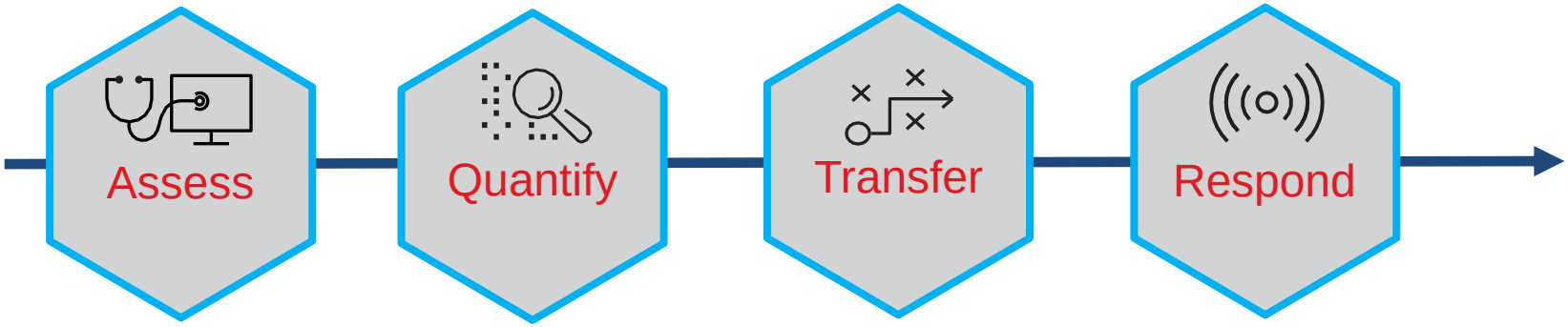
Risk Management In the Certification and GDPR Realm

Cyber Risk Management | Adopting a Risk-Based Cyber Insurance Strategy



- Helping clients optimise the total cost of risk associated with cyber exposures

Holistic integration with Enterprise Risk Management (ERM) framework: appetite, financing, and insurance

Includes harmonized input from Compliance, Legal, Finance, HR, BUs, Internal Audit + Cybersecurity and IT

AON
Empower Results®

Risk Management | a monitoring tool aimed at continuous improvement

Considering the different definitions of risk, it is perceived as “anything with the **potential** to **hinder** the attainment of **objectives and** targets.” the process aims to enable the cycle **PDCA** in which we clearly lay out who is to manage each separate risk and in what manner, periodically determine the management status, and conduct revisions

Assessing the management system, to identify the possible improvements. Knowing outputs are desired helps to develop a plan to fix the process.

Allowing the plan from the previous step to be enacted. Small changes are usually tested, and data is gathered to see how effective the change is.

Requiring corrective actions on significant differences between actual and planned results.

Check is aimed to analyze the evolution of the PDCA over time. This helps to see how the improvements suggested *even through risk management* are more effective

AON
Empower Results®

Risk Management | Certification and GDPR Realm

Risk management as initiatives necessary for establishing and promoting internal control systems.

The Main objective is to recognize, analyze, and evaluate all risks in IT and business activities and share awareness within the an organization of preventing risk from materializing.

The ISO 27001:2013 is a risk-based standard approach for the information security management system.

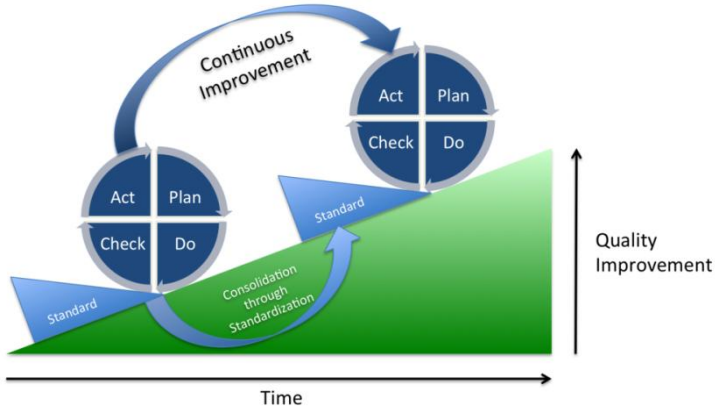
As prescribed by the ISO 31000 and ISO 27001, **Risk Management , and cyber risk management could be** the level of adoption of the risk-based approach are the coordinated activities to direct and control the organization with regard to risk (effect of uncertainty on objectives), with a strong relationship with the periodical management review through the Risk Treatment Plan.

AON
Empower Results®

Risk Management | Certification and GDPR Realm

As stated in ISO 29134 To determine the relevant **privacy safeguarding requirements** for the purpose of the program, information system or process **under assessment**.

The main expected output is the **list of privacy safeguarding requirements** to identify risks to relevant stakeholders arising from the program, information system or process under assessment



The identified risks should be documented in the PIA report, which is comparable to a risk management report or *risk treatment plan* the input for the management review and the continuous improvement in terms of Data Protection Management System with the aim of summarizing the main points discussed Risk Management aims to:

- Provide a view of the risk scenarios applicable to organizations
- Manage and control the risks (e.g. information security, Data Protection)
- Identify the "critical" areas of the Organization
- Define a process of continuous improvement of information security considering a cost / benefit strategy

AON
Empower Results®