ENTERPRISE CYBER SECURITY

CYBER RISK MANAGEMENT

University of Glasgow

OVERVIEW

- principles of risk management, risk management framework and risk management process itself.
- refining the aforementioned to support cyber risk assessment.
- understand the difference between non-malicious and malicious risk.

RISK MANAGEMENT

RISK MANAGEMENT

- activities used to coordinate efforts and employees with regards to risk.

- risk management process should be built atop a framework and principles.

- framework should supporting integrating the risk management process itself in the management processes for an enterprise.

RISK MANAGEMENT

PRINCIPLES

FRAMEWORK

PROCESS

PRINCIPLES

PRINCIPLES OF RISK MANAGEMENT (ISO31000)

- **creates and protects value** by contributing to the objectives of the enterprise and improving processes.
- **part of all processes** and is the responsibility of every manager and employee, not a single individual.
- **integral to decision making** as it supports allocation of scare resources and prioritisation of efforts.
- **explicitly addressing uncertainties** an enterprise will encounter.

PRINCIPLES OF RISK MANAGEMENT (ISO31000)

- **systematic and structured process** to management to ensure consistent, comparable and reliable results.

- **based on strong evidence** and data drawn from multiple sources.

- strong evidence can include historical data, research papers, forecasts, observation, expert opinion and stakeholder feedback.

- **tailored to the enterprise** in terms of their risk appetite and external/internal considerations.

PRINCIPLES OF RISK MANAGEMENT (ISO31000)

- **consider human factors** and individual differences of employees.

- **transparent and inclusive** in terms of employee contracts, annual reviews and all stakeholders kept up-to-date.

- **responsive and iterative** to changes in environment and introduce of new avenues of risk.

- **support continual improvement** to ensure the risk management process remains effective and efficient.

FRAMEWORK

RISK MANAGEMENT FRAMEWORK

- purpose of the risk management process must be part of the **overall management of the enterprise**.

- risk management framework is designed to support **integrating risk management** into overall management.

- risk management framework should be built up on the **principles of risk management**.

- principle is to create and protect value, need to understand and appreciate the business objectives.

DESIGN

- understand the **external** forces on the enterprise in terms of stakeholders, influences and environment.
- understand the **internal** culture, governance, standards, procedures and stakeholders of the enterprise.
- formulate and define **commitment** to risk management and communicate direction or intention.
- determine **accountability** for risk and how performance will be measured and escalation handled.

RISK MANAGEMENT FRAMEWORK

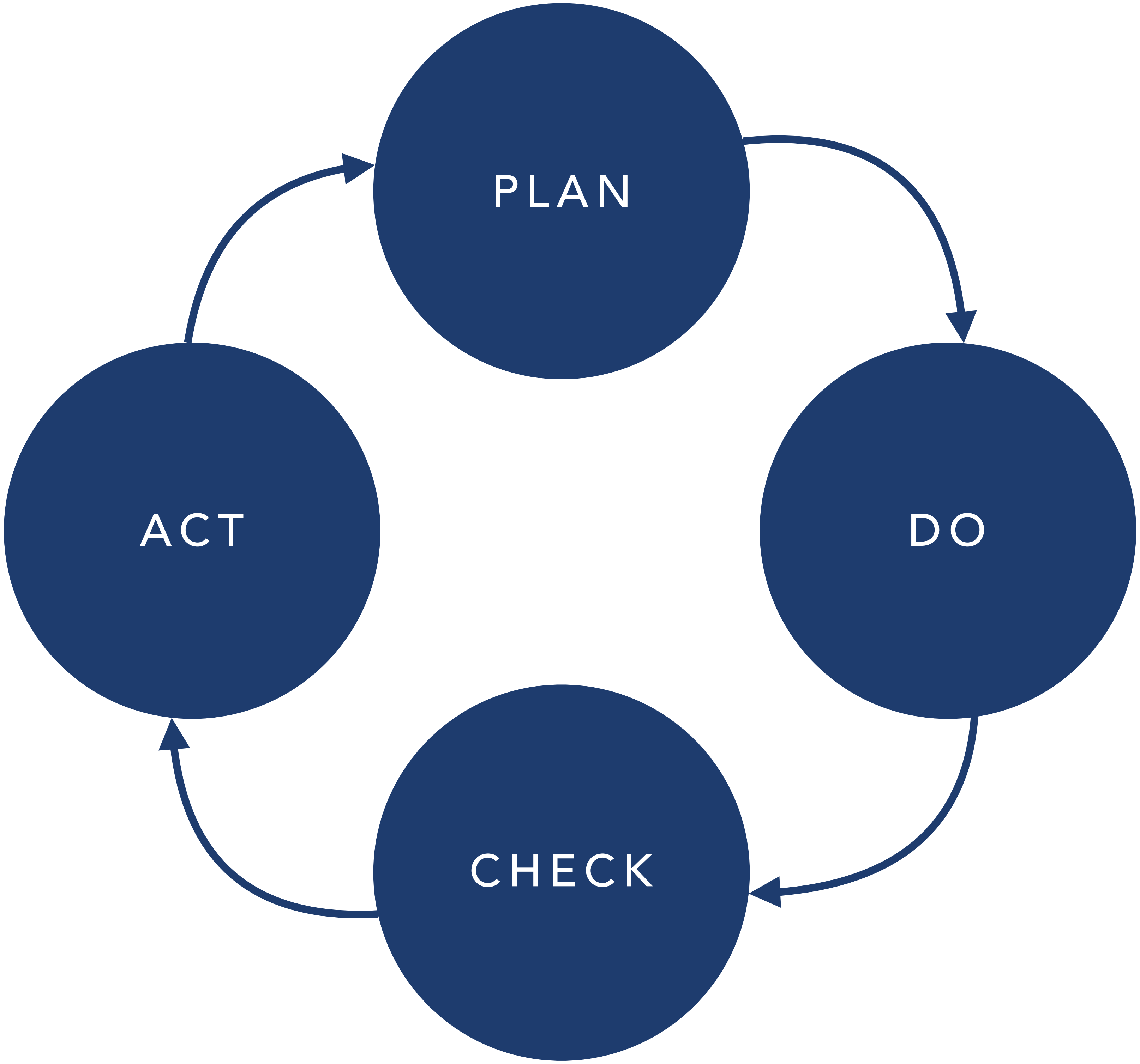
- allocate **dedicate resources** to the process of risk management to ensure it is effective.
- establish clear **communication mechanisms** for internal and external actors.
- **implement risk management** within the general management approach of the enterprise.

PLAN, DO, CHECK, ACT (PDCA)

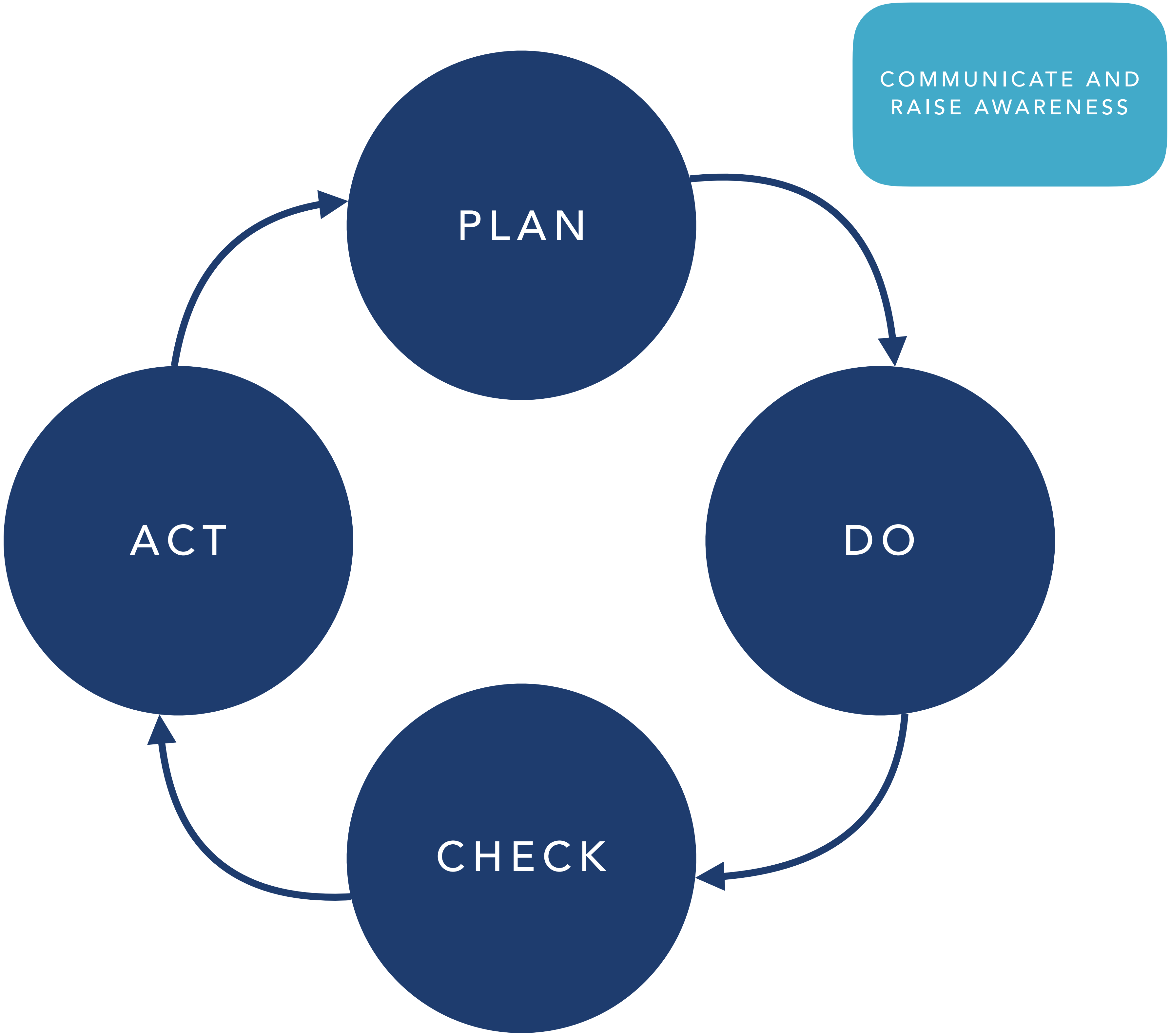
PDCA

- proposed by Edwards Deming as an approach to improve effectiveness of business processes.
- understand the problem by collecting and analysing data, devise a plan to address it.
- develop a solution to the problem and deploy it, collect measurements to understand effectiveness.
- check that solution actually addresses the perceived problem.
- produce report, communicate changes and identify the next set of problems.

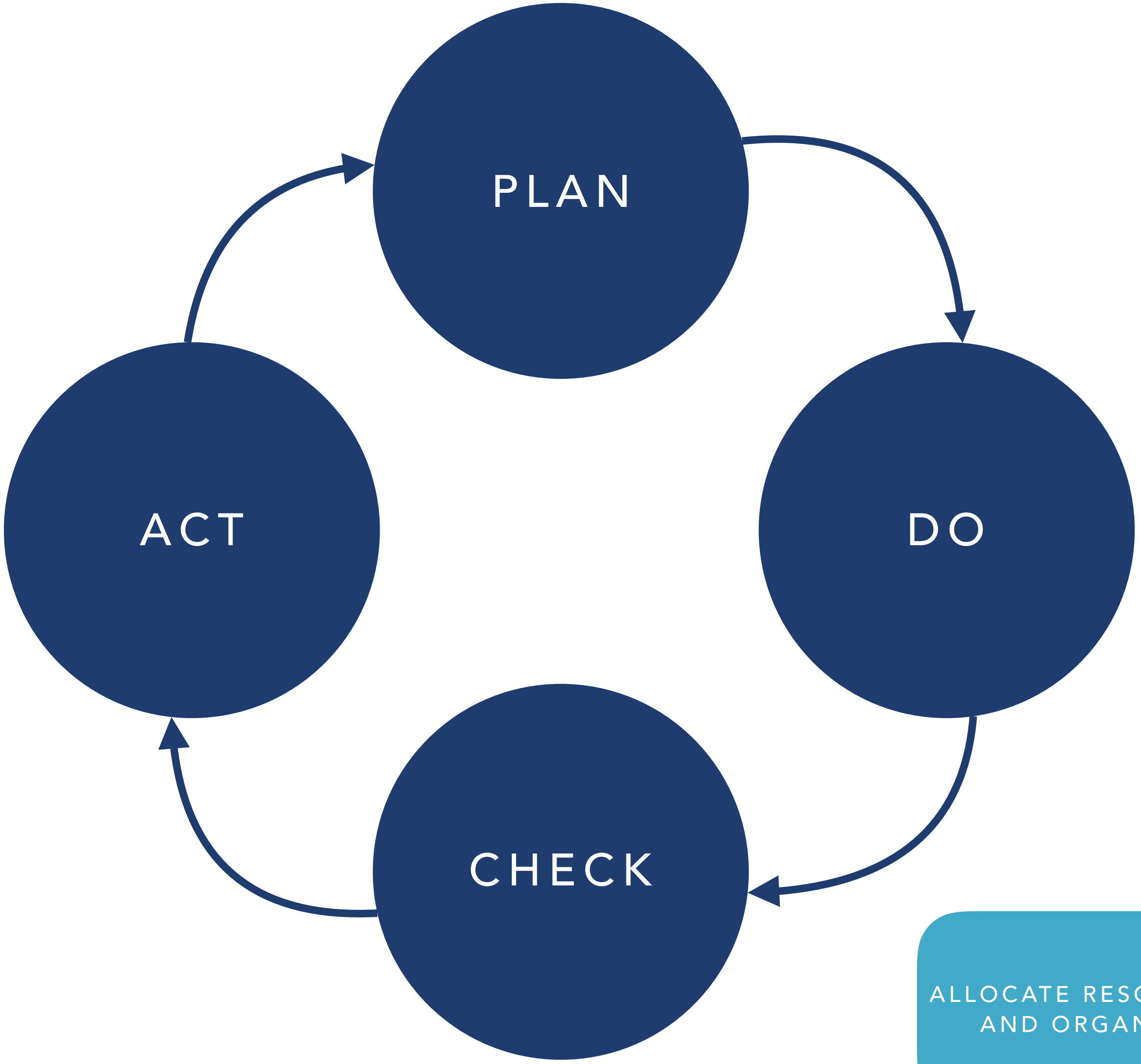
PDCA



PDCA

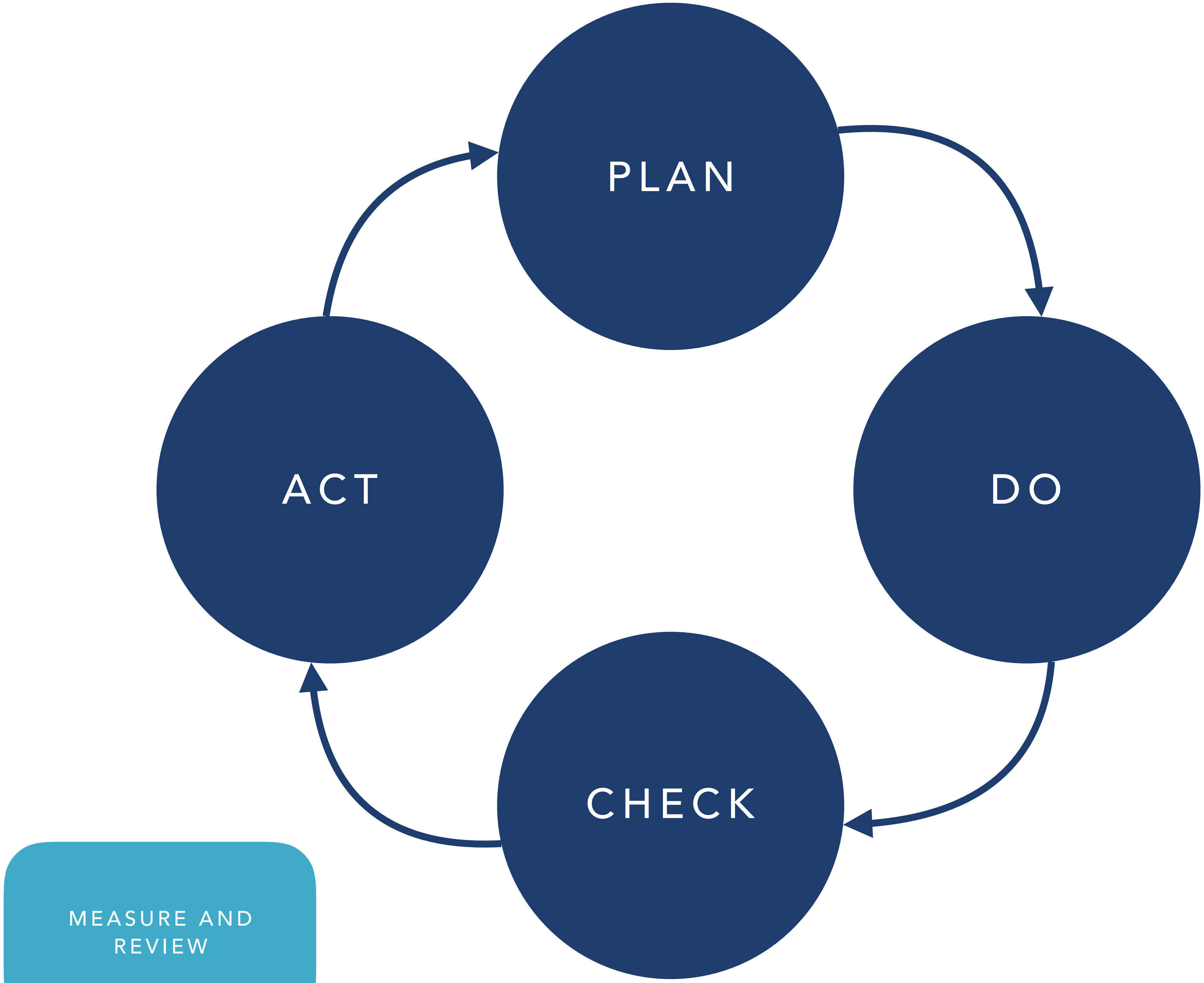


PDCA



ALLOCATE RESOURCES AND ORGANISE

PDCA



PLAN

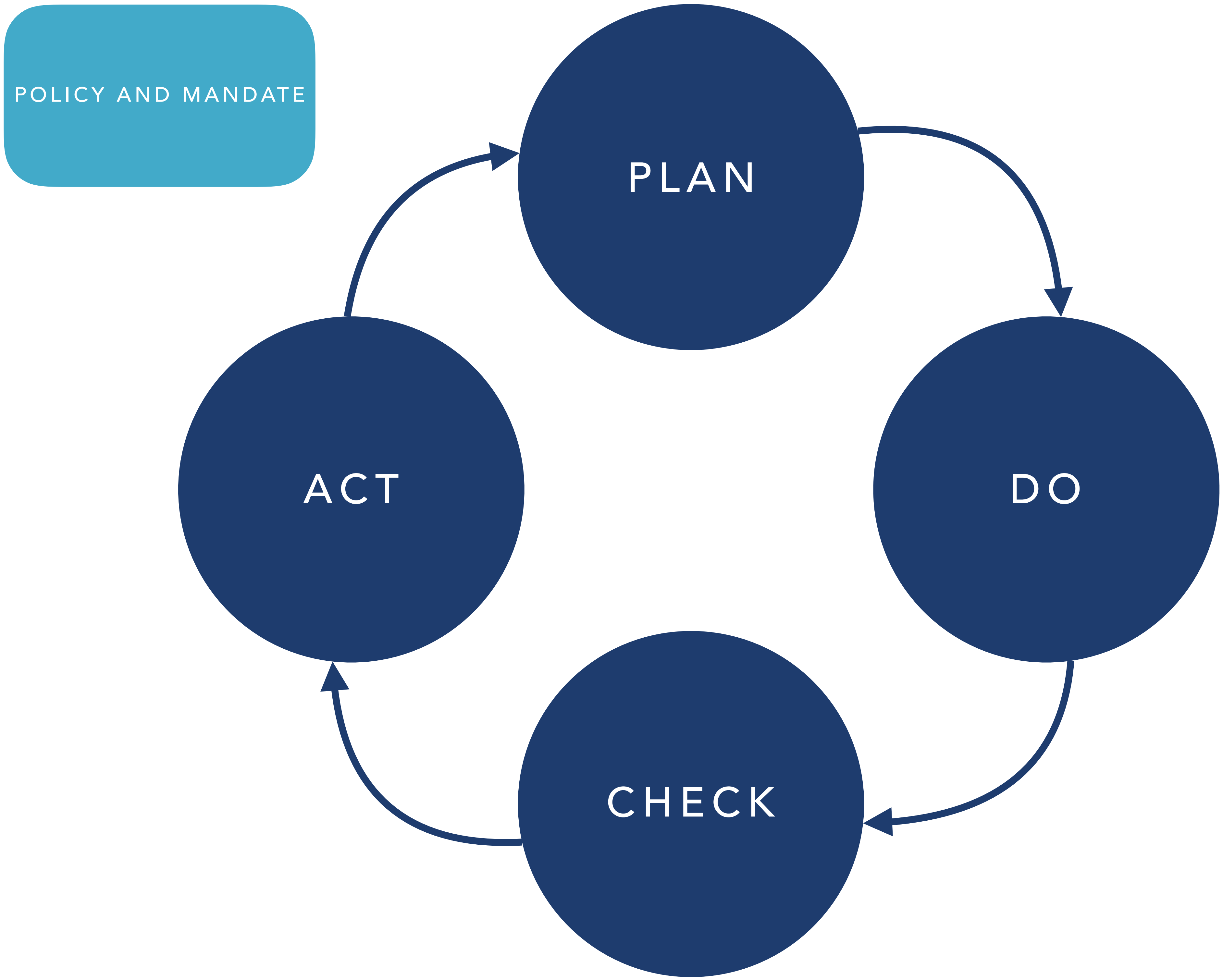
DO

CHECK

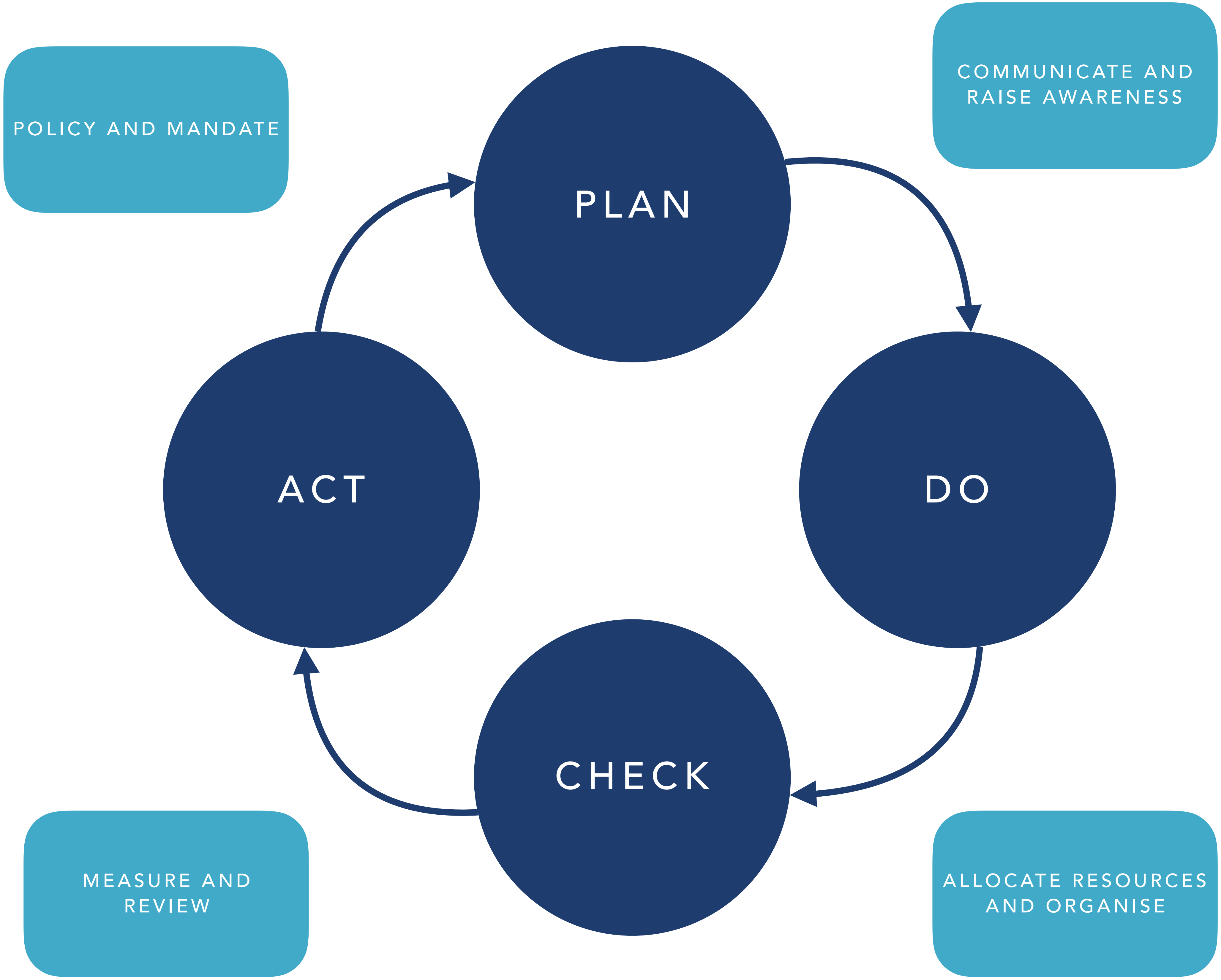
ACT

MEASURE AND REVIEW

PDCA



PDCA



POLICY AND MANDATE

COMMUNICATE AND RAISE AWARENESS

PLAN

ACT

DO

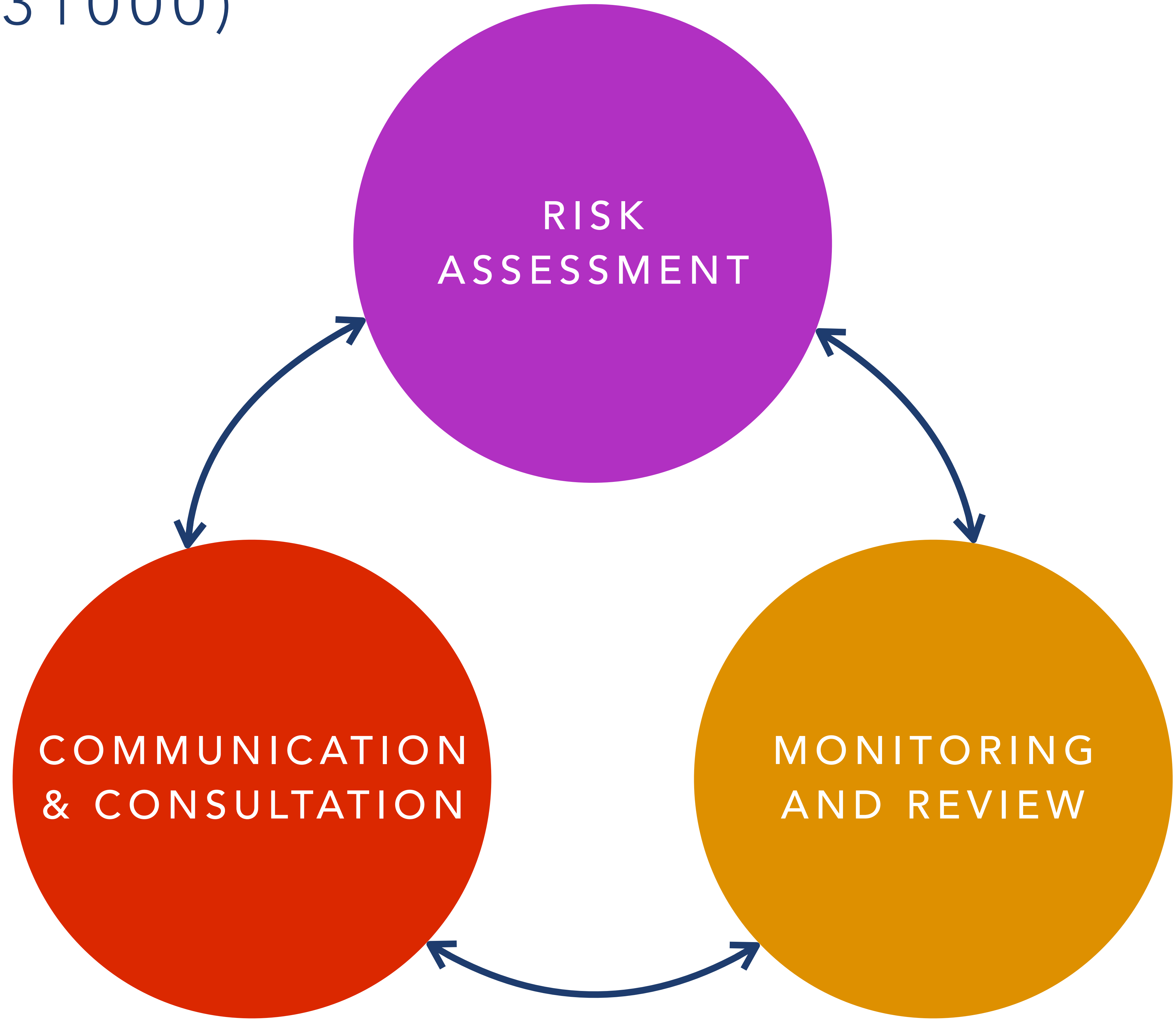
CHECK

MEASURE AND REVIEW

ALLOCATE RESOURCES AND ORGANISE

PROCESS

RISK MANAGEMENT PROCESS (ISO31000)



RISK ASSESSMENT

COMMUNICATION & CONSULTATION

MONITORING AND REVIEW

COMMUNICATION AND CONSULTATION

COMMUNICATION AND CONSULTATION

- processes that obtain, provide and share information pertaining to risk with stakeholders.
- information sharing should support decision making throughout the enterprise.
- communication of risk should be championed, planned and endorsed by management.
- management support for risk management is crucial in ensuring an effective and efficient process.

TEAM

- team tasked with obtaining and sharing information with internal and external stakeholders.

- effective communication of risk management process ensure responsibility is shared and understood throughout enterprise.

- team may comprise of internal and external stakeholders, key decision makers and knowledgeable staff.

- subsystems may option for a risk-lead rather than a team, focus is on communication and consultation not isolation.

PLAN

- perceptions may different within an organisation, between business units and other subsystems.
- such perceptions need to be considered when attempting to address risk within an enterprise.
- team should develop procedures and plans to support the overall risk management process.
- focusing on ensuring the relevant evidence is gathered and that important stakeholders are consulted.

ENDORSEMENT

- effective risk management requires key-decision makers and employees to proceed in the same way.

- communication of risk management process cements the importance within the organisation.

- consultation risk with essential employees and key-decision makes ensures they understand their responsibility for risk management.

MONITORING AND REVIEW

MONITORING AND REVIEW

- review the framework for risk management as well as the process itself.
- understand any legal or competition changes that may mean parts of either need to be reconsidered.
- review asset value, internal and external context changes that may introduce new threats as well as the possibility of new vulnerabilities.
- ensure the framework itself is compliment to the business objectives and policies.

RISK ASSESSMENT

CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT

CONTEXT

- determine the goals as well as the **external** and **internal** factors that have influence.
- define the **target of assessment** in terms of the people and process that are of interest.
- understanding the target and assets we can develop **scales** and **evaluation** criteria.
- determine risk level from the output of considering likelihoods and consequences.

IDENTIFICATION

- documenting possible risks and risk sources.
- risks are always associated with an incident.
- risks can not exist if there is no asset, vulnerability and threat.
- aim is to understand threats, that exploit vulnerabilities that lead to incidents.

IDENTIFICATION

- need to consider what the sources of threats.
- threats could come from individuals or they could come from other sources, e.g. fire.
- threats sources can be tangible or intangible.
- identification of some threats or incidents may lead to the identification of others.

ANALYSIS

- determine the actual risk level from the identified risks.
- need to consider the consequences and likelihood together.
- consider that actual source of threats thoroughly and if they are likely to actually arise.
- determine the risk level using the functions determines during context definition.

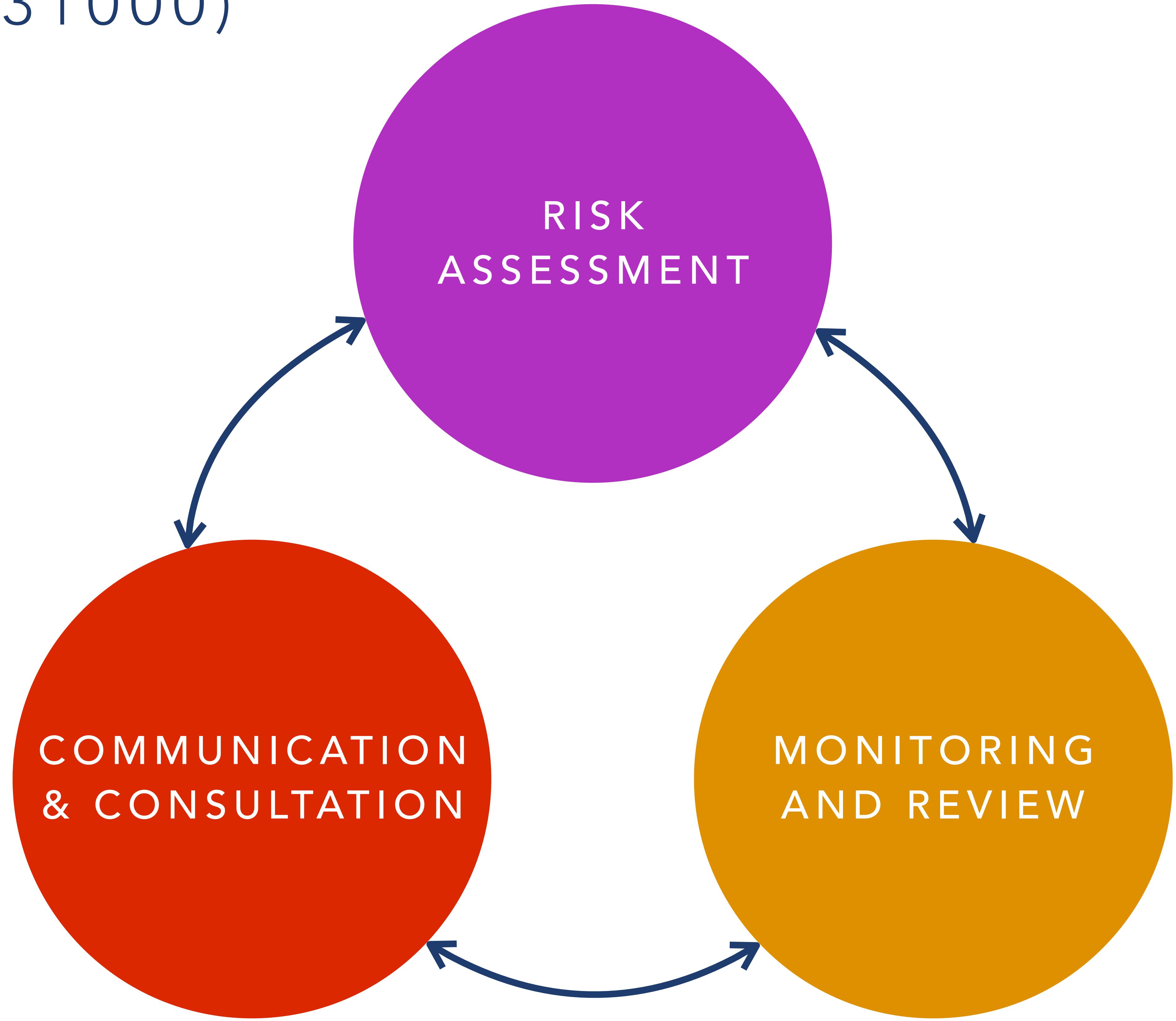
EVALUATION

- risks have been identified and throughly considered, the next step is determine the risks to receive treatment.

- consider the risks once again with stakeholders to be determine if original perception was accurate.

- consider grouping risks that share similar characteristics, for example threat source etc.

RISK MANAGEMENT PROCESS (ISO31000)



RISK MANAGEMENT

PRINCIPLES

FRAMEWORK

PROCESS

CYBER RISK MANAGEMENT

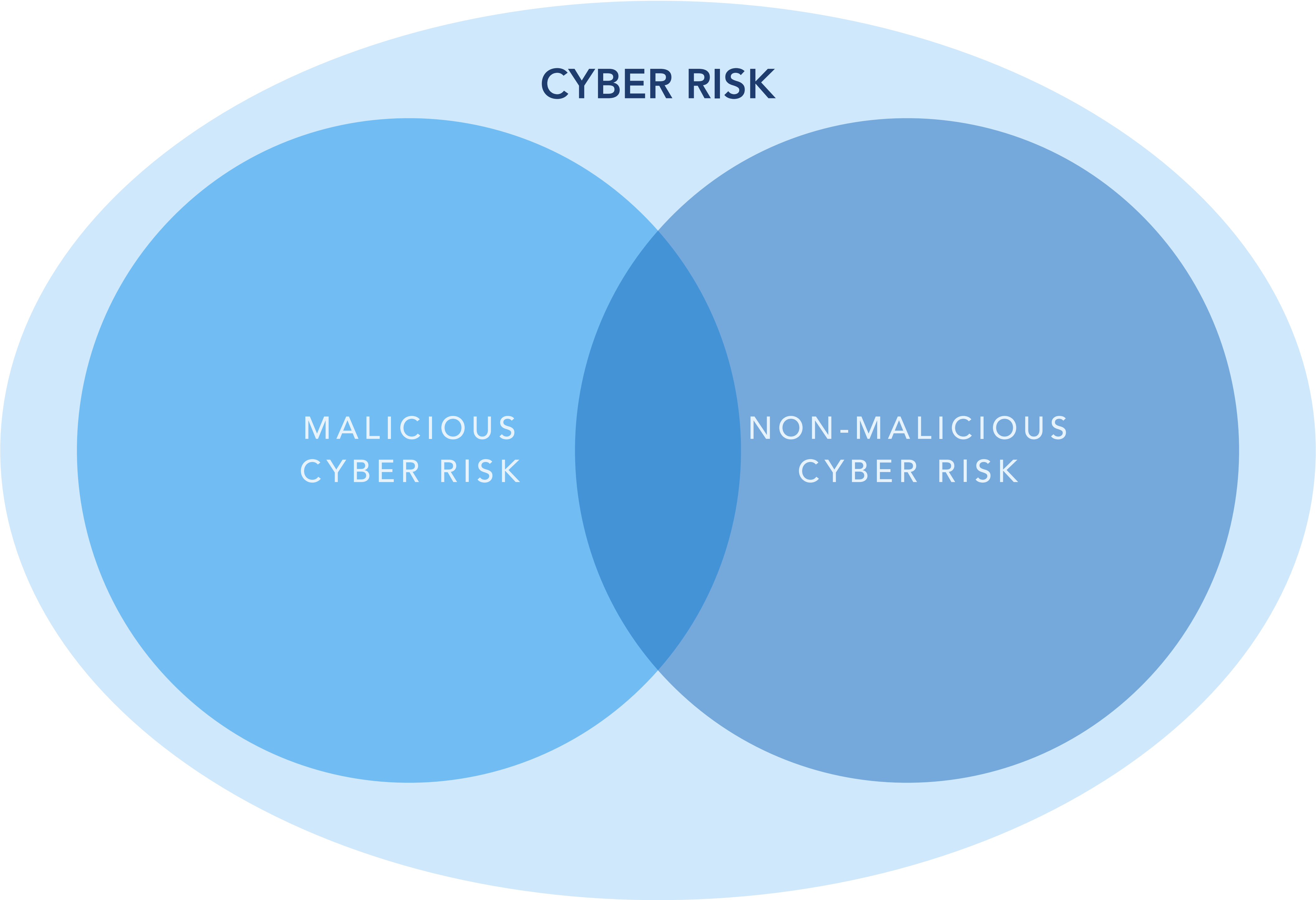
CYBER RISK MANAGEMENT

- cyber space does influence the threats and risks an enterprise has to consider.

- cyber space is so vast, expansive and connects so many subsystems, that sources of threats could come from many different places.

- cyber risk management is primarily concerned about cyber threats, threats exploiting cyber space.

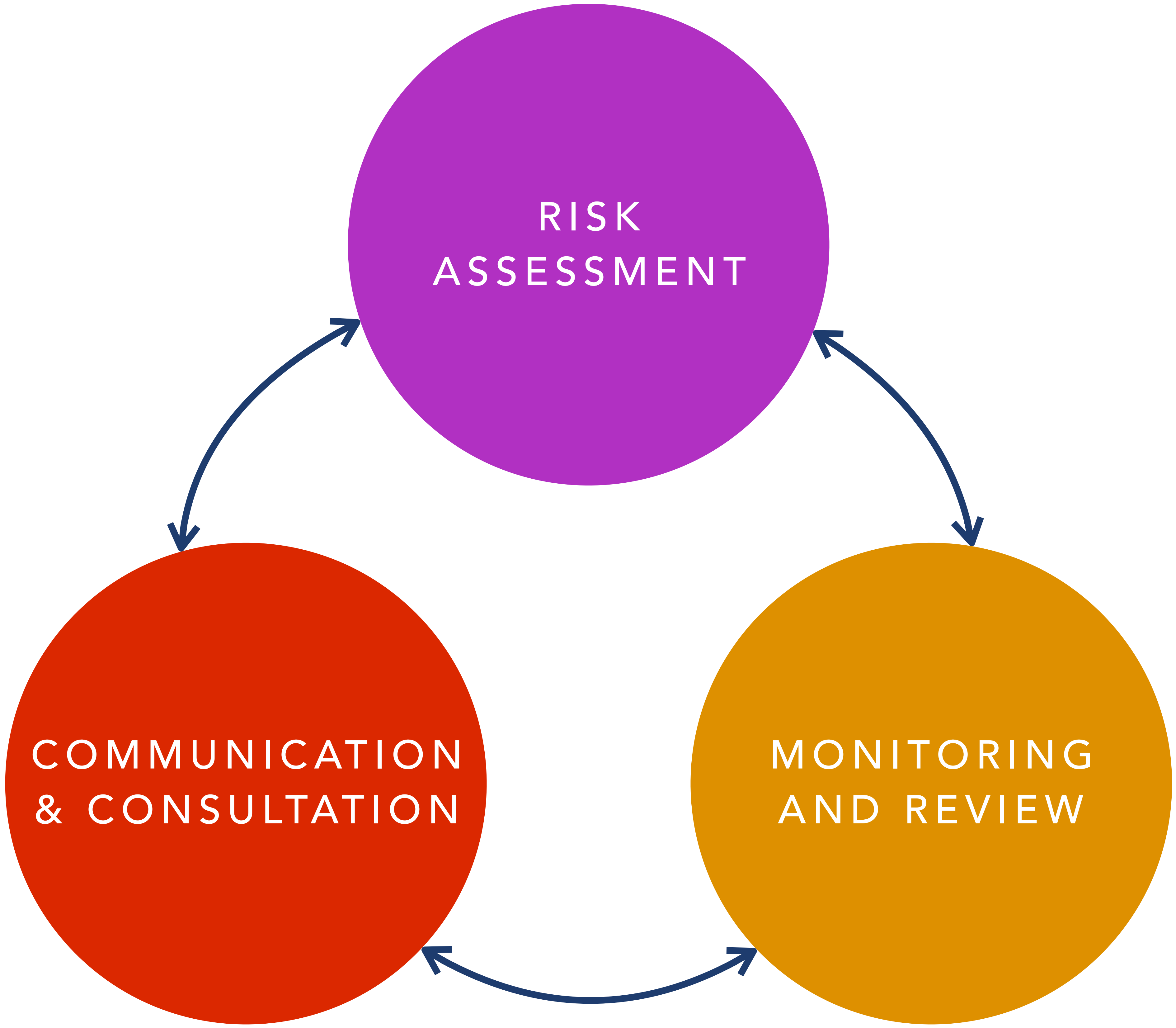
- cyber systems can be exposed to many threats, not all related to cyber space, floods and fires for example.


CYBER RISK
MALICIOUS CYBER RISK
NON-MALICIOUS CYBER RISK

CYBER RISK

- The nature of cyber risk can be categorised as **malicious** or **non-malicious**.
- Cyber-risk can also be considered both malicious and non-malicious.
- Cyber-risk could also be the product of both a malicious and non-malicious threat.

CYBER RISK MANAGEMENT PROCESS



RISK ASSESSMENT

COMMUNICATION & CONSULTATION

MONITORING AND REVIEW

COMMUNICATION AND CONSULTATION OF CYBER RISKS

COMMUNICATION AND CONSULTATIONS OF CYBER RISKS

- cyber systems ensures that stakeholders could come in many different forms and from many different places.

- consider the research, cloud service providers, customers, external clients.

- need to consider the optimal approach to communicate and consulate with these stakeholders.

- plans and procedures need to be developed and utilised to ensure a consistent approach in retrieving and sharing information.

COMMUNICATION AND CONSULTATIONS OF CYBER RISKS

- cyber space also ensures there potentially many more threats stemming from several different locations.

- consider the research, resources to utilise vulnerabilities and mount attacks is low.

- significant global events or incidents could have ripples across multiple organisations.

- also consider the research, in terms of the complexities introduced in certain deployments.

COMMUNICATION AND CONSULTATIONS OF CYBER RISKS

- wealth of data pertaining to numerous vulnerabilities, threats and incidents could be overwhelming to enterprises.

- establish categories and classifications to support better understanding and more informed decision making.

- recall the system attacking us, attackers are much better at sharing, disclosing and categorising information.

- employ standards, best practice as well as contribute and utilise repositories and stores of known information, e.g. Common Vulnerabilities and Exposures (CVEs) .

MONITORING AND REVIEW

MONITORING CYBER RISK

- able to keep many logs as well as gathering information from various other technical solutions, for example intrusion detection systems.
- develop internal **risk register** that compiles the known threats and vulnerabilities for stakeholders.
- develop and monitor important metrics relevant to cyber risk and use to have a clear illustration of overall cyber risk to the enterprise, for example failed authentication attempts.

CYBER RISK ASSESSMENT

CYBER RISK ASSESSMENT

- cyber space is **vast**, expansive and connects so many subsystems, that sources of threats could come from many different places.

- complexity associated with cyber space and systems ensures that there could be numerous **non-malicious** and **malicious** threats.

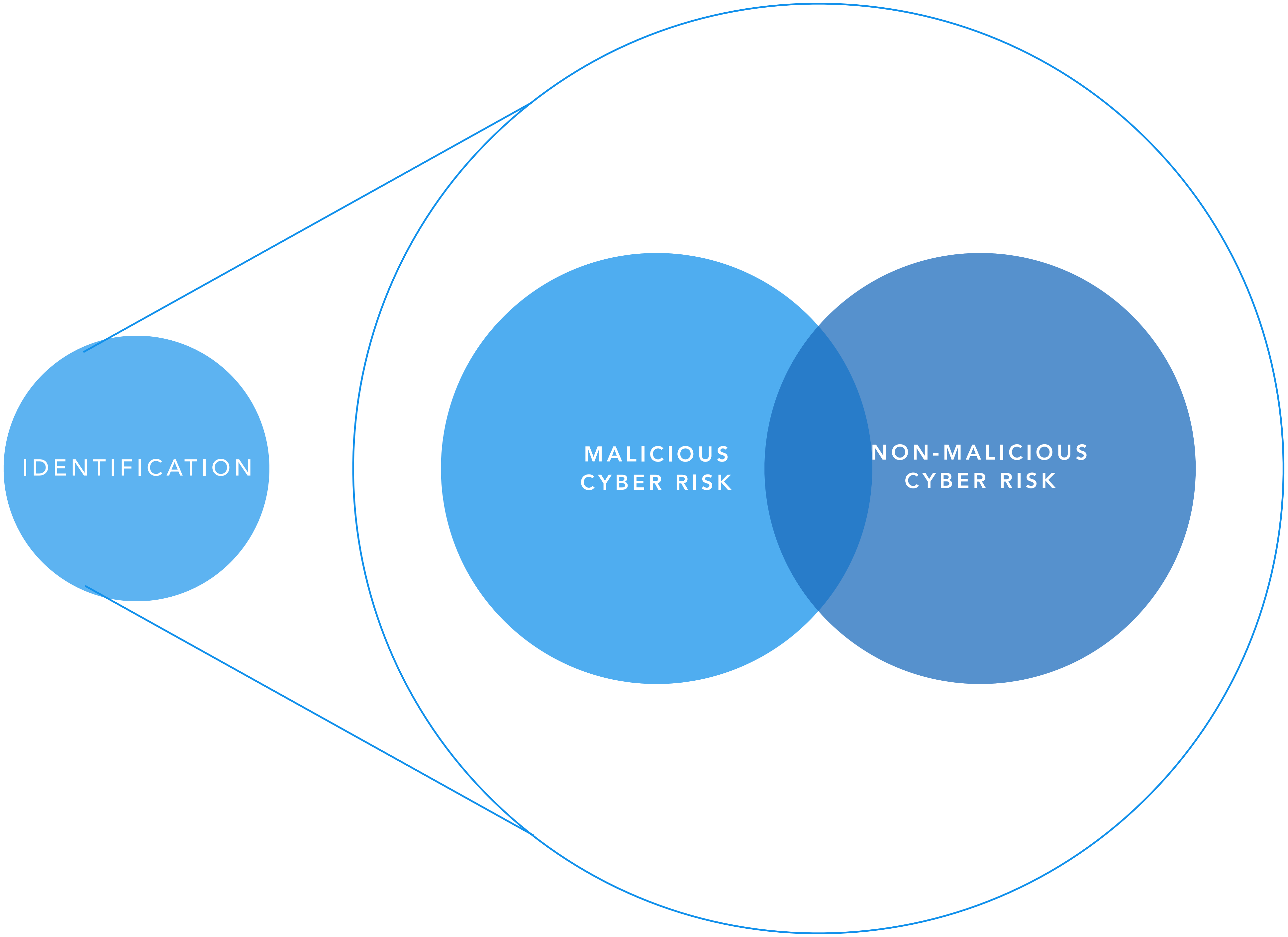
CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT


IDENTIFICATION
MALICIOUS CYBER RISK
NON-MALICIOUS CYBER RISK

CONTEXT

IDENTIFICATION

ANALYSIS

EVALUATION

TREATMENT

CONTEXT

- understand how the **cyber system interacts** with cyber space, including connections.
- need to consider the **attack surface** of the cyber system with cyber space, i.e. entry and exit points for threats and data.
- connection of cyber system to cyber space helps informs identification of risk.
- also need to appreciate the wider implications from exploitation of threats, reputation for example.

IDENTIFICATION

- consider the research, cyber risks to the enterprise can be non-malicious and/or malicious.

- it is an important aspect of the identification stage within cyber risk assessment.

- non-malicious risk could give rise to a malicious risk.

MALICIOUS INTENT

- adversaries in a game, the aim is to win the game by predicting the moves of our adversary.
- risk assessment is observing the game and furnishing our opponent with guidance.
- adversarial attack strategies are constrained in terms of strengths and weakness.
- understand the adversaries and document the threats, then they can be subsequently analysed.

NON-MALICIOUS INTENT

- no attack strategy, no malicious intent or any real motive in attempting to cause harm to the enterprise.

- influences the approach to determine the different risks.

- understand the assets, incidents that could involve these assets.

- leading to understanding the vulnerabilities, threats and sources that can allow the incident to occur.

ANALYSIS

- cyber systems afford enterprise significant insight in terms of testing, monitoring and logging that can greatly enhance analysis of the risk identified.

- malicious threats that are derived by individual intent can be incredibly difficulty to properly assess in terms of likelihood.

ANALYSIS

- MITRE corporation manages the **Common Vulnerabilities and Exposures (CVE)** reference system for known issues in general release software.

- includes consideration of typical consequences and the impact from exploit of vulnerability.

- **National Vulnerability Database (NVD)** is a repository for issues, also attempts to quantify risks in CVE.

- **Open Web Application Security Project (OWASP)** issues charts about common vulnerabilities for various applications.

EVALUATION

- differences emerge because of the presence of malicious and non-malicious risks.
- consolidation of cyber risk needs to consider the likelihoods for both non-malicious and malicious risks.
- integrity, for example, through disruption of data - determine the likelihood by combining malicious and non-malicious risks.

TREATMENT

- cyber systems are technical in nature, often resulting in the risk treatment in many cases being technical.
- differences between malicious and non-malicious risks has impact on the treatment of risks.
- treatment of malicious risks is challenging, focus may be on the interaction with cyber space.
- non-malicious treatment can be also addressed through training and policies but must ensure we do not introduce problems.

SUMMARY

- principles of risk management, risk management framework and risk management process itself.
- refining the aforementioned to support cyber risk assessment.
- understand the difference between non-malicious and malicious risk.