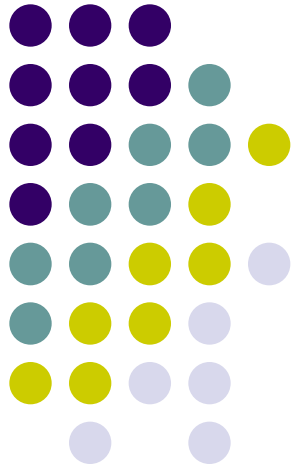
“The Role of ISO Standards in Governance, Risk and Compliance Management for Today’s Business”

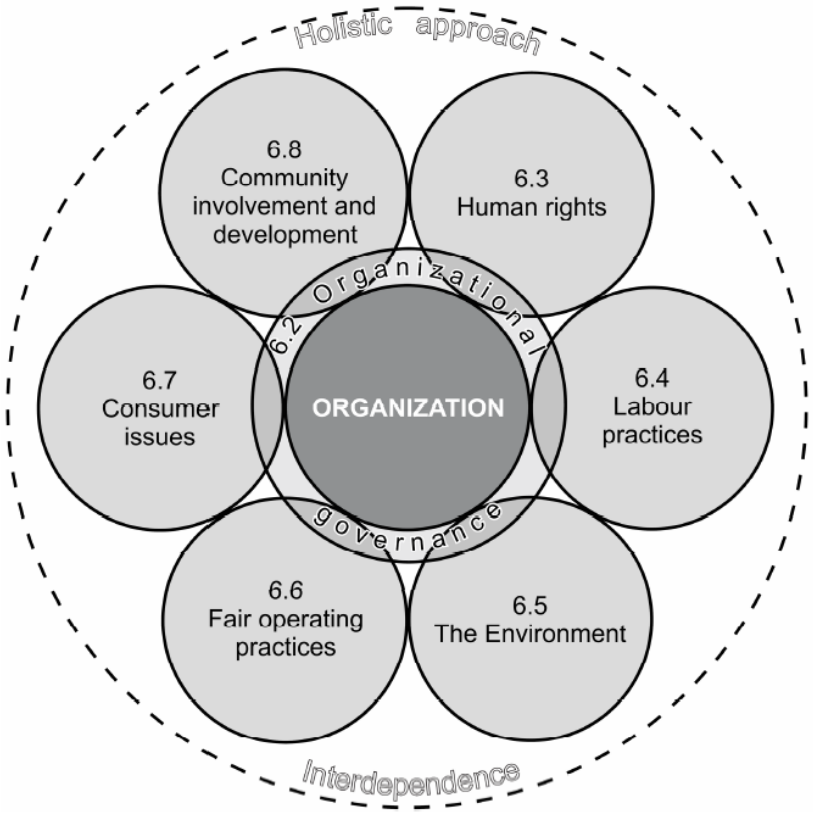


HKQAA Symposium 2017

Dr Nigel H Croft

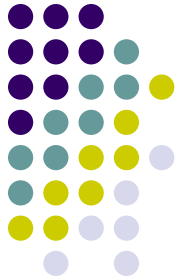
Governance

- ***"The way in which an organization makes and implements decisions in pursuit of its objectives"***
- It is the glue which holds the organisation together, while risk management provides the resilience.
- Risk = "The effect of uncertainty" (on objectives / expected results)
- Resilience = ability of an organization to anticipate, prepare for, and respond and adapt to incremental change and sudden disruptions in order to survive and prosper (ISO 22316)



(Taken from ISO 26000)

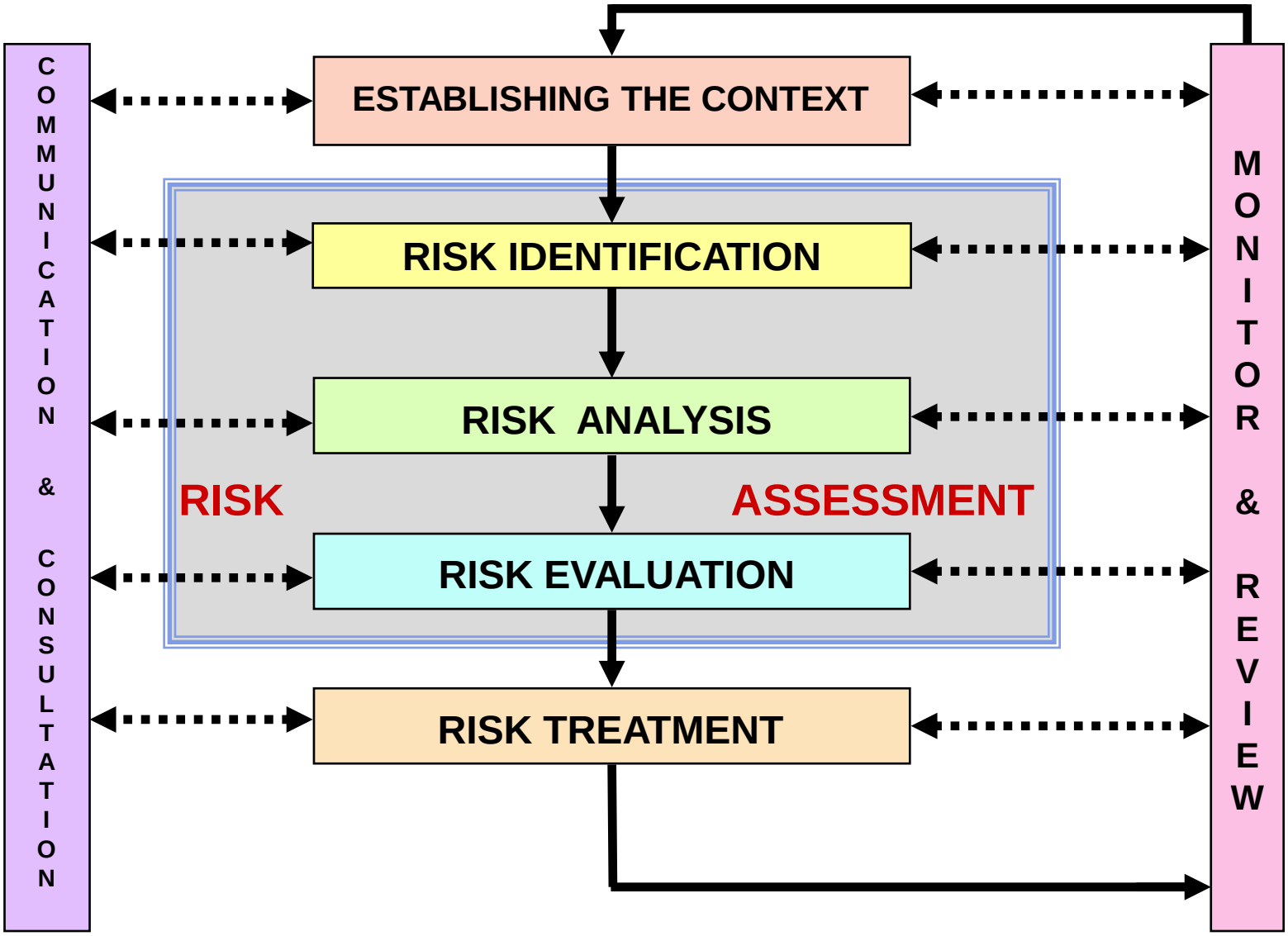
Some key ISO standards for Governance, Risk and Compliance Management



- ISO 31000 Risk management
- ISO 19600 Compliance Management*
- ISO 26000 Social Responsibility
- ISO 37001 Anti-bribery Management*
- ISO 22301 Business Continuity Management*
- ISO 28000 Supply chain security management
- ISO 55001 Asset Management*
- ISO 27001 Information security management*
- ISO/IEC 38500 IT Governance
- ISO 21505 Project, programme and portfolio governance
- ISO 30408 Governance for Human resource management
- ISO 22316 Organizational resilience

* = Uses common ISO “High-level structure”

ISO 31000:2009 Process Overview



We should be turning uncertainty into an advantage!

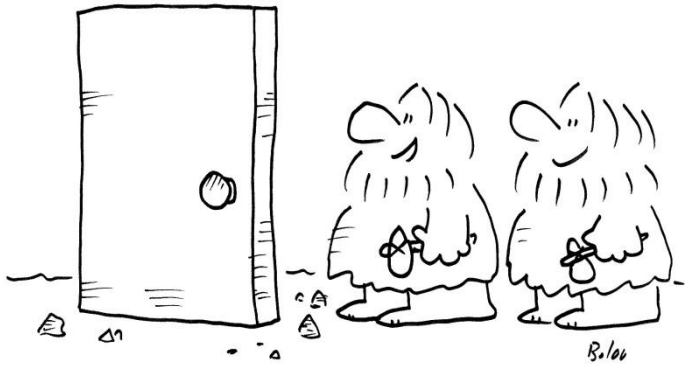
ISO 9001 – “Risk-based thinking”

Manage risks
Maximise opportunities

www.CartoonStock.com

If opportunity ***doesn't*** knock, then ***build*** a door!

WHEN OPPORTUNITY KNOCKS, ANSWER THE DOOR



"There! — now we wait for *opportunity* to knock!"

www.CartoonStock.com

What is “ISO 19600”?

- ISO ***Guidance*** document for Compliance management systems
  - “Compliance” = “Meeting all the requirements that an organization ***has to*** or ***chooses to*** comply with”

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

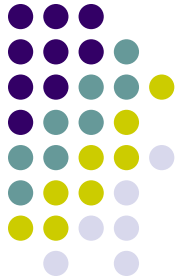
For example, corporate governance criteria; industry codes of conduct etc

- ISO 19600 follows the same overall philosophy and structure as ISO 9001, but contains only Guidance (“should’s”, not “shall’s”)
- Not appropriate for certification, but could be included in corporate (internal) audits

Rationale for ISO 19600

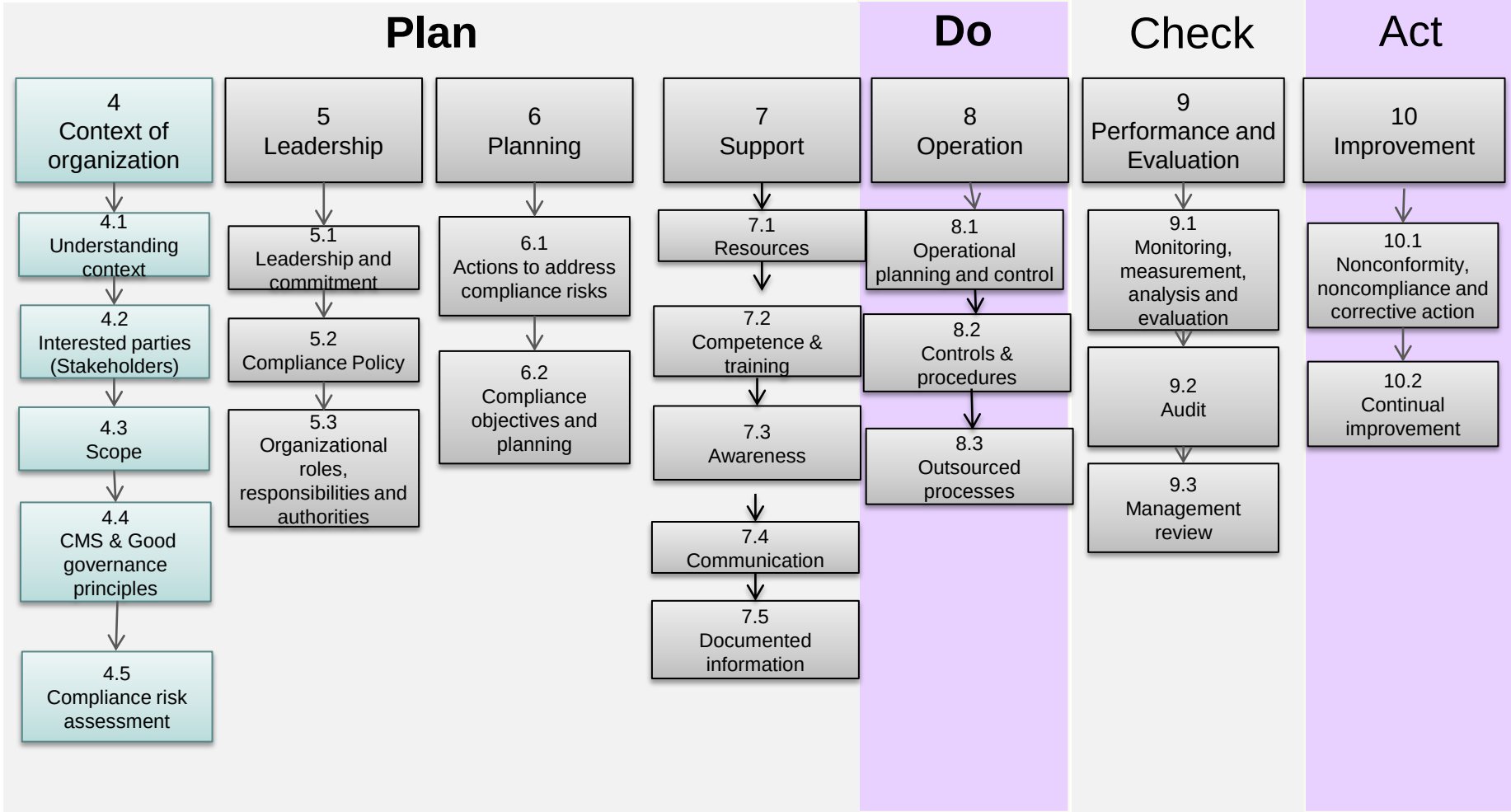
- “An organization’s approach to compliance is ideally shaped by the leadership applying **core values** and **generally accepted corporate governance, ethical and community standards**.”
- Embedding compliance in the **behaviour** of the people working for an organization depends above all on leadership at all levels and clear values of an organization, as well as an acknowledgement and implementation of measures to promote compliant behaviour.”

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 19600 Clause structure

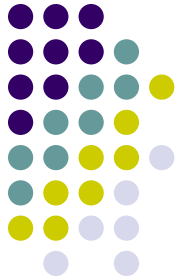


Compliance risks

- 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

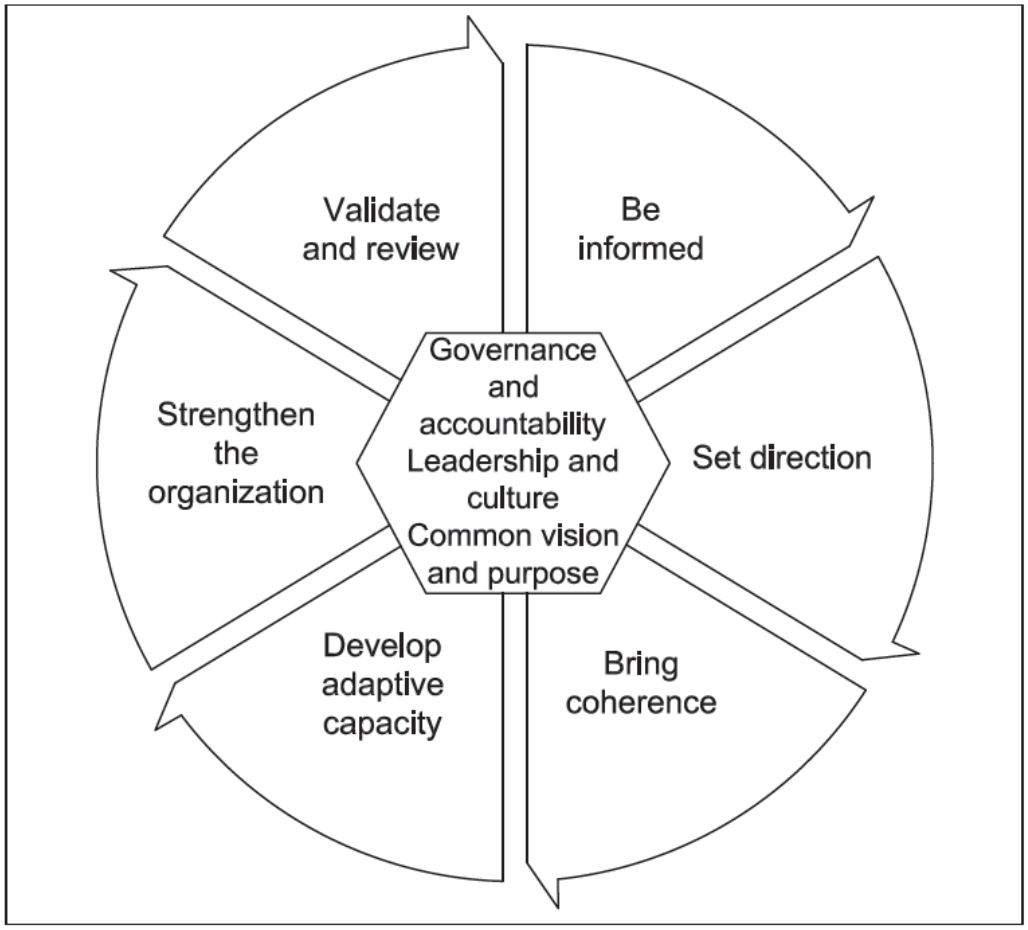
New ISO Standard on resilience



- ISO 22316:2017 “Organizational resilience - Principles and attributes” includes topics such as:

- quality management
- risk management
- asset management
- stakeholder and collaboration management
- reputation management;
- horizon scanning;
- environmental management
- health and safety
- fraud control;
- business continuity
- information, communications and technology (ICT) continuity
- cyber security
- change management;
- information security
- physical security;
- facilities management;
- emergency management;
- crisis management
- supply chain
- human resource planning;
- financial control;

ISO 22316 Model



Conclusions

- ISO standards can make many contributions to Governance, Risk and Compliance Management
- Just 2 examples:
  - ISO 19600 provides guidance on compliance
    - Mandatory (legal) requirements and/or “Voluntary” commitments
    - Totally aligned with ISO 9001, 14001 etc
  - New ISO 22316 promotes organizational resilience
    - outcome of good business practice and effectively managing risk.

THANK YOU!

nhc@tcaglobal.org