ENTERPRISE CYBER SECURITY

ASSESSING CYBER RISK

University of Glasgow

OVERVIEW

- consider the cyber risk assessment process in more detail.
- small group teaching using your assignment groups to discuss and develop outputs for each stage.
- use running example to walkthrough various stages of the cyber risk approach.

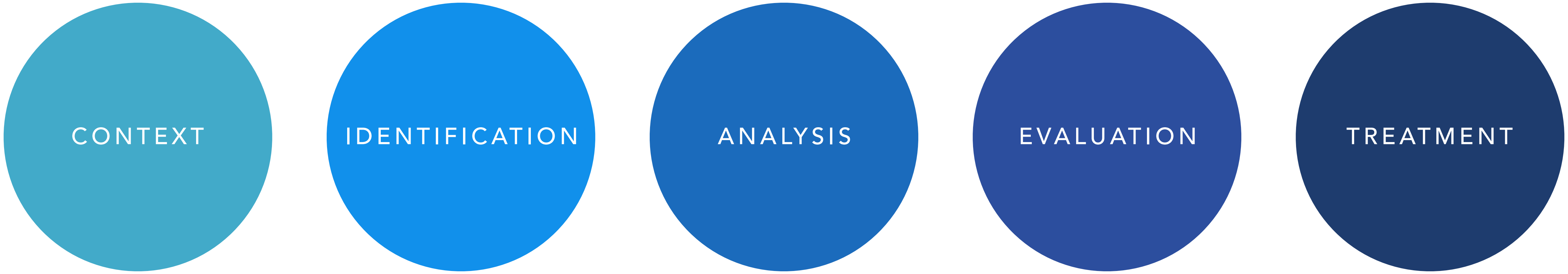
TEXTBOOK EXAMPLE SMART GRID

- smart grid potentially allows for more efficient generation and use of energy.

- system comprises of a distributor of energy and a customer of energy.

- consumer will have a terminal, meter and limiter and the distributor will have a central system and management system.

- distributor will be connected to the consumer through the Internet and a cellular connection.



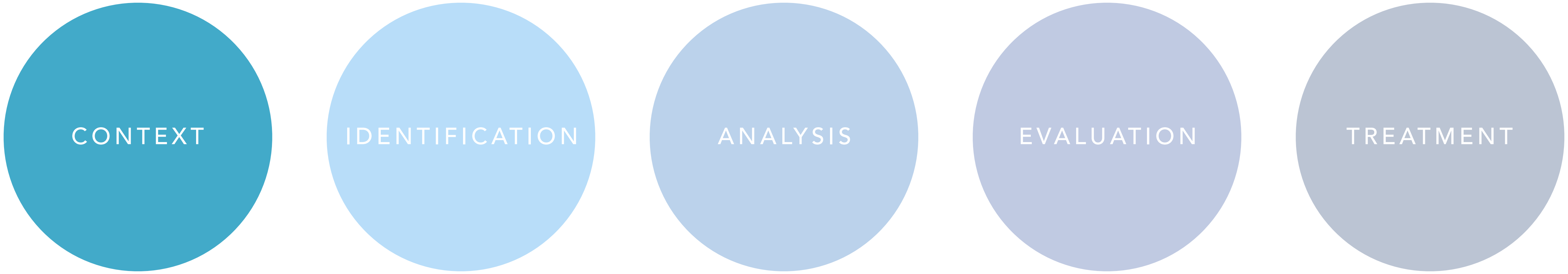
CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT



CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT

CONTEXT

- crucial step in the cyber risk assessment process and ultimately determine the overall success or failure of the process.

- understand and document how the cyber system interacts with the cyber space.

- develop an understanding how the **attack surface**, cyber system and cyber space all interact.

- expand focus to consider impact beyond the intangible, physical harm and operating environment.

CONSIDERING CONTEXT

- consider the **external context**, all the factors and environmental parameters that influence business objectives and how they manage risk.
- consider the **internal context**, the factors that influence how an organisation manages risk and attains objectives.
- **attack surface** and the interface to cyber space.
- consider the overall view, the **target of assessment**, that is the subsystem(s) and aspects of interest.

AIMS

- **aims and objectives** of performing the risk assessment itself.
- primarily to **manage risk and reduce the likelihood** of undesirable incidents.
- **communication** to several internal and external stakeholders that do not necessarily know anything about cyber security.
- **compliance** with legal requirements.

SCOPE AND ASSUMPTIONS

- improves communications between various individuals if we have clear documentation of scope, focus and assumptions made in risk assessment.
- limit the **scope** of the assessment, e.g. back-end system may be vulnerable, but beyond consideration.
- the primary **focus** of the assessment what is being focused on within the assessment, e.g. physical attacks may be inside scope, but not the focus of assessment.
- **assumptions** we are making about the internal and external threat sources, for example disruption to society as well as financial gain

ASSETS AND SCALES

- assets inform what needs to be protected and what risk are pertinent.

- need to have scales to determine the optimal measurement of the risk (e.g. likelihood and consequence scales).

- **risk matrix** can be used to determine solutions for the risk.

RISK MATRIX

LIKELIHOOD

CONSEQUENCE

	RARE	UNLIKELY	POSSIBLE	LIKELY	CERTAIN
CRITICAL	🟧	🟥	🟥	🟥	🟥
MAJOR		🟧	🟥	🟥	🟥
MODERATE			🟧	🟥	🟥
MINOR				🟧	🟥
INSIGNIFICANT					🟧

SMART GRID

- consider the **internal**, **external** contexts as well as the **objectives**.

- determine the **target of assessment**, considering the **scope** and **focus**.

- consider the **attack surface**.

- what are the **assets**, **consequences** and the **likelihood** of something happening.

EXTERNAL CONTEXT

INTERNAL CONTEXT

OBJECTIVES

TARGET OF ASSESSMENT

ATTACK SURFACE

ATTACK SURFACE

LOCATION		

ATTACK SURFACE

LOCATION	CONSUMER	PROVIDER
Remote Location Attack	Connection Between Meter And The Internet/ Cellular	Connect Between Central System And The Internet/Cellular
Physical Nearby Attack	Interfering Between The Different Elements Of The Meter	Interfering Between The Different Elements Of The Central System

SCOPE

FOCUS

ASSETS

ASSETS

ASSET	DESCRIPTION

ASSETS

ASSET	DESCRIPTION
Meter Data Integrity	Ensure Meter Data Is Protected From The Consumer Unit To The Central System
Meter Data Availability	Ensure Meter Is Available From The Meter All The Time

LIKELIHOOD

LIKELIHOOD

VALUE	DESCRIPTION

LIKELIHOOD

VALUE	DESCRIPTION
Rare	Less Than 20 Years
Unlikely	Less Than 4 Years
Possible	Less Than 4 Times A Year
Likely	More Than Once A Month
Certain	Weekly

CONSEQUENCES

CONSEQUENCES

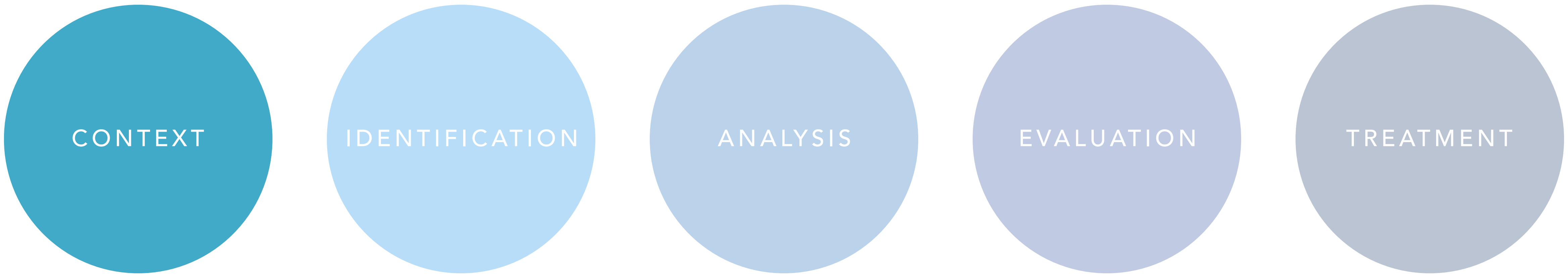
VALUE	DESCRIPTION

CONSEQUENCES (INTEGRITY)

VALUE	DESCRIPTION
Insignificant	Less Than 50 Customers
Minor	Less Than 200 Customers
Adequate	Less Than 500 Customers
Significant	Less Than 2000 Customers
Critical	More Than 4000 Customers

CONSEQUENCES (AVAILABILITY)

VALUE	DESCRIPTION
Insignificant	Less Than 12 Hours
Minor	Less Than 24 Hours
Adequate	Less Than 3 Days
Significant	Less Than 7 Days
Critical	More Than 21 Days



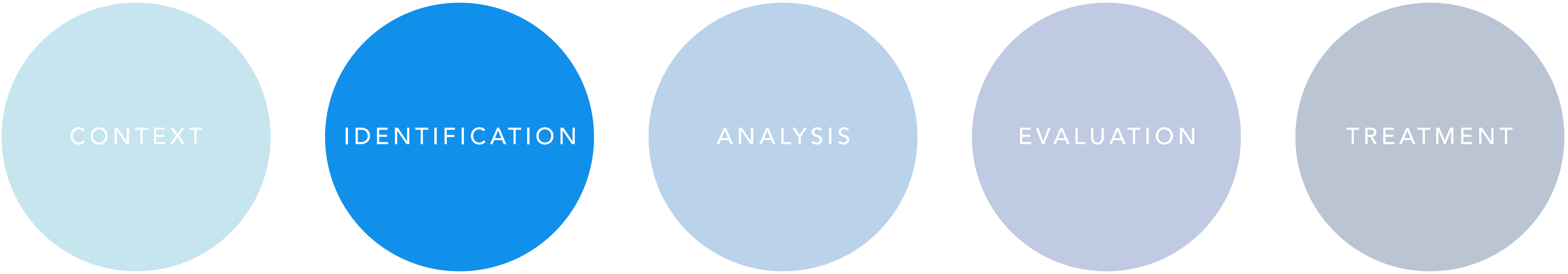
CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT



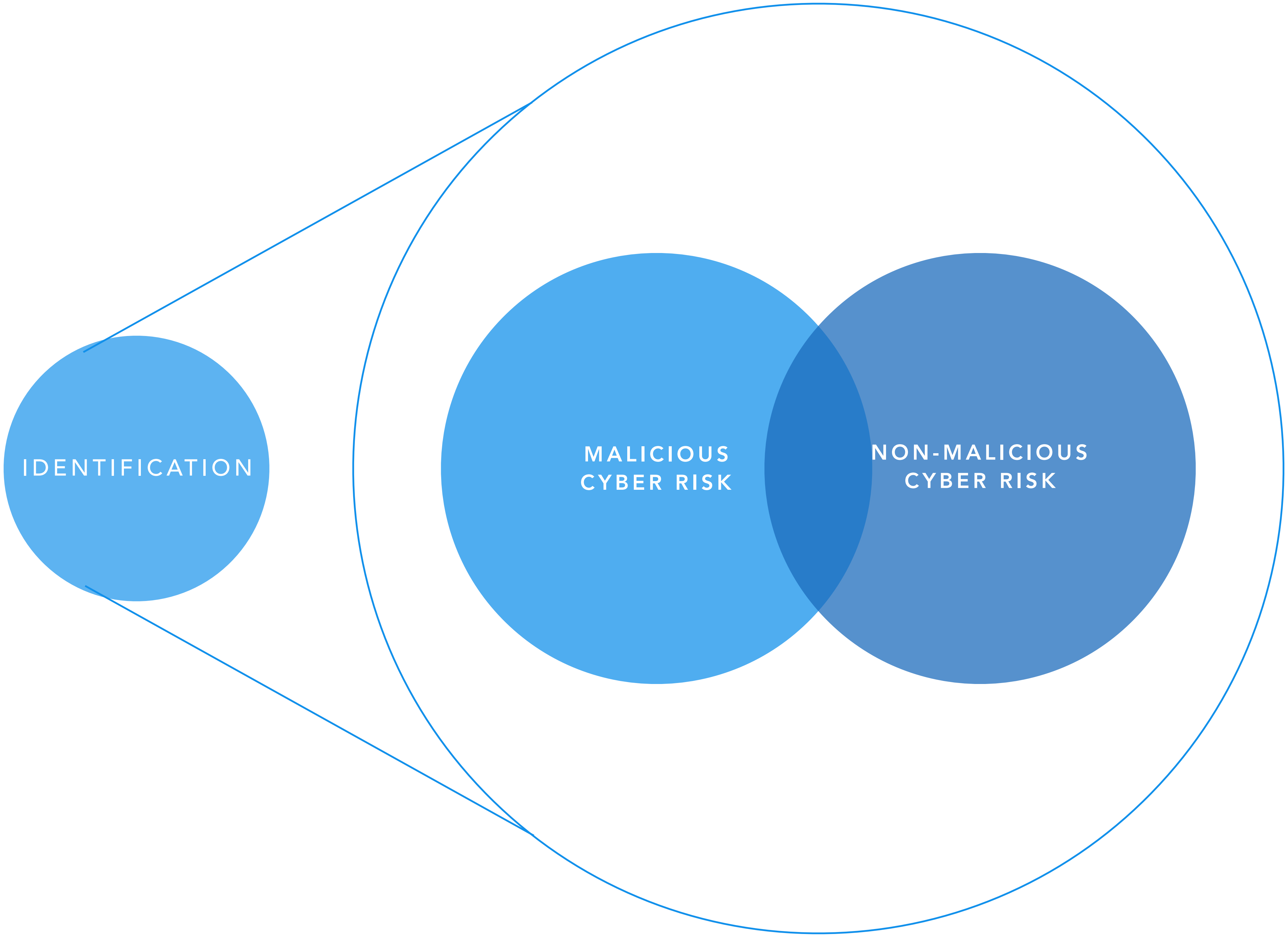
CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT


IDENTIFICATION
MALICIOUS CYBER RISK
NON-MALICIOUS CYBER RISK

TECHNIQUES

- often **technical** problem so lots of data available for analysis and consideration, for example logs.
- technical test may not confirm the presence of vulnerability, that does not mean **should not be considered**.
- consider **evidence from other sources** that are relevant to the risk assessment.
- risk identification can emerge not only from the consideration of logs and outputs from tests, but **people** as well.

TECHNICAL

- often technical problem so **lots of data** and information available (e.g. intrusion detection systems, logs). could be a lot of it

- **walk through** the target description, consider how the cyber systems interacts with cyber space and the assets themselves.

- determine relevant sources of evidence and data, potentially co-determine relevant employees and/or stakeholders.

- caution should be exercised in terms of using **historical data to make predictions of future** issues.

TECHNICAL TESTS

TARGET OF ASSESSMENT	SOURCE DESCRIPTION	REFERENCE

RISK IDENTIFICATION

TARGET OF ASSESSMENT	SOURCE DESCRIPTION	REFERENCE
Connection Between Client And Server.	Test Performed Between Client And Server To Ensure Sanitation	Testdoc.Pdf

NON-TECHNICAL

- testing does not **confirm the absence** vulnerabilities, consequently it does not mean we can simply ignore it.
- focus is at this stage is not the likelihood or the severity of consequences but **identification** of potential risks.
- consider open source repositories, standards, current trends, news reports, research papers etc.
- challenge becomes the relevancy of evidence within the target of assessment and domain.

SOURCES

1. develop and devise **relevancy criteria**, using the domain, asset or system type to inform.
2. **identify good sources** of evidence and information based on the devised criteria.
3. focus on the **aspects of evidence that are relevant** to your assessment.
4. ensure they are reconsidered or **reformed** from a general perspective to the **specialised perspective**.

PEOPLE (1/2)

- risk identification can emerge not only from the consideration of logs and outputs from test, but **people** as well.

- consider **viewpoints** from developers, maintenance, operators as well as specialists (e.g. security officers, sales, managers etc).

- **external experts** could also prove invaluable in identifying risks for particular systems.

PEOPLE (2/2)

- **interview** staff with planned questions that follow a strict structure, possibly consider mixed approach with open as well as follow-up questions.
- **questionnaires** can be used to probe staff, inexpensive compared to interviews but lack follow-up option.
- **brainstorm** with stakeholders as well as other personnel with intimate or working knowledge.

MALICIOUS

IDENTIFICATION (MALICIOUS)

- document potential adversaries and their properties, we need to identify potential **threat sources**.

- understand the **potential threats** the adversaries represent and the asset attack surface.

- focus on the assets attack focus to determine **vulnerabilities** and understand current defences.

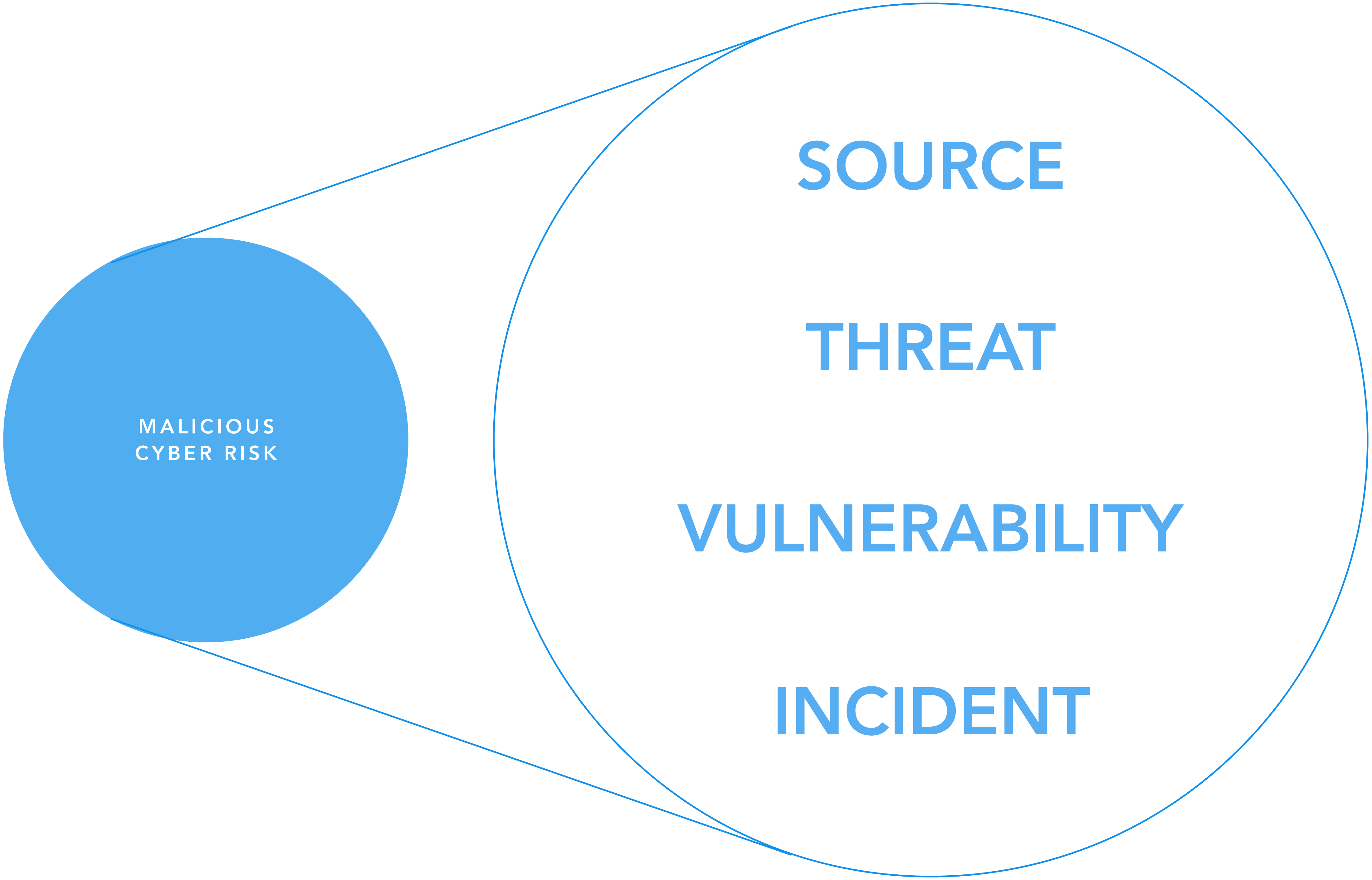
- predict **potential incidents** stemming from the combination of vulnerabilities and threats.

IDENITIFCATION (MALICIOUS)

- consider threat sources, essentially the potential **adversaries**.
- potential **attacks**, **vulnerabilities** that will be exploited and the resulting **incidents**.
- outcome of stage is to establish a focused, complete collection of pertinent threat sources, threats, vulnerabilities and incidents.

IDENTIFICATION (NON-MALICIOUS)

- determine **potential incidents** that could be consequence of accident and error.
- understand **potential vulnerabilities** by understanding routines and review current business processes.
- predict **threats** that stem from the envisaged incidents and vulnerabilities.
- determine the **source** of such threats, determine the users of the cyber system and the other entities utilising it.



MALICIOUS
CYBER RISK

SOURCE

THREAT

VULNERABILITY

INCIDENT

SOURCE

- understand who is going to initiate an attack and why would they want to do this
- important to understand the **motives and characterises** as well as the **capabilities and resources** and these need to be documented
- information of common threats sources can be drawn from relevant bodies (e.g. NIST etc).

SOURCES OF MALICIOUS THREATS

SOURCE	MOTIVE	CAPABILITY

SOURCES OF MALICIOUS THREATS

SOURCE	MOTIVE	CAPABILITY
Insider	An Disgruntled Employee Who Has Personal Gain Or A Grudge.	Potentially Has Authorisation To A Lot Of The Data And Understand The Architecture Of The System
Malware	Malicious Software Designed To Harm Hardware But May Not Be Tailored To The Specific Systems	Highly Sophisticated Software That Cause Severe Problems On The Off-Shelf-Hardware.

THREAT

- we have the **sources of threats**, we now need to consider **each threat** they may issue
- we attempt to understand how the threat source will **exploit the attack surface** established during the previous stage
- we need to demonstrate how the attack surface is exploited by the threat
- this important for later risk analysis, standards examples

MALICIOUS THREATS

SOURCE	ATTACK POINT	THREAT

MALICIOUS THREATS

SOURCE	ATTACK POINT	THREAT
Insider	Central System	Signal sent from the central system to the limiter in the consumer meter.
Malware	Meter	Meter becomes infected with malware.

VULNERABILITY

- we have identified the adversaries and the threats they may issue, the next step is to **identify the vulnerabilities** they may make use of
- pay attention to the **weaknesses** of the defence processes or **lack of defence**.
- live system could consider running tests to identify vulnerabilities.

VULNERABILITIES EXPLOITED BY MALICIOUS THREATS

THREAT	VULNERABILITY	DESCRIPTION

VULNERABILITIES EXPLOITED BY MALICIOUS THREATS

THREAT	VULNERABILITY	DESCRIPTION
Signal sent from the central system to the limiter in the consumer meter.	No logging of actions or use of four-eye principle.	There is no proper authorisation procedure implemented on the central system.
Meter becomes infected with malware.	Outdate protection against malware on the meter.	Meter connected to Internet needs proper antivirus protection, library needs to be kept updated.

INCIDENT

- before analysis we need to determine the potential incidents that could harm the assets
- much of the documentation to identify threats and sources can be used to determine the potential incidents.
- or the actual risks to our assets

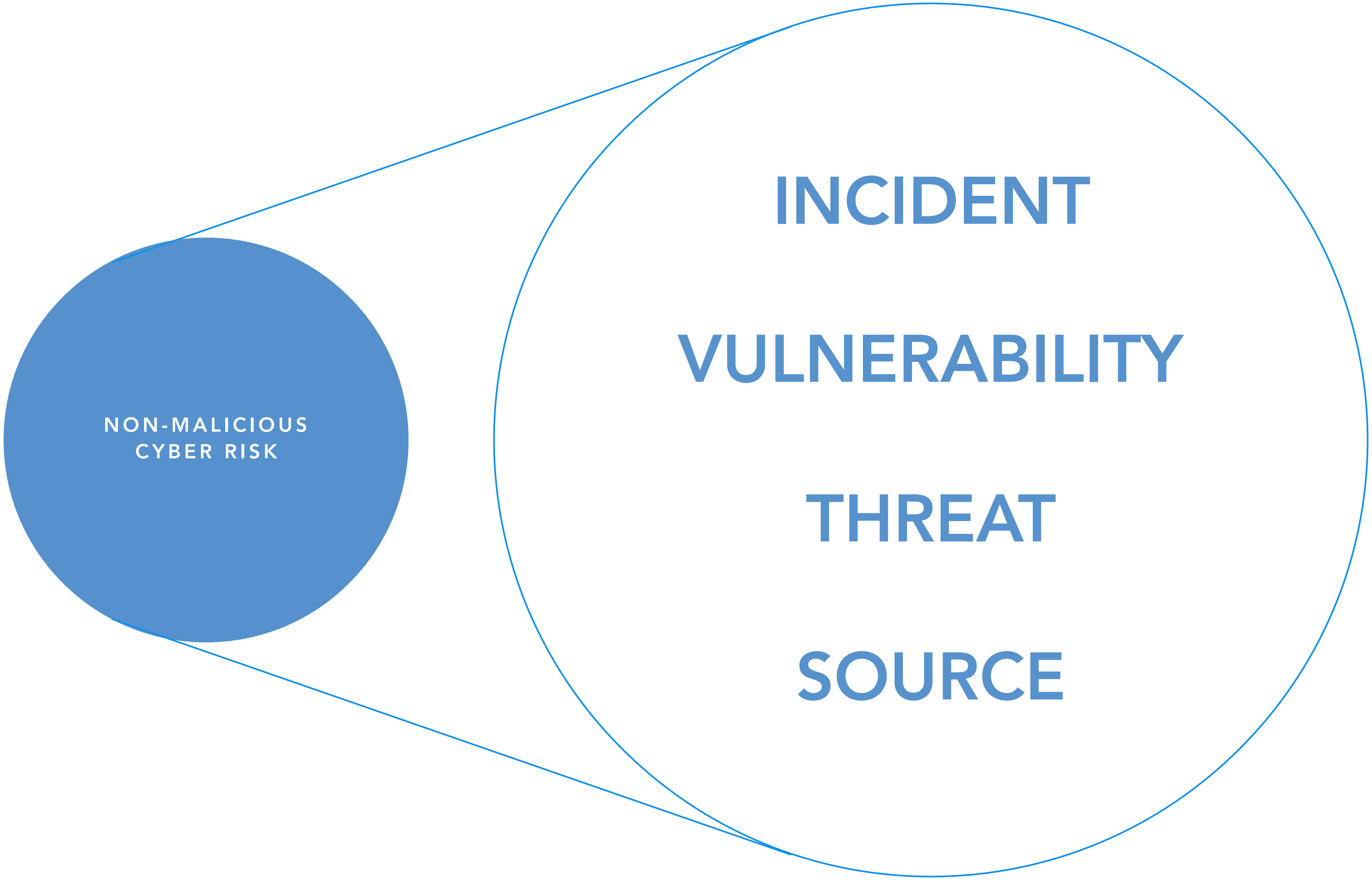
INCIDENTS FROM MALICIOUS THREATS

THREAT	INCIDENT	ASSET

INCIDENTS FROM MALICIOUS THREATS

THREAT	INCIDENT	ASSET
Signal sent from the central system to the limiter in the consumer	Bad signal issued to the limiter on the meter for specific consumers.	Energy supply.
Meter becomes infected with malware.	Malware interferes with the transmission of energy usage.	Meter data.
Meter becomes infected with malware.	Malware interfere with limiter function of the meter.	Energy supply.

NON-MALICIOUS



NON-MALICIOUS CYBER RISK

INCIDENT

VULNERABILITY

THREAT

SOURCE

IDENTIFICATION (NON-MALICIOUS)

- different **order of steps** for the identification for non-malicious cyber risks.
- they stem from accidents, consequently to ensure we focus so that we work our way back
- this is an useful approach but does necessarily need to be followed strictly.

INCIDENT

- consider the harm that can come to assets
- can make use of sources such as systems logs, monitored data, historical data etc

INCIDENTS FROM NON-MALICIOUS THREATS

ASSET	INCIDENT	DESCRIPTION

INCIDENTS FROM NON-MALICIOUS THREATS

ASSET	INCIDENT	DESCRIPTION
Energy provision.	Bugs in software disrupt the limiter.	Software designed to run on the meter may have errors in design that affect the limiter.
Meter Data Availability.	Maintenance on the meter disrupts transmission of energy usage.	Annual maintenance on the meter could result in faulty connection configuration of the meter.

VULNERABILITY

- attempt to **determine the vulnerabilities** that allow an incident to occur.
- typical vulnerabilities are often connected with the human element of the system.
- consider the training, sophistication, organisation as well stress and pressures.
- also consider technical vulnerabilities when considering non-malicious threats.

VULNERABILITIES ENABLING NON-MALICIOUS THREATS

INCIDENT	VULNERABILITY	DESCRIPTION

VULNERABILITIES ENABLING NON-MALICIOUS THREATS

INCIDENT	VULNERABILITY	DESCRIPTION
Bugs in software disrupt the limiter.	Poor design and testing.	Testing approaches used by the suppliers of software for meter are not effective.
Maintenance on the meter disrupts transmission of energy usage.	Heavy workload and inadequate training.	Overworked employees and lack of time for training on new systems and meters has led to problems.

THREAT

- determine the potential threats that could cause an incident due to the vulnerabilities
- we also try an understand the elements of the system that allow the threat to occur

NON-MALICIOUS THREATS

INCIDENT	THREAT	ENTRY POINT

NON-MALICIOUS THREATS

INCIDENT	THREAT	ENTRY POINT
Bugs in software disrupt the limiter.	Faulty software distributed to meters.	Meter.
Maintenance on the meter disrupts transmission of energy usage.	Errors during maintenance of meter.	Meter.

SOURCE

- for each threat we attempt to discover the source of these threats.
- focus on technical errors that might emerge from an individual interacting with system.

SOURCES OF NON-MALICIOUS THREATS

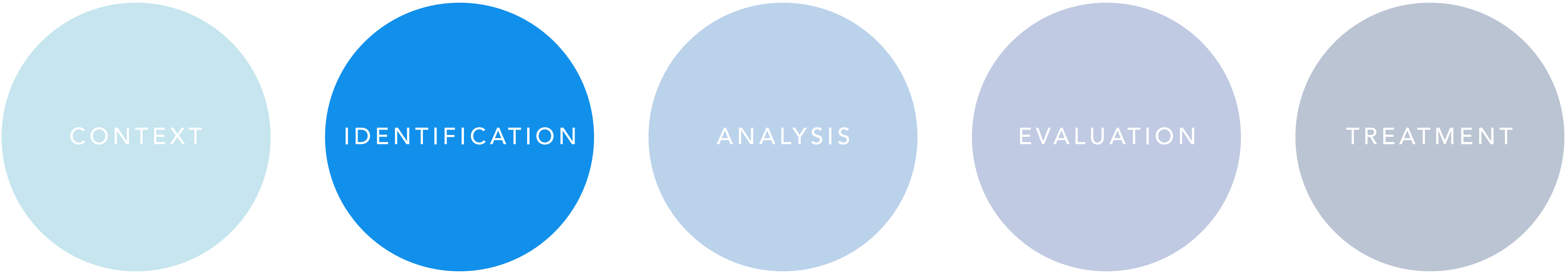
THREAT	SOURCE	DESCRIPTION

SOURCES OF NON-MALICIOUS THREATS

THREAT	SOURCE	DESCRIPTION
Faulty software distributed to meters.	Software bugs.	Software faults that stem from mistakes in design.
Errors during maintenance of meter.	Maintenance staff.	Mistakes by the maintenance staff during routine maintenance of the meter, interfere with configuration of connection.

TABLE DATA

- tables presented are useful for supporting understanding and use of evidence.
- examples presented are simple and sparse for presentation purposes.
- expect more detail and referencing of evidence to support estimates and arguments.



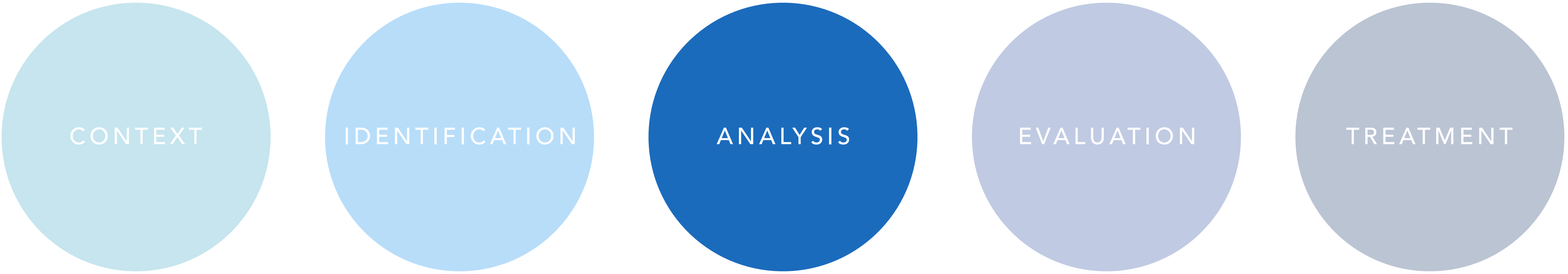
CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT



CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT

ANALYSIS

- challenge is to determine the **likelihood** of threats as well as the **consequences**.
- measuring and collection various data points can be overwhelming.
- understand the sources of threats, the essence of them, vulnerabilities exploited and resulting perceived incident.
- consult repositories of attacks and associated estimations of likelihood.

ANALYSIS

- typically look at non-malicious and malicious **separately**, but may be some crossover

- should also consider **combination** and should also tend to consider them as malicious

ANALYSIS

- likelihood of the **threats** actually occurring.
- severity of the **vulnerabilities** themselves
- determine if **incidents** are actually likely to happen.
- impact of the incident on **assets**.

ANALYSIS OF MALICIOUS THREATS

THREAT	**LIKELIHOOD**	ESTIMATE

ANALYSIS OF MALICIOUS THREATS

THREAT	LIKELIHOOD	ESTIMATE
Meter becomes infected with malware.		

LIKELIHOOD

VALUE	DESCRIPTION
Rare	Less Than 20 Years
Unlikely	Less Than 4 Years
Possible	Less Than 4 Times A Year
Likely	More Than Once A Month
Certain	Weekly

ANALYSIS OF MALICIOUS THREATS

THREAT	**LIKELIHOOD**	ESTIMATE
Meter becomes infected with malware.	**Rare**	Meter may be connected to cyber space but does not utilise off the shelf components and does not utilise any software targeted by potential identified malware.

VULNERABILITY ANALYSIS

- consider that the **ease for us to conduct testing**, ease for the potential **adversary**.
- make use of typical source, information experts and open repositories.
- can also perform vulnerability scans and security testing as well as penetration testing.
- for non-malicious threats we are trying to understand what barriers are missing to stop accidents.

VULNERABILITY ANALYSIS FOR MALICIOUS THREATS

VULNERABILITY	SEVERITY	EXPLANATION

VULNERABILITY ANALYSIS FOR MALICIOUS THREATS

VULNERABILITY	SEVERITY	EXPLANATION
Antivirus protection not up to date.	High	The antivirus software on the meter system is rarely updated.

LIKELIHOOD

- initial likelihood of incident can be estimated from considering the **threats** and **vulnerabilities** they exploit.

- consider an **incident**, that is due to a **threat** exploiting a **vulnerability**.

LIKELIHOOD AND CONSEQUENCES FOR MALICIOUS THREATS

INCIDENT	ASSET	LIKELIHOOD	CONSEQUENCE

INCIDENTS FROM MALICIOUS THREATS

THREAT	INCIDENT	ASSET
Signal sent from the central system to the limiter in the consumer	Bad signal issued to the limiter on the meter for specific consumers.	Energy supply.
Meter becomes infected with malware.	**Malware interferes with the transmission of energy usage.**	**Availability of Meter Data.**
Meter becomes infected with malware.	Malware interfere with limiter function of the meter.	Energy supply.

ANALYSIS OF MALICIOUS THREATS

THREAT	LIKELIHOOD	ESTIMATE
Meter becomes infected with malware.	Rare	Meter may be connected to cyber space but does not utilise off the shelf components and does not utilise any software targeted by potential malware.

LIKELIHOOD AND CONSEQUENCES FOR MALICIOUS THREATS

INCIDENT	ASSET	LIKELIHOOD	CONSEQUENCE

LIKELIHOOD AND CONSEQUENCES FOR MALICIOUS THREATS

INCIDENT	ASSET	LIKELIHOOD	CONSEQUENCE
Malware interferes with the transmission of energy usage.	Availability of Meter Data	Rare	

CONSEQUENCES (AVAILABILITY)

VALUE	DESCRIPTION
Insignificant	Less Than 12 Hours
Minor	Less Than 24 Hours
Adequate	Less Than 3 Days
Significant	Less Than 7 Days
Critical	More Than 21 Days

LIKELIHOOD AND CONSEQUENCES FOR MALICIOUS THREATS

INCIDENT	ASSET	LIKELIHOOD	CONSEQUENCE
Malware interferes with the transmission of energy usage.	Availability of Meter Data	Rare	Adequate

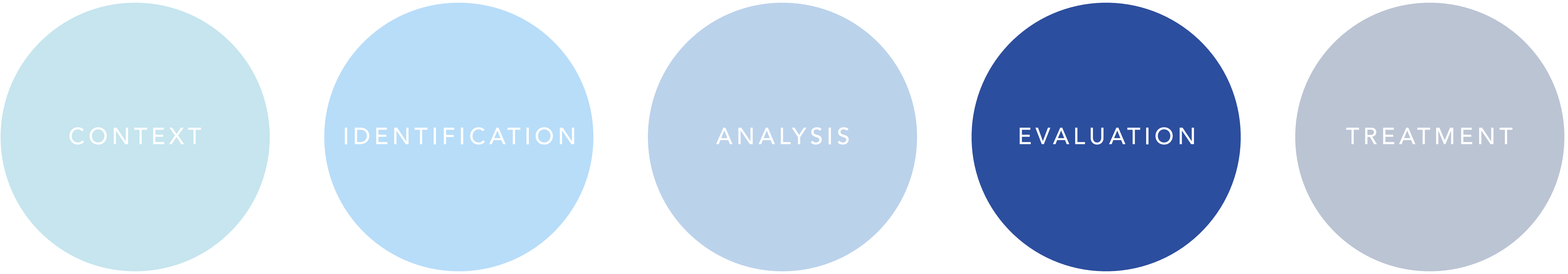
CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT



CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT

EVALUATION

- risk **consolidation**, risk **evaluation** and risk **aggregation** and risk **grouping**
- consolidation: focus on risks with uncertain estimates and where this may sway levels.
- for aggregation we must consider risks together that yield higher risk level
- grouping to similar level, distinction are the malicious and non malicious

CONSOLIDATION

- purposes of consolidation is to ensure correct risk level is assigned to each.
- focus is the risk level is correct, not so much the consequences and likelihood.
- ensure proper consideration of malicious and non-malicious risk as well as the combination.
- key-decision makers may decide to alter aspects of context after insight drawn from the process.

RISK EVALUATION

LIKELIHOOD

CONSEQUENCE

	RARE	UNLIKELY	POSSIBLE	LIKELY	CERTAIN
CRITICAL	🟧	🟥	🟥	🟥	🟥
SIGNIFICANT		🟧	🟥	🟥	🟥
ADEQUATE			🟧	🟥	🟥
MINOR				🟧	🟥
INSIGNIFICANT					🟧

AGGREGATION

- several risk may actually progress in a similar direction or nature, may consider aggregating together.
- incident harms **different assets of the same party**, example independently they may have low consequences, combined could higher consequences.
- separate incidents may be **variant of a common abstraction** or two incidents stems from the **same threat**.

GROUPING

- treatments may address several risks, consequently may be advisable to group risk together.
- groups risks together may support higher expense, than seeking costs for treatment of single risk.
- already have grouping of sorts in terms of malicious and non-malicious concerns.
- other groups could include common vulnerabilities, sources of threat and threats themselves.

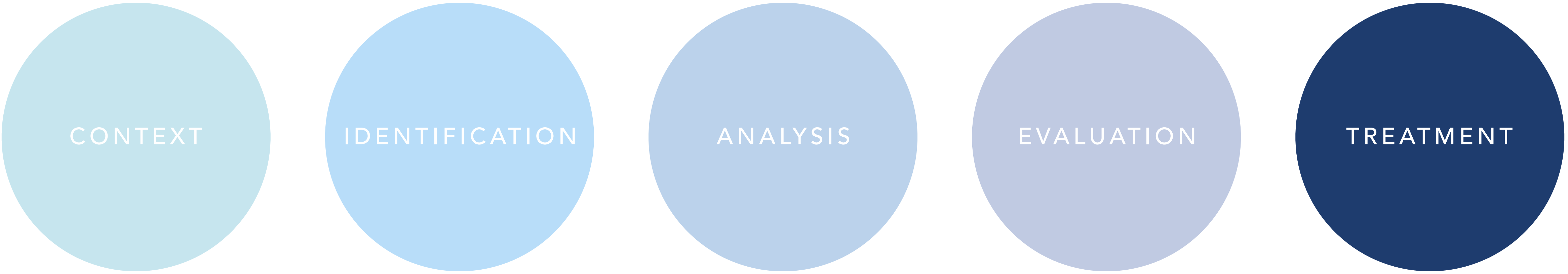
CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT



CONTEXT

IDENTIFICATION

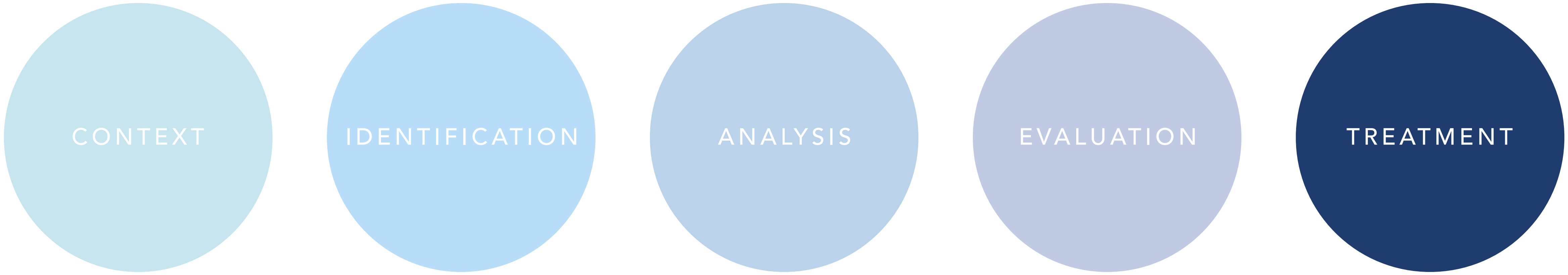
ANALYSIS

EVALUATION

TREATMENT

TREATMENT

- aim is focus on the most important risks, simply not realistically to address all perceived risks.
- threats are technical in nature and so often are solutions are very technical.
- the separation of non malicious and malicious has implications for how we treat them.
- need to consider the estimate effect on risk level on risks before considering cost.



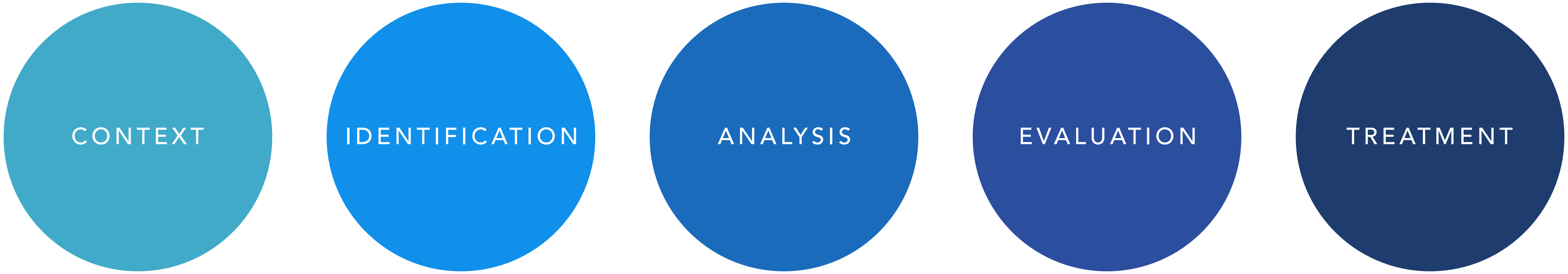
CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT



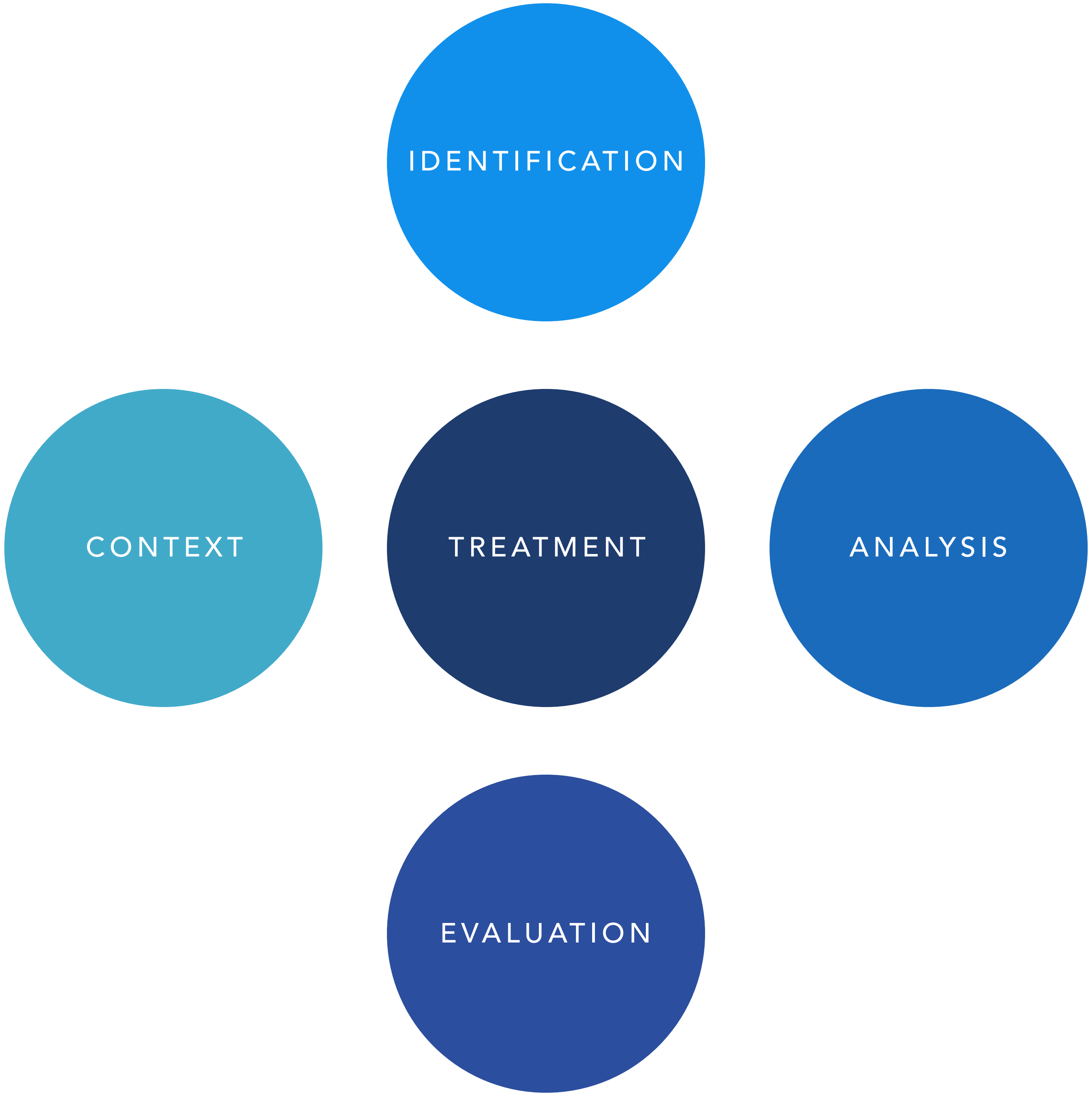
CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT



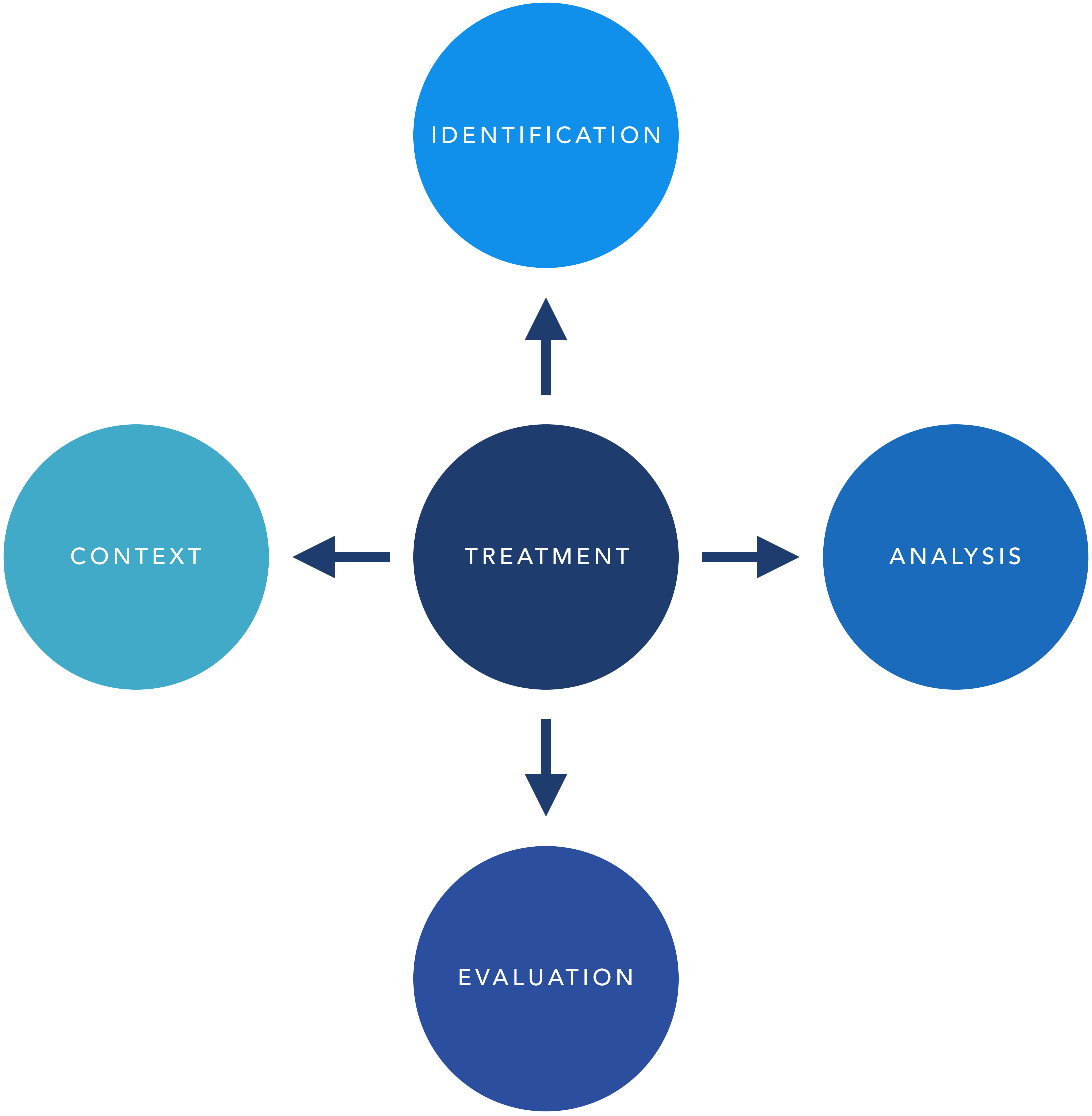
IDENTIFICATION

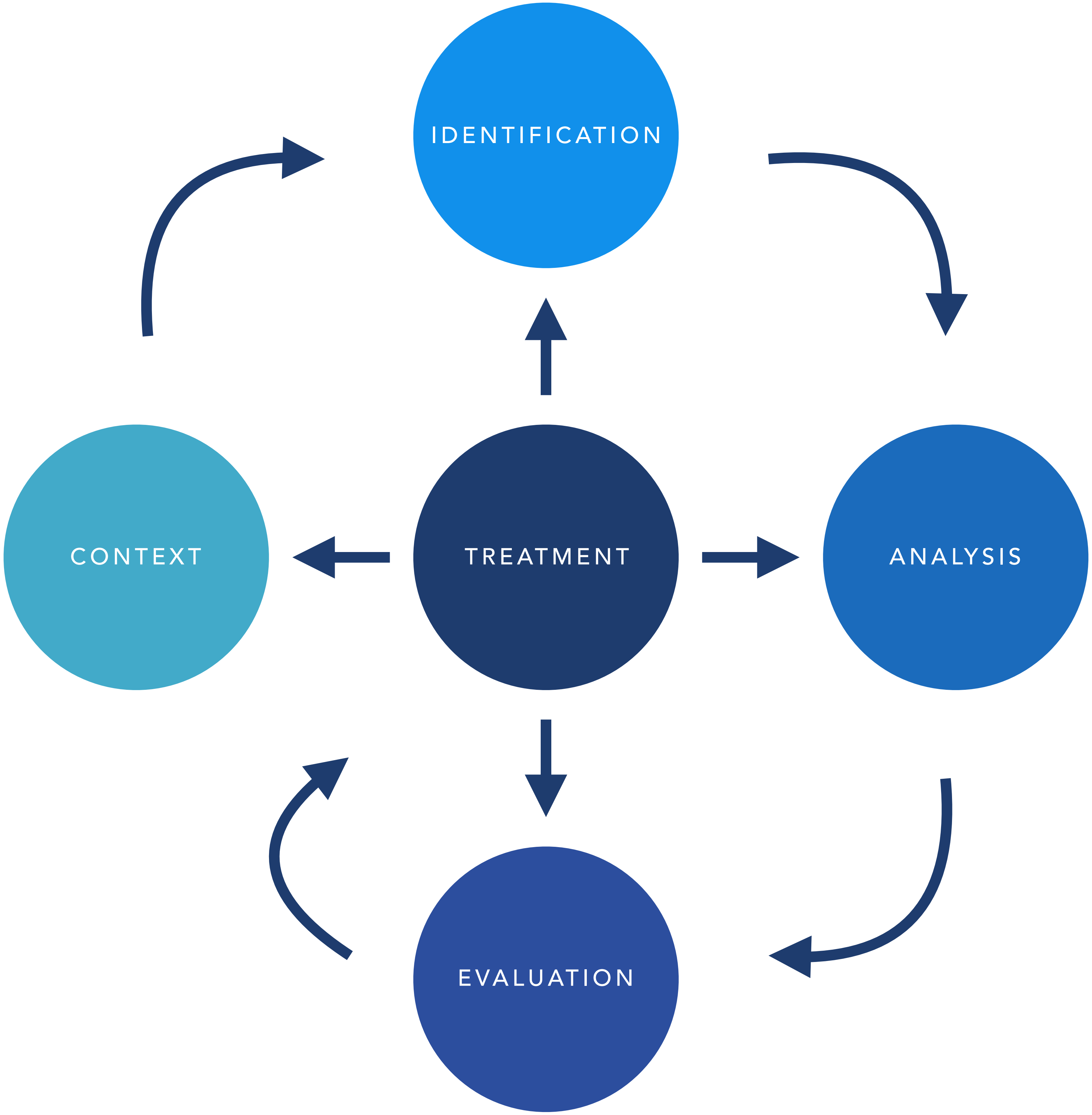
CONTEXT

TREATMENT

ANALYSIS

EVALUATION


IDENTIFICATION
CONTEXT
TREATMENT
ANALYSIS
EVALUATION


IDENTIFICATION
CONTEXT
TREATMENT
ANALYSIS
EVALUATION

OVERVIEW

- consider the cyber risk assessment process in more detail.
- small group teaching using your assignment groups to discuss and develop outputs for each stage.
- use running example to walkthrough various stages of the cyber risk approach.