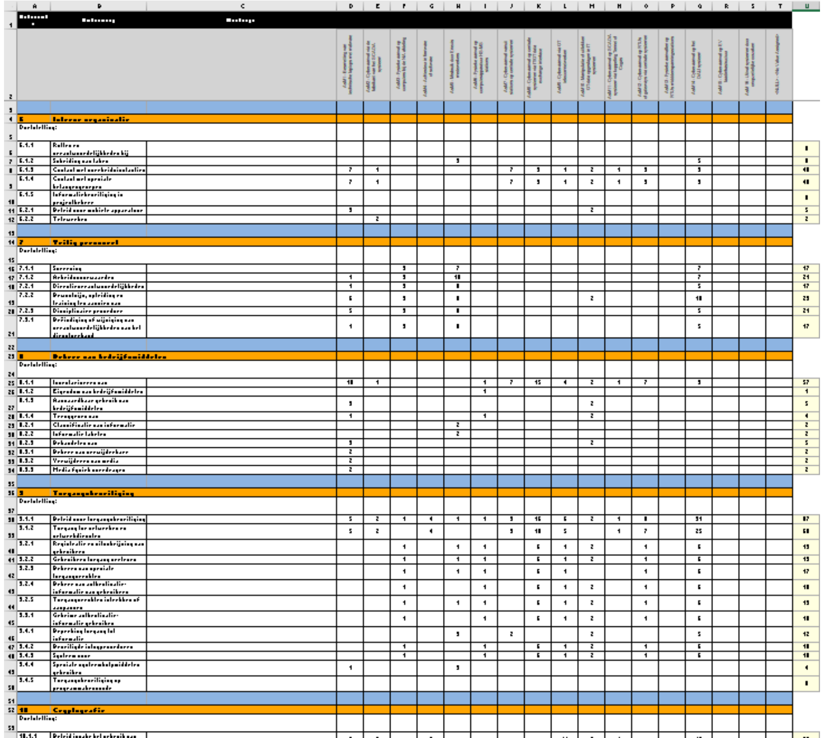
The Enexis risk management process

Mapping of our barriers to the ISO 27001:2017 Annex A controls (see clause 6.1.3c)

The 114 controls of the ISO 27001 Annex A

The number of times that a control is used in our bowties, easy to identify key controls

All our OT security risk categories (detailed in bowties)



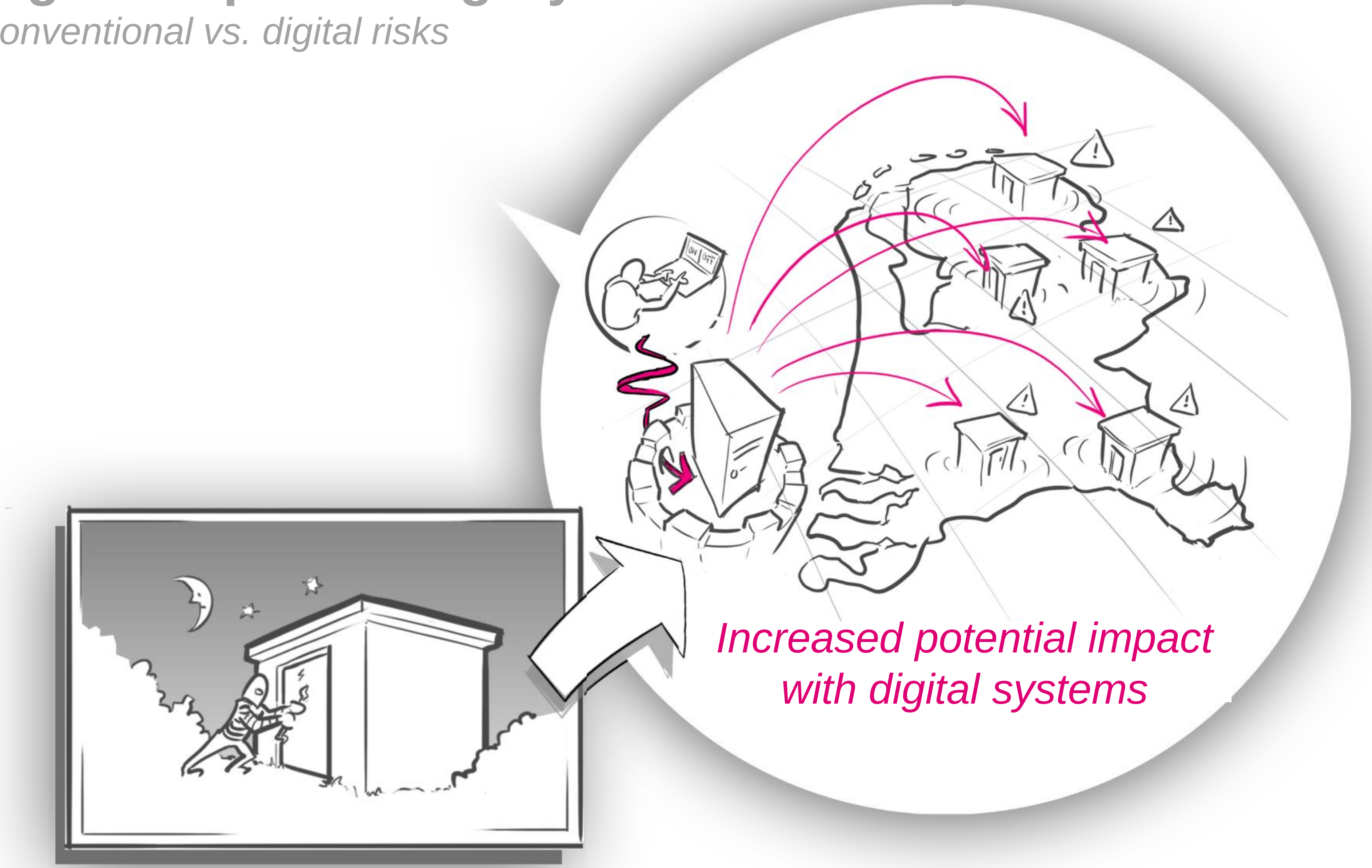
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
[illegible]	[illegible]	[illegible]																		
			AAM1 : [illegible]	AAM2 : Cyberaanval via de [illegible] SCADA systeem	AAM3 : [illegible]	AAM4 : [illegible]	AAM5 : [illegible]	AAM6 : [illegible]	AAM7 : [illegible]	AAM8 : [illegible]	AAM9 : Cyberaanval via OT [illegible]	AAM10 : [illegible]	AAM11 : Cyberaanval op SCADA [illegible]	AAM12 : Cyberaanval op RTU's [illegible]	AAM13 : [illegible]	AAM14 : Cyberaanval op het DALI systeem	AAM15 : Cyberaanval op EV [illegible]	AAM16 : [illegible]	<NULL> : <No Value Assigned>	
6	Interne organisatie																			
Doelstelling:																				
6.1.1	Rollen en verantwoordelijkheden bij																			0
6.1.2	Scheiding van taken						3									5				8
6.1.3	Contact met overheidsinstanties		7	1					7	3	1	2	1	3		3				40
6.1.4	Contact met speciale belangengroepen		7	1					7	3	1	2	1	3		3				40
6.1.5	Informatiebeveiliging in projectbeheer																			0
6.2.1	Beleid voor mobiele apparatuur		3									2								5
6.2.2	Telewerken			2																2
7	Veilig personeel																			
Doelstelling:																				
7.1.1	Screening				3		7									7				17
7.1.2	Arbeidsvoorwaarden		1		3		10									7				21
7.2.1	Directieverantwoordelijkheden		1		3		8									5				17
7.2.2	Bewustzijn, opleiding en training ten aanzien van		6		3		8					2				10				29
7.2.3	Disciplinaire procedure		5		3		8									5				21
7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband		1		3		8									5				17
8	Beheer van bedrijfsmiddelen																			
Doelstelling:																				
8.1.1	Inventariseren van		10	1				1	7	15	4	2	1	7		3				57
8.1.2	Eigendom van bedrijfsmiddelen							1												1
8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen		3									2								5
8.1.4	Teruggeven van		1					1				2								4
8.2.1	Classificatie van informatie						2													2
8.2.2	Informatie labelen						2													2
8.2.3	Behandelen van		3									2								5
8.3.1	Beheer van verwijderbare		2																	2
8.3.2	Verwijderen van media		2																	2
8.3.3	Media fysiek overdragen		2																	2
9	Toegangsbeveiliging																			
Doelstelling:																				
9.1.1	Beleid voor toegangsbeveiliging		5	2	1	4	1	1	3	16	6	2	1	8		31				87
9.1.2	Toegang tot netwerken en netwerkdiensten		5	2		4			3	10	5		1	7		25				68
9.2.1	Registratie en afmelden van gebruikers				1		1	1		6	1	2		1		6				19
9.2.2	Gebruikers toegang verlenen				1		1	1		6	1	2		1		6				19
9.2.3	Beheren van speciale toegangsrechten				1		1	1		6	1			1		6				17
9.2.4	Beheer van geheime authenticatie-informatie van gebruikers				1			1		6	1	2		1		6				18
9.2.5	Toegangsrechten intrekken of aanpassen				1		1	1		6	1	2		1		6				19
9.3.1	Geheime authenticatie-informatie gebruiken				1			1		6	1	2		1		6				18
9.4.1	Beperking toegang tot informatie						3		2			2				5				12
9.4.2	Beveiligde inlogprocedures				1			1		6	1	2		1		6				18
9.4.3	Systeem voor				1			1		6	1	2		1		6				18
9.4.4	Speciale systeemhulpmiddelen gebruiken		1				3													4
9.4.5	Toegangsbeveiliging op programmabroncode																			0
10	Cryptografie																			
Doelstelling:																				
10.1.1	Beleid inzake het gebruik van																			

1-click xls report from our bowtie development application BowtieXP

DigiTrust
ISO 27001
MANAGEMENTSYSTEEM VOOR INFORMATIEBEVEILIGING
MGMT. SYS. RvA C 618

Higher impact category for OT security risks

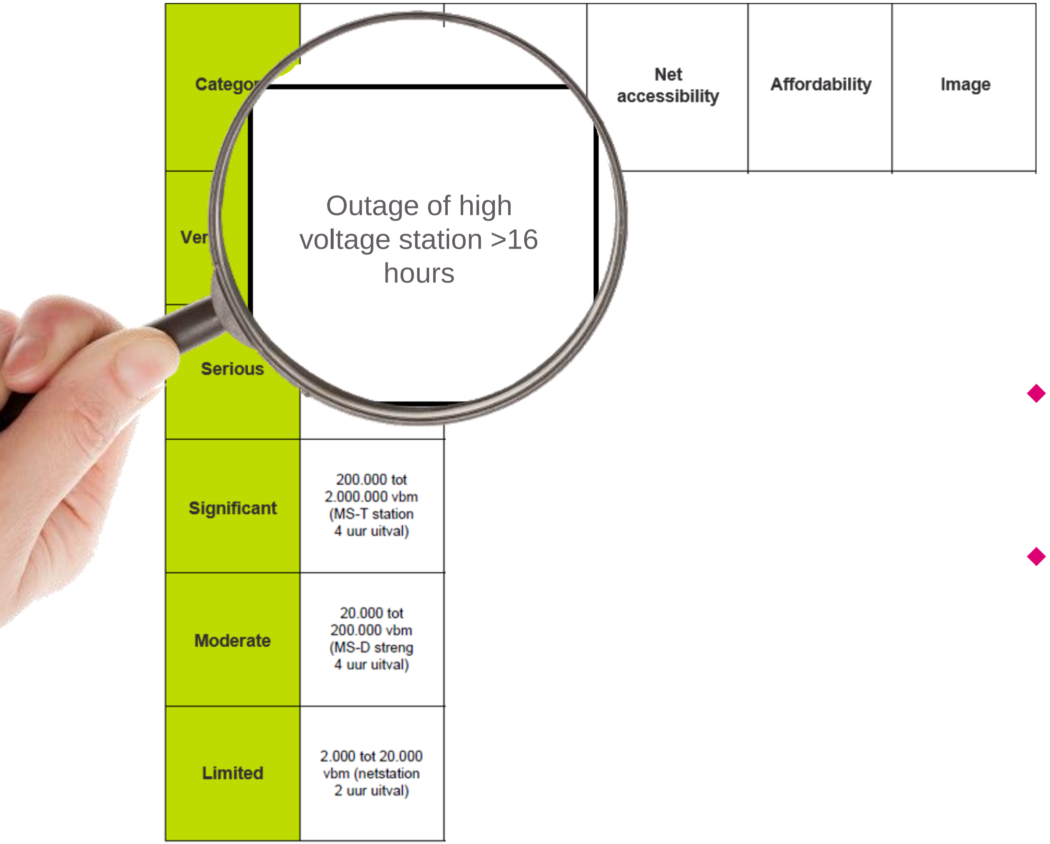
Conventional vs. digital risks



Increased potential impact with digital systems

Higher impact category for OT security risks

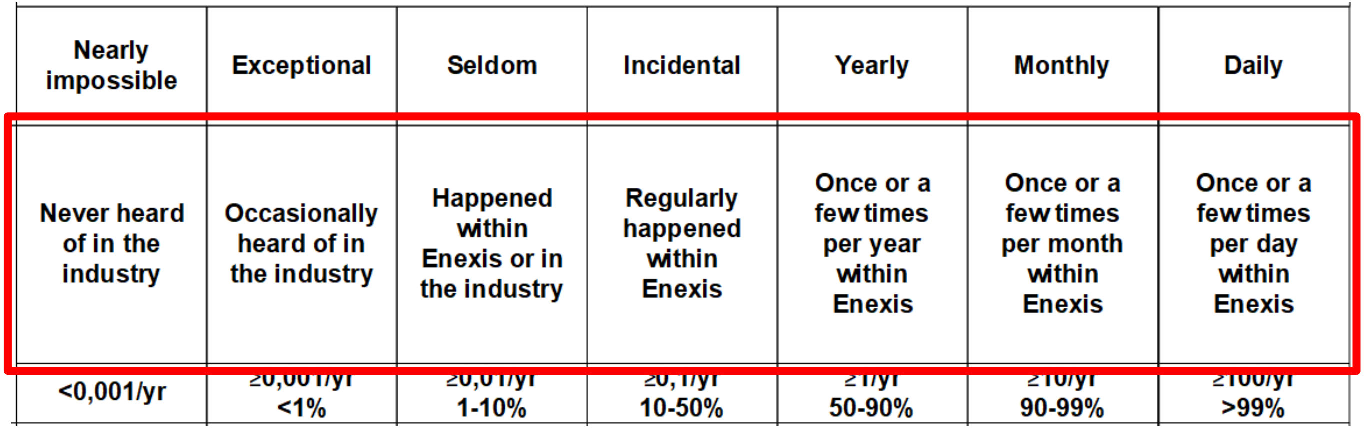
Conventional vs. digital risks



Catego			Net accessibility	Affordability	Image
Ver	Outage of high voltage station >16 hours				
Serious					
Significant	200.000 tot 2.000.000 vbm (MS-T station 4 uur uitval)				
Moderate	20.000 tot 200.000 vbm (MS-D streng 4 uur uitval)				
Limited	2.000 tot 20.000 vbm (netstation 2 uur uitval)				

- Highest reliability impact category is 'very serious':
  - Outage of high voltage station >16 hours;
  - This is ok for conventional risks like physical break-in in substation.
- Introduced impact category 'disastrous' for digital risks:
  - Outage 10 HV stations >16 hours;
  - Digital attack could lead to outage of multiple HV stations;
  - Often same equipment and vulnerabilities on multiple locations;
  - Much higher impact with similar effort by attacker.

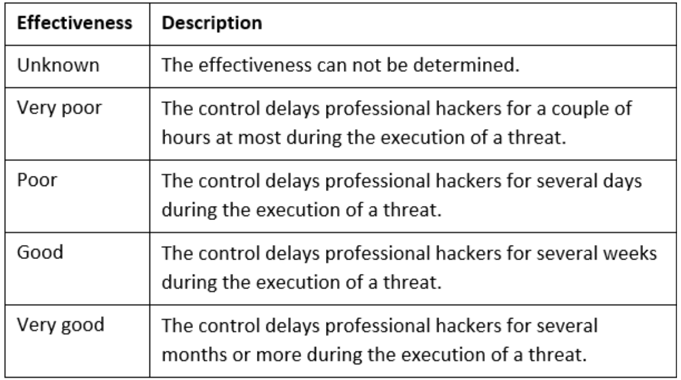
Determining the likelihood of OT security risks



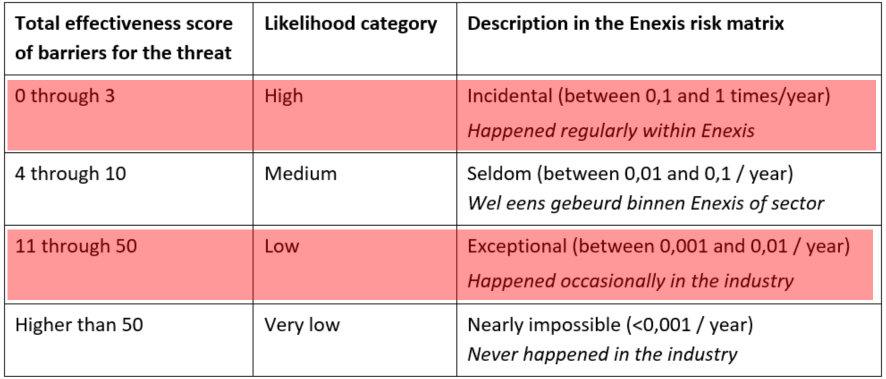
Nearly impossible	Exceptional	Seldom	Incidental	Yearly	Monthly	Daily
Never heard of in the industry	Occasionally heard of in the industry	Happened within Enexis or in the industry	Regularly happened within Enexis	Once or a few times per year within Enexis	Once or a few times per month within Enexis	Once or a few times per day within Enexis
<0,001/yr	≥0,001/yr <1%	≥0,01/yr 1-10%	≥0,1/yr 10-50%	≥1/yr 50-90%	≥10/yr 90-99%	≥100/yr >99%

Determining the likelihood of OT security risks

- Little historical data about digital incidents
- Our approach:
  - Use control effectiveness as a starting point;
  - Convert effectiveness to a numerical score;
  - Indication of the number of days a professional hacker will need to circumvent a control;
  - Plot the effectiveness score on the ROBAM risk matrix.
- Justification for the effectiveness table:
  - Based on an analysis of the threat landscape and (the limited amount of) previous incidents;
  - Likelihood high: small incidents (viruses, ransomware): couple of hours work for attacker;
  - Likelihood low: Ukraine in December 2015 and 2015: probably took several weeks of preparation.
- Currently working on the introduction of LOPA*



Effectiveness	**Description**
Unknown	The effectiveness can not be determined.
Very poor	The control delays professional hackers for a couple of hours at most during the execution of a threat.
Poor	The control delays professional hackers for several days during the execution of a threat.
Good	The control delays professional hackers for several weeks during the execution of a threat.
Very good	The control delays professional hackers for several months or more during the execution of a threat.



Total effectiveness score of barriers for the threat	**Likelihood category**	**Description in the Enexis risk matrix**
0 through 3	High	Incidental (between 0,1 and 1 times/year) *Happened regularly within Enexis*
4 through 10	Medium	Seldom (between 0,01 and 0,1 / year) *Wel eens gebeurd binnen Enexis of sector*
11 through 50	Low	Exceptional (between 0,001 and 0,01 / year) *Happened occasionally in the industry*
Higher than 50	Very low	Nearly impossible (<0,001 / year) *Never happened in the industry*

*: Layers of Protection Analysis, incl. separate estimation of inherent effectiveness and control maturity.

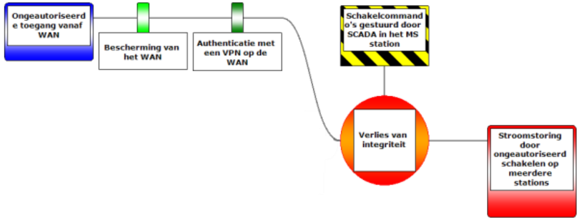
Lessons learned

Advantages of our approach:

- Easy to discuss results with colleagues not directly involved in OT security;
- Clear conceptual model for risks;
- Easy to relate controls to threats;
- Good insight in the effectiveness of controls, easy to assign actions;
- Easy to map risks to Annex A controls;
- Clear link between loss of C/I/A and impact on Enexis company values.

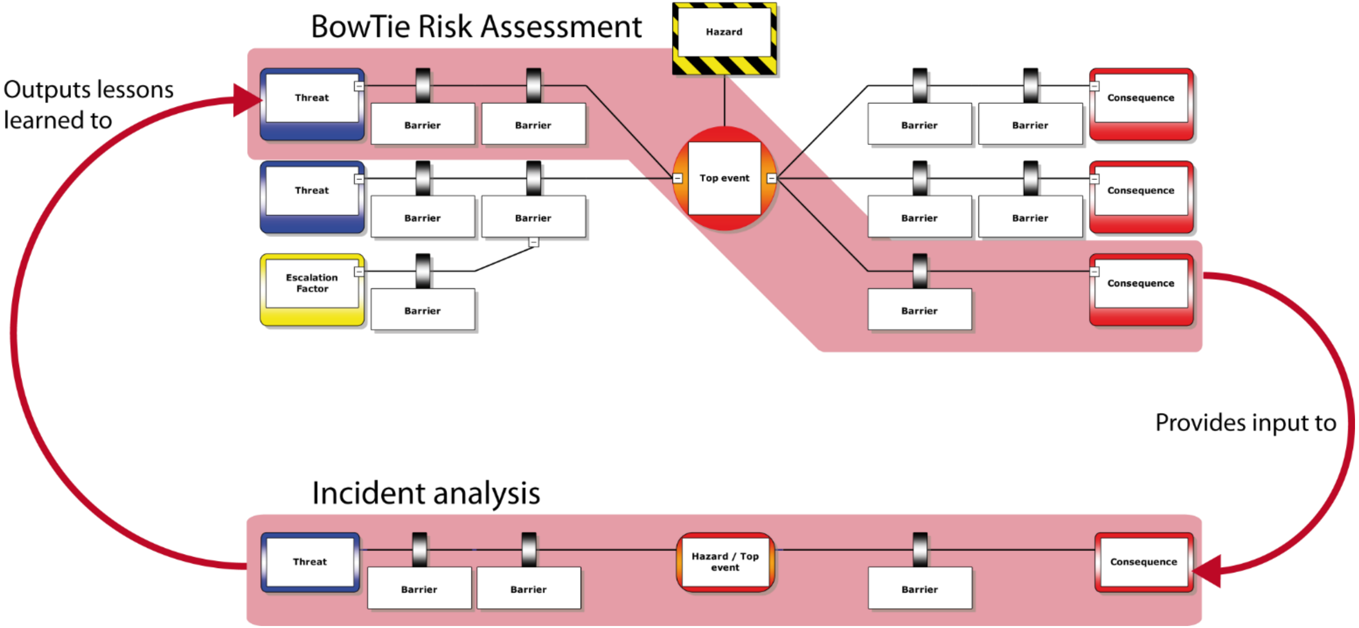
Disadvantages:

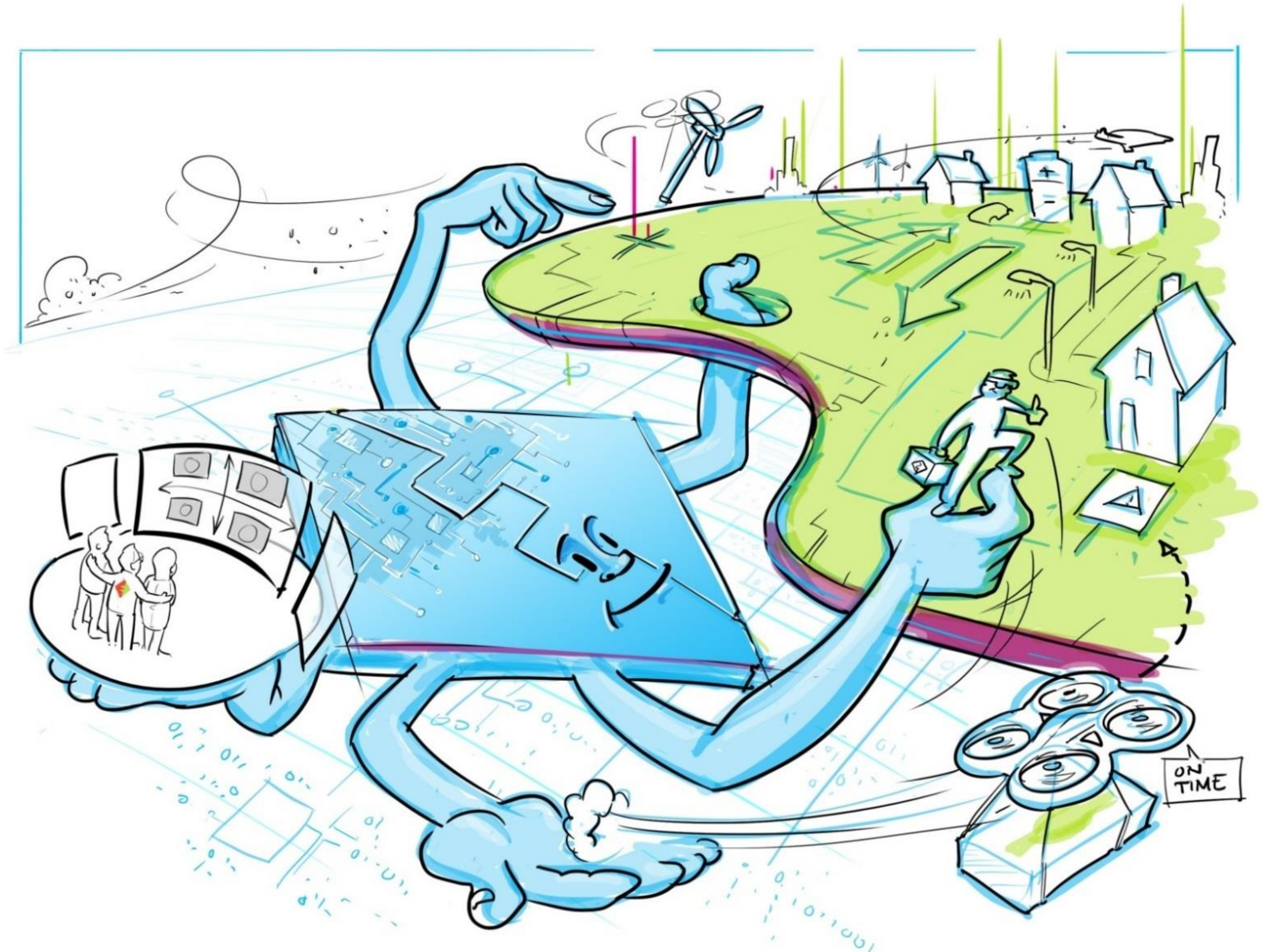
- Maintaining all bowties is labour intensive;
- Many different hazards and top events, easy to lose overview;
- Creating and updating bowties consistently requires discipline and experience;
- Determination of likelihood too subjective;
- Contribution of individual controls (in 'threat string') to risk reduction not always clear.


Ongeautoriseerde toegang vanaf WAN
Bescherming van het WAN
Authenticatie met een VPN op de WAN
Schakelcommando's gestuurd door SCADA in het MS station
Verlies van integriteit
Stroomstoring door ongeautoriseerd schakelen op meerdere stations

Future plans

Performing incident investigation based on our bowties





Philip Westbroek
OT security officer
Philip.westbroek@enexis.nl

Graphics by Wilco Prinsen
www.jamvisualthinking.com