GDPR and Cyber Security – Implementing Compliance, Risk Management, and Safeguard Measures

ISO Compliance Management Systems – The Latest Trend and Updates

Dr Nigel H Croft
Chair - ISO Joint Technical Coordination Group for Management System Standards

Presentation outline

1) Background
   - What is GDPR and why is cybersecurity so important?
   - How can Management System Standards help?
2) Compliance Management
   - ISO 31000 Risk Management Guidelines
   - The new ISO 37301:2021 Requirement Standard
3) Information and Cybersecurity
   - The ISO/IEC suite of Information Security Management Standards

Part 1

Background

- What is GDPR and why is cybersecurity so important?
- How can Management System Standards help?

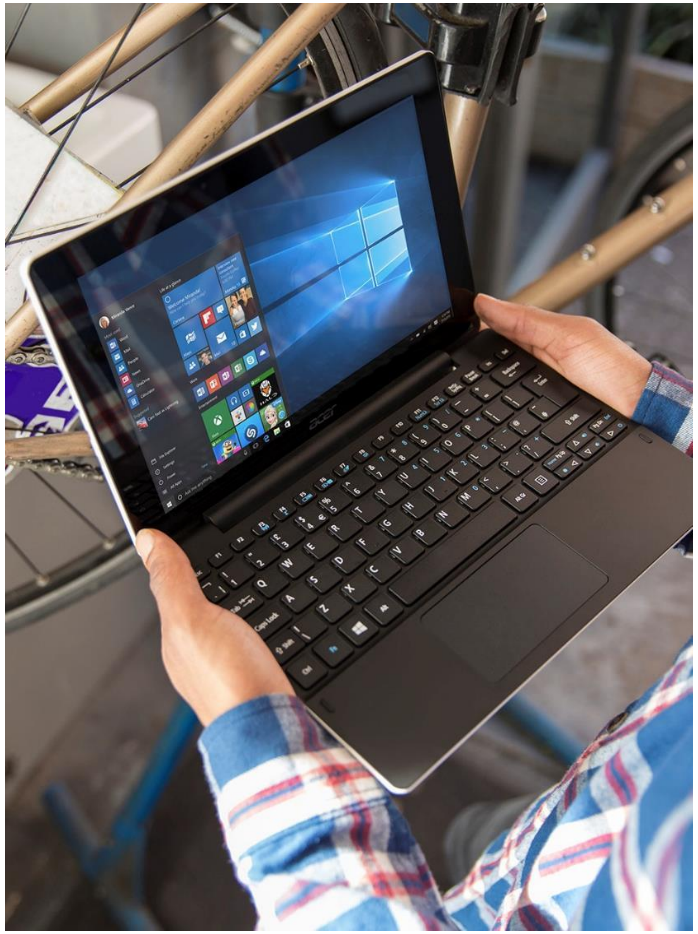
General Data Protection Regulation

- GDPR - Regulation (EU) 2016/679 of the European Parliament, the Council of the European Union and the European Commission
- Published April 27th 2016; Came into effect May 25th 2018
- Requires all organizations that collect or use personal data related to EU subjects to ***manage that data more effectively.***
- Includes data on
  - customers,
  - employees,
  - contacts
  - any other relevant persons
- Similar legislation in other countries

Personal data

- Formal definition (GDPR Article 4):
  - “any information relating to an identified or identifiable natural person (‘data subject’);
  - an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as
    - a name
    - an identification number
    - location data
    - an online identifier
    - one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”
- **Data subject** –the person the data is about
- **Data controller** – the organisation that ‘determines the purposes’, that decides to gather and use the information

NOTE: “Sensitive personal data” is defined later as “Any information relating to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, alleged or actual criminal activity and criminal record.



Core Principles of GDPR

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

What GDPR is ***not***!

- It's ***not just*** an Information Security issue
- It's ***not just*** a Legal issue
- It's ***not just*** a Compliance issue
- It's ***not just*** a Risk issue
- It's ***not just*** a Data issue
- ***It's ALL of these, and more…***

Dr W. Edwards Deming

“How could there be life without aims and hopes? Everyone has aims, hopes, plans.

But a goal that lies beyond the means of accomplishment will lead to discouragement, frustration, demoralization.

In other words, there must be a method to achieve an aim***……….BY WHAT METHOD??”***

“The Method”……

Management system

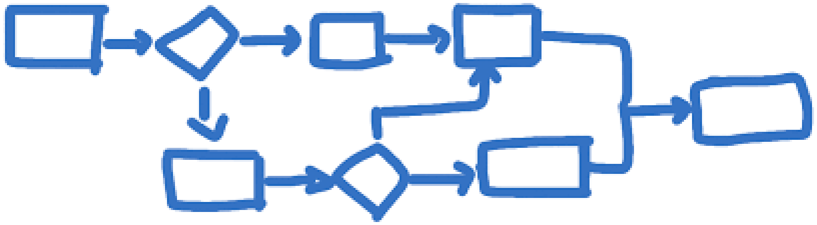
- “set of interrelated or interacting elements ……… to establish policies and objectives, as well as processes ***to achieve those objectives***” (ISO Directives Annex SL 2021 definition)

In other words…….. ***RESULTS FOCUSED***

- ISO 9001 – “Consistent, conforming products & services”
- ISO 37301 – “Compliance with relevant regulations, codes and standards”
- ISO/IEC 27001 – “Secure information”
- ISO/IEC
- etc

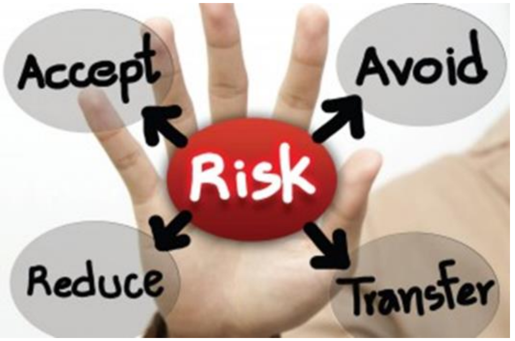
3 core concepts ……

Understand the ***processes*** needed to achieve the planned results



Continually monitor the ***risks*** ("Risk-based thinking")

- Not all processes have the same impact



Manage the processes and the system using ***"PDCA"*** at all levels

PLAN
STEP 1
DO
STEP 2
CHECK
STEP 3
ACT
STEP 4
quality
data
reporting
management
report
processes

Part 2

Compliance Management Systems

- ISO 31000 Risk Management Guidelines
- The new ISO 37301:2021 Requirement Standard

Opportunity

- “a time or set of circumstances that makes it possible to do something” (Wikipedia)

Some examples:

- New technologies (eg Blockchain; Big Data; AI)
- Social media (increased public awareness)
- New legislation
- Intergovernmental collaboration
- More transparency in tax havens
- etc

Risk

- "the potential of losing something of value, weighed against the potential to gain something of value" (Wikipedia).
- Examples:
  - Personal information
  - Cyberattacks

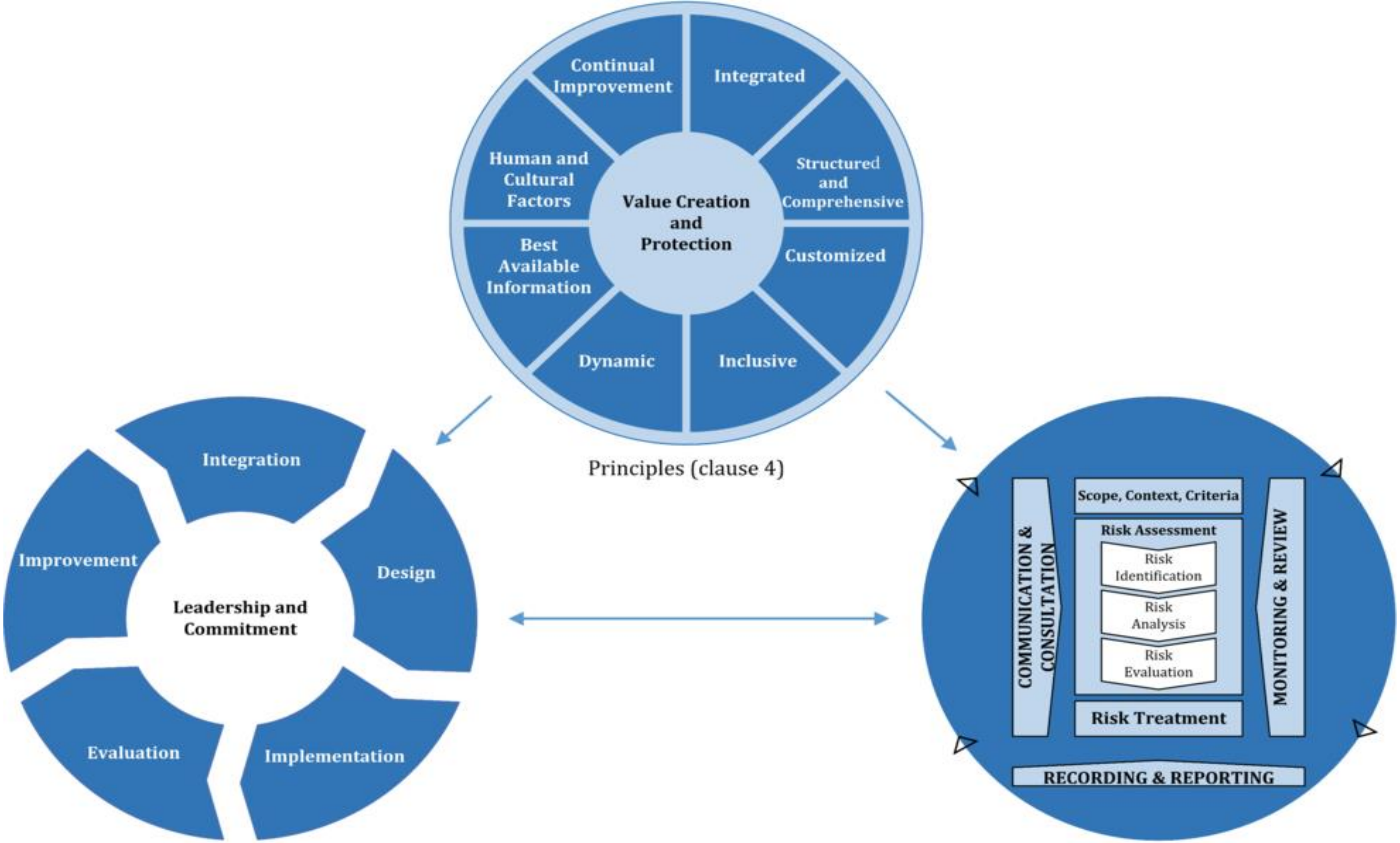
"effect of uncertainty on objectives" (ISO 31000)

- Can be positive or negative
- Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood

ISO 31000:2018

- “Risk management – Guidelines”
  - A “Management Standard” NOT a “Management Systems Standard”
  - Not “certifiable”
- First published 2009; updated in 2018
  - Principles of risk management revised and simplified
  - Emphasis on leadership by top management
  - Need for integration of risk management, starting with the governance of the organization;
  - Greater emphasis on the iterative nature of risk management (new experiences, knowledge and analysis)

Framework of ISO 31000:2018



Principles (clause 4)

Framework (clause 5)

Process (clause 6)

What is “Compliance”?

- “Meeting all the requirements that an organization:
  - mandatorily has to comply with
  - voluntarily chooses to comply with”

For example, legal and/or regulatory requirements (International, regional or local)

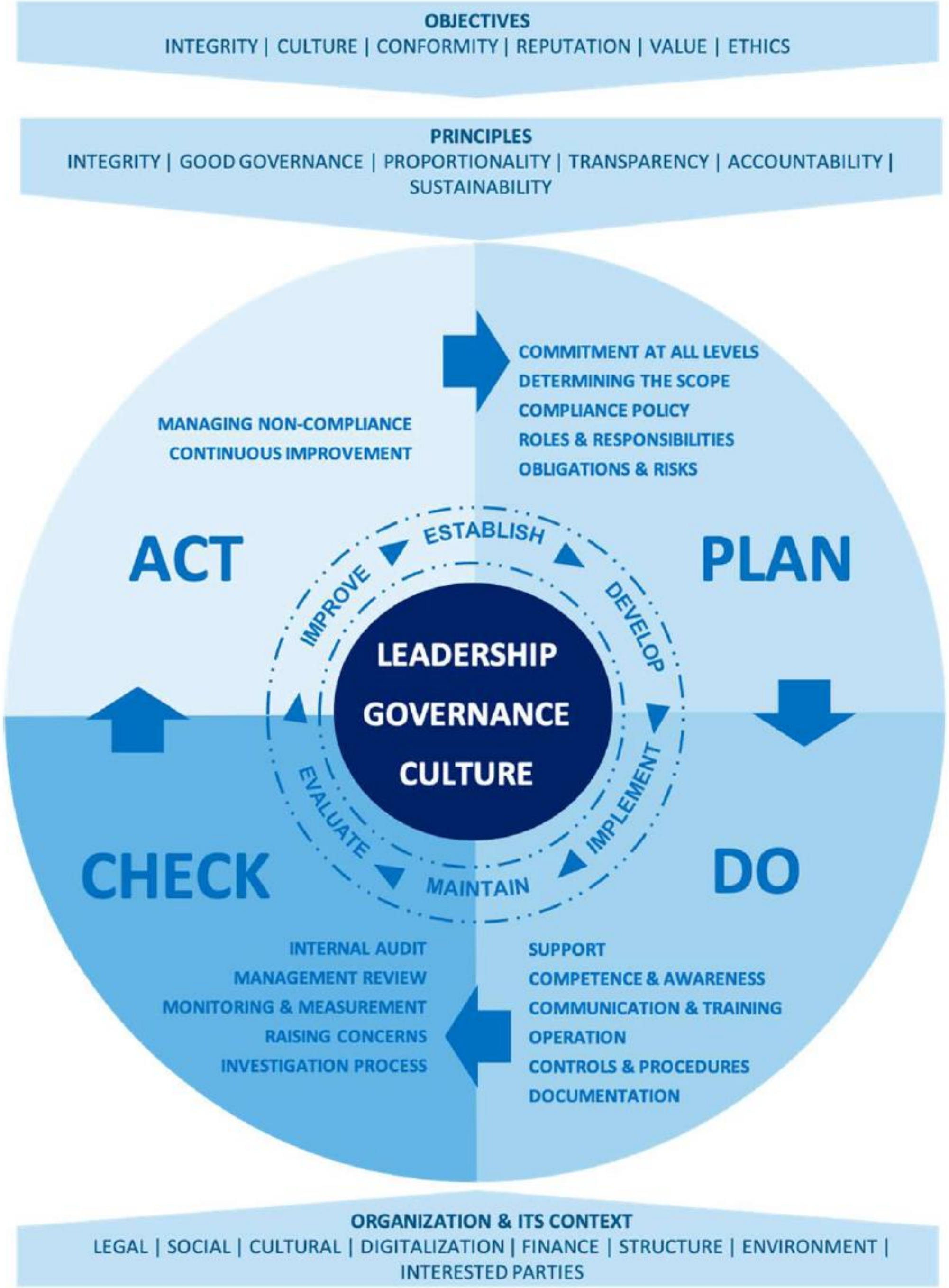
For example, corporate governance criteria; industry codes of conduct etc

Mandatory and “voluntary”

- “Compliance requirements” (Mandatory) include:
  - laws and regulations;
  - permits, licences or other forms of authorization;
  - orders, rules or guidance issued by regulatory agencies;
  - judgments of courts or administrative tribunals;
  - treaties, conventions and protocols.
- “Compliance commitments” (“Voluntary”) include:
  - agreements with community groups or NGOs
  - agreements with public authorities and customers;
  - organizational requirements, such as policies and procedures;
  - voluntary principles or codes of practice;
  - voluntary labelling or environmental commitments;
  - obligations arising under contractual arrangements with the organization;
  - relevant organizational and industry standards.

ISO 37301:2021 Compliance management systems — Requirements with guidance for use

- “An organization’s approach to compliance is ideally shaped by the leadership applying **core values** and **generally accepted corporate governance, ethical and community standards**.”
- Embedding compliance in the behaviour of the people working for an organization depends above all on leadership at all levels and clear values of an organization, as well as an acknowledgement and implementation of measures to promote compliant behaviour.”
- Originally published as a GUIDELINES standard in 2014 (ISO 19600)
- Revised and transformed into a REQUIREMENTS standard (certifiable) April 2021



OBJECTIVES
INTEGRITY | CULTURE | CONFORMITY | REPUTATION | VALUE | ETHICS

PRINCIPLES
INTEGRITY | GOOD GOVERNANCE | PROPORTIONALITY | TRANSPARENCY | ACCOUNTABILITY | SUSTAINABILITY

PLAN
- COMMITMENT AT ALL LEVELS
- DETERMINING THE SCOPE
- COMPLIANCE POLICY
- ROLES & RESPONSIBILITIES
- OBLIGATIONS & RISKS

DO
- SUPPORT
- COMPETENCE & AWARENESS
- COMMUNICATION & TRAINING
- OPERATION
- CONTROLS & PROCEDURES
- DOCUMENTATION

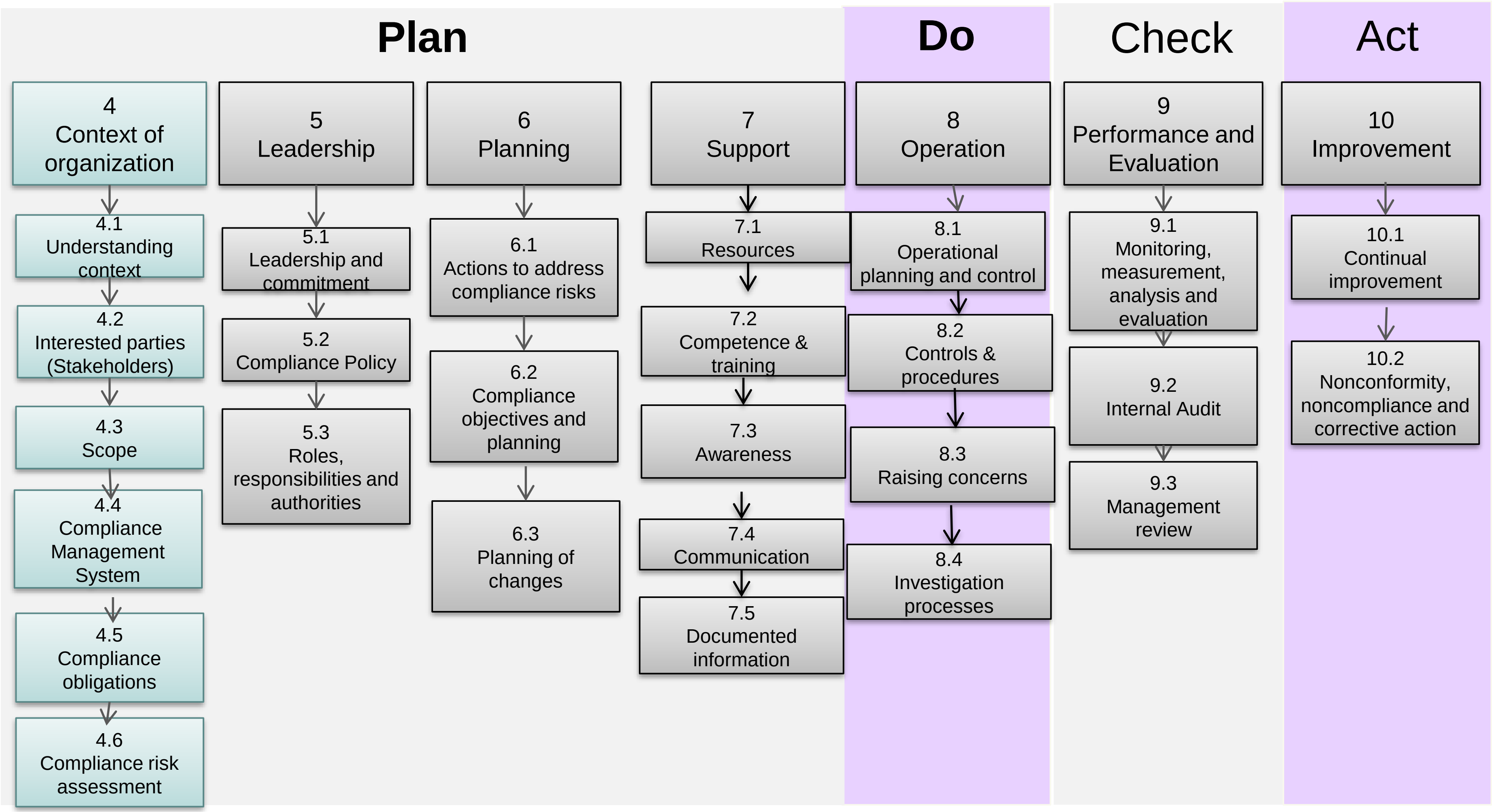
CHECK
- INTERNAL AUDIT
- MANAGEMENT REVIEW
- MONITORING & MEASUREMENT
- RAISING CONCERNS
- INVESTIGATION PROCESS

ACT
- MANAGING NON-COMPLIANCE
- CONTINUOUS IMPROVEMENT

LEADERSHIP
GOVERNANCE
CULTURE

ORGANIZATION & ITS CONTEXT
LEGAL | SOCIAL | CULTURAL | DIGITALIZATION | FINANCE | STRUCTURE | ENVIRONMENT | INTERESTED PARTIES

ISO 37301 Clause structure (Based on 2021 version of “Annex SL”)



Plan

4 Context of organization
- 4.1 Understanding context
- 4.2 Interested parties (Stakeholders)
- 4.3 Scope
- 4.4 Compliance Management System
- 4.5 Compliance obligations
- 4.6 Compliance risk assessment

5 Leadership
- 5.1 Leadership and commitment
- 5.2 Compliance Policy
- 5.3 Roles, responsibilities and authorities

6 Planning
- 6.1 Actions to address compliance risks
- 6.2 Compliance objectives and planning
- 6.3 Planning of changes

7 Support
- 7.1 Resources
- 7.2 Competence & training
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented information

Do

8 Operation
- 8.1 Operational planning and control
- 8.2 Controls & procedures
- 8.3 Raising concerns
- 8.4 Investigation processes

Check

9 Performance and Evaluation
- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal Audit
- 9.3 Management review

Act

10 Improvement
- 10.1 Continual improvement
- 10.2 Nonconformity, noncompliance and corrective action

Compliance risks (Guidance in Annex)

- Analyse compliance risks by considering ***causes and sources*** of noncompliance
- Consider ***likelihood***, and ***severity of the consequences***
  - Consequences can include, for example, personal and environmental harm, economic loss, reputational harm and administrative liability.

OR

Recommended steps for implementation

- If you already have ISO 9001 QMS in place…….
  - Build on ISO 9001 structure and methodologies to incorporate Compliance, using ISO 37301
    - Define policy; assign responsibilities and authorities (“Plan”)
    - Implement (“Do”)
    - Monitor and review; internal audits & management review (“Check”)
    - Improve (“Act”)
- If you don’t have ISO 9001 QMS in place……
  - EITHER implement ISO 9001 first, and then build onto it

OR

  - Implement both simultaneously (incorporate compliance within the QMS)
- Important NOT to consider as “2 distinct systems”!

Part 3

Information and Cyber-security Management

- The ISO/IEC suite of Information Security Management Standards

The ISO/IEC 27001 “toolbox” for Cybersecurity

- Managing the RISKS associated with new technologies
- Cyberspace
  - Complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.
  - Collaboration is essential to ensure a safe online environment, and the various standards developed by ISO/IEC JTC 1 form part of the so-called ISO/IEC 27001 “cyber-risk toolbox”.
- Information security management is not a new topic, but recent events including “ransomware”, alleged cyber-interference by Russia in the US election campaign and others have brought cyber security to the forefront of global concerns.

Evolution of Information Security Management Standards

- 1992 - British Department of Trade and Industry (DTI) published 'Code of Practice for Information Security Management'.
- 2005 – Publication of ISO/IEC 27001 "Information security management systems – Requirements".
- 2013 – Publication of current version of ISO/IEC 27001
  - Supplemented by ISO/IEC 27002 (Guidelines for organizational information security standards and information security management practices).
- Many more standards developed by ISO/IEC JTC 1, a joint technical group of ISO and the IEC (International Electrotechnical Commission) to address the ever-evolving risks and opportunities provided by modern Information and Communications Technologies (ICT).

ISO/IEC 27701:2019

- Privacy Information Management — Requirements and guidelines
- Certifiable extension to ISO/IEC 27001.
- Aims to provide confidence that personal information is being managed in a secure and responsible way for:
    - employees
    - customers
    - contacts
    - other stakeholders

ISO/IEC 27032:2012

- “Guidelines for cybersecurity”
- Aims to improve cybersecurity by addressing its unique aspects and its dependencies on other security domains such as:
  - information security,
  - network security,
  - internet security, and
  - critical information infrastructure protection (CIIP).
- Covers baseline security practices for stakeholders in Cyberspace and includes:
  - an overview of Cybersecurity,
  - an explanation of the relationship between Cybersecurity and other types of security,
  - a definition of stakeholders and a description of their roles in Cybersecurity,
  - guidance for addressing common Cybersecurity issues, and
  - a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

ISO/IEC 27017:2015

- Code of practice for information security controls for cloud services
- As use of the cloud increases, users need confidence that data stored and processed in the cloud is safe.
- Marketplace for cloud services is global, with providers dispersed across wide geographical areas, and data is routinely transferred across national boundaries. International guidance is therefore key.
- ISO/IEC 27017 emphasizes that selection of appropriate information security controls, and the application of the guidance provided, depends on risk assessment and any legal, contractual, regulatory or other cloud-sector specific information security requirements.

ISO/IEC 27018:2014

- “Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”
- Builds on the foundations of ISO/IEC 27001
- Offers specific guidance to help Cloud Service Providers (CSPs) assess the risks and implement controls for the protection of PII stored in the cloud
- Has the following key objectives:
  - Help cloud service providers that process PII to address applicable legal obligations as well as customer expectations
  - Enable transparency so customers can choose well-governed cloud services
  - Facilitate the creation of contracts for cloud services
  - Provide cloud customers with a mechanism to ensure cloud providers’ compliance with legal and other obligations

Conclusions

- New information and communication technologies bring a lot of OPPORTUNITIES, but also RISKS that need to be managed
- ISO has a whole suite of management system standards with a common approach, to address:
  - Quality
  - Risk
  - Compliance
  - Information and cyber-security
- All of these can be used to address GDPR-related challenges!

THANK YOU!

nhc@tcaglobal.org