

Compliance Management Systems

The Implementation of Compliance Management Systems in Hong Kong

Mr. William Wong
Hong Kong Quality Assurance Agency



Introduction for HKQAA

Corporate Profile

Established in 1989 as a non-profit-distributing organisation by the Hong Kong Government, Hong Kong Quality Assurance Agency (HKQAA) helps industry and commerce in the development of quality, environmental, safety, hygiene, social and other management systems

The professionals in HKQAA possess a wide range of international and industrial knowledge and experience to provide the market with a full spectrum of conformity assessment services

Web site: www.hkqaa.org

Compliance Management

What is Compliance anyway ?

Compliance - meeting all the organization's compliance obligations

Compliance obligations - **requirements** that an organization mandatorily has to comply with as well as those that an organization voluntarily chooses to comply with

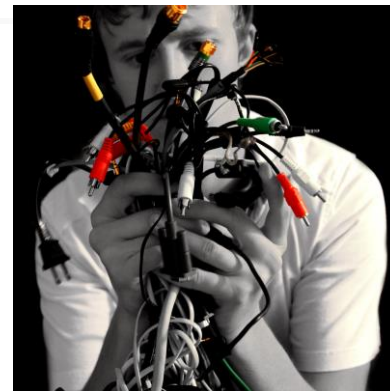
Requirement - need or expectation that is stated, generally implied or obligatory

Source: ISO 37301:2021

Compliance Management

What is Compliance anyway ?

So in other words, **Compliance is**



Meeting all the needs or expectations that are stated, generally implied or obligatory that an organization has to comply with or chooses to voluntarily comply with



Compliance Management

Why Compliance Management

Recent Cases



Some recent popular examples:

- **Fa**b**k** will pay over half a billion dollars to settle a class action lawsuit that alleged systematic violation of a consumer privacy law
- **Fa**b**ok** and **Go***le** hit with \$8.8 billion in lawsuits on day one of GDPR
- **H**C** to pay \$1.9 billion U.S. fine in money-laundering case
- **Lead in paint prompts M*tt*I to Recall 967,000 Toys**



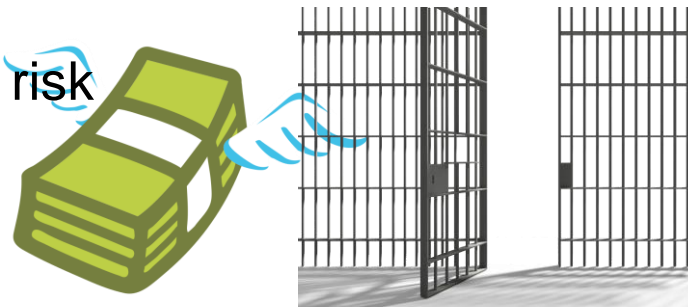
Compliance Management

Why Compliance Management is Important?

- Helps to manage risks
 - Changing product and service offerings
 - New legislation, regulation, interpretations, court decisions that address developments in the marketplace and are relevant to the product and service offerings of the organization
- Noncompliance may result in:
 - Litigation, monetary penalties, and other formal enforcement actions

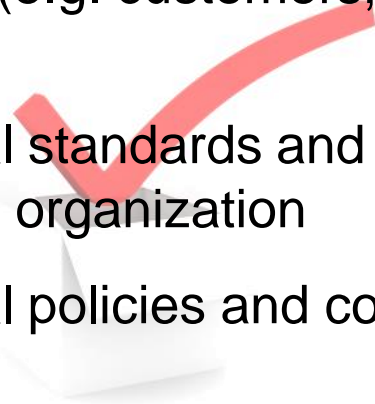
– reputation risk

.....



Compliance Management

- Integrity and compliance are the basis for a successful and sustainable organization
- But compliance management is more than just compliance to laws and regulations
- Organizations are also required to deal with varying requirements from
 - Stakeholders (e.g. customers, community, etc.), industry codes
 - Organizational standards and benchmarks voluntarily chosen by the organization
 - Organizational policies and codes



Compliance Management System

- An effective compliance management system enables an organization to demonstrate its commitment to compliance with relevant laws, including legislative requirements, industry codes and organizational standards
- In jurisdictions, the courts may consider an organization's commitment to compliance through its compliance management system when determining the appropriate penalty –

- **Due diligence**



ISO 37301:2021 Compliance Management Systems

- ISO 37301:2021 Compliance management systems - Requirements with guidance for use
 - Published in April 2021
 - Replace ISO19600:2014
 - Becomes a certifiable standard complimented by guidance in Annex A



ISO

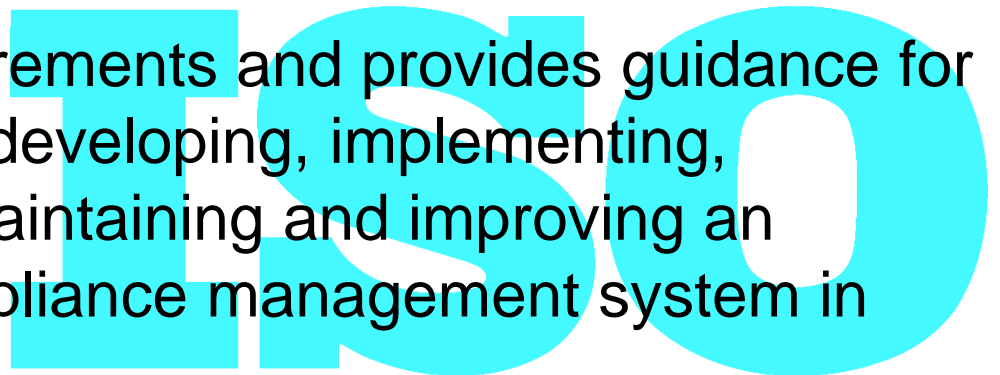
ISO 37301:2021 Compliance Management Systems

- ISO 37301:2021 Compliance management systems - Requirements with guidance for use
 - Some new elements from ISO 19600:2014 are
 - the inclusion of the employment process - due diligence in hiring and promotion and disciplinary action in case of violation of compliance obligations
 - further strengthening of employee reporting and employee protection
 - principles for investigation processes



ISO 37301:2021 Compliance Management Systems

- ISO 37301:2021 Compliance management systems - Requirements with guidance for use
 - provides a framework to assist in the implementation of specific compliance-related requirements in any management system
 - Defines requirements and provides guidance for establishing, developing, implementing, evaluating, maintaining and improving an effective compliance management system in organizations



ISO 37301:2021 Compliance Management Systems

- ISO 37301:2021 Compliance management systems - Requirements with guidance for use
 - Applicable to all types of organizations regardless of the type, size and nature of the activity, public, private or non-profit sector



ISO 37301:2021 Compliance Management Systems

- Adopted the “**high-level structure**” (i.e. common clause sequence, common text and common terminology) developed by ISO to improve alignment among various and numerous management systems standards



ISO 37301:2021 Compliance Management Systems

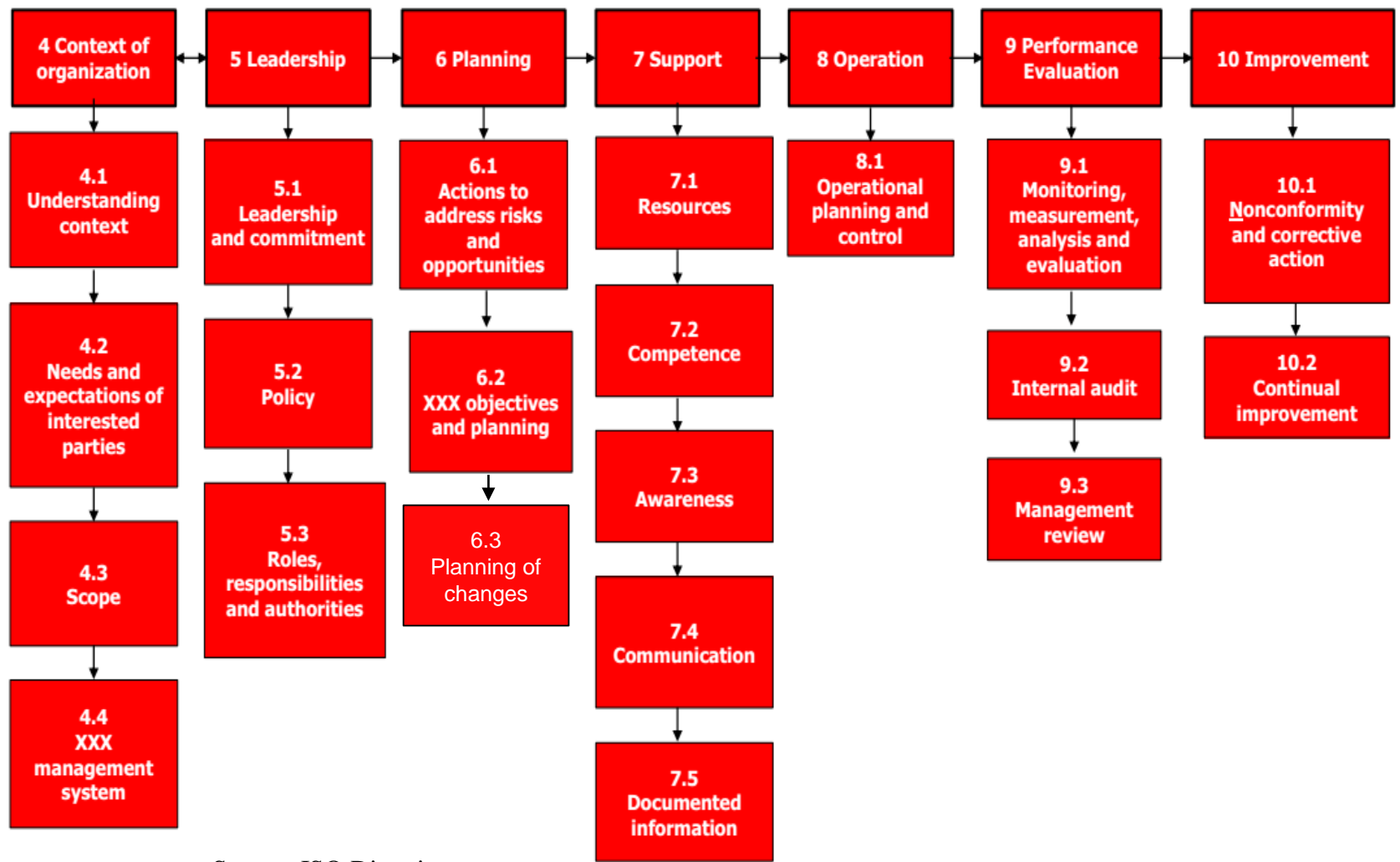
> HLS STRUCTURE

Introduction

- 1 SCOPE
- 2 NORMATIVE REFERENCES
- 3 TERMS AND DEFINITIONS
- 4 CONTEXT OF THE ORGANIZATION
- 5 LEADERSHIP
- 6 PLANNING
- 7 SUPPORT
- 8 OPERATION
- 9 PERFORMANCE EVALUATION
- 10 IMPROVEMENT



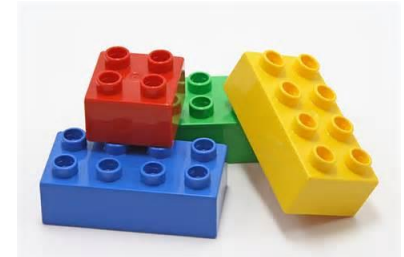
ISO Directives High Level Structure



Source: ISO Directives

ISO Directives “High Level Structure” - HLS

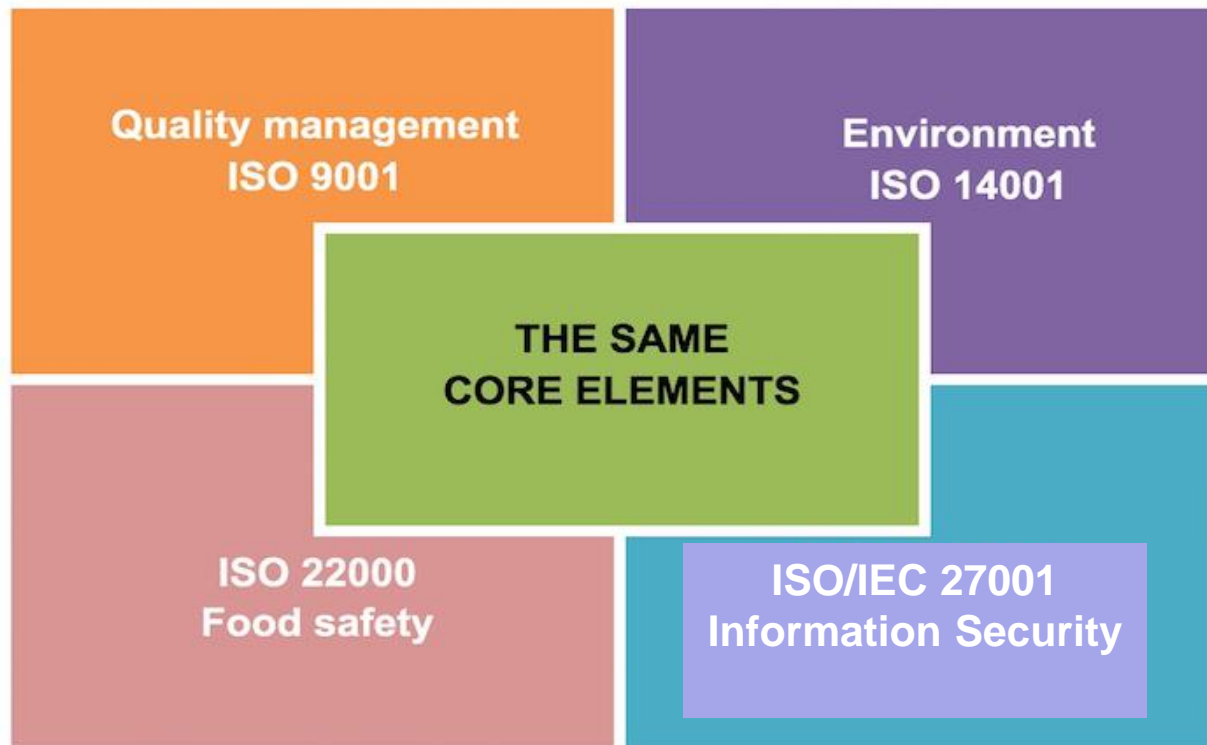
	Introduction
1.	Scope
2.	Normative references
3.	Terms and definitions
4.	Context of the organization
5.	Leadership
6.	Planning
7.	Support
8.	Operation
9.	Performance evaluation
10.	Improvement



30%
Identical
core text

ISO 37301:2021 Compliance Management Systems

- Can be combined with existing management system standards (e.g. ISO 9001, ISO 14001, ISO 22000, ISO/IEC 27001, ISO 37001) and generic guidelines (e.g. ISO 31000, ISO 26000).



ISO 37301:2021 Compliance Management Systems

- The well known “Plan-Do-Check-Act” Cycle



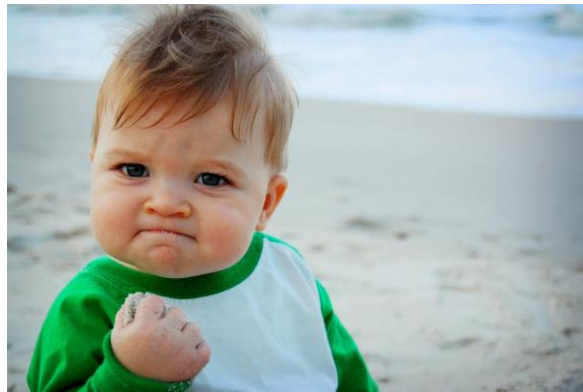
Source: ISO 37301:2021

ISO 37301:2021 Compliance Management Systems - structures

Foreword						
Introduction						
1 Scope						
2 Normative references						
3 Terms and definitions						
PLAN			DO		CHECK	ACT
4 Context of the organization	5 Leadership	6 Planning	7 Support	8 Operation	9 Performance evaluation	10 Improvement
4.1 Understanding the organization and its context	5.1 Leadership and commitment	6.1 Actions to address risks and opportunities	7.1 Resources	8.1 Operational planning and control	9.1 Monitoring, measurement, analysis and evaluation	10.1 Continual improvement
4.2 Understanding the needs and expectations of interested parties	5.1.1 Governing body and top management	6.2 Compliance objectives and planning to achieve them	7.2 Competence	8.2 Establishing controls and procedures	9.1.1 General	10.2 Nonconformity and corrective action
4.3 Determining the scope of the compliance management system	5.1.2 Compliance culture	6.3 Planning of changes	7.2.1 General		9.1.2 Sources of feedback on compliance performance	
4.4 Compliance management system	5.1.3 Compliance governance		7.2.2 Employment process	CHECK	9.1.3 Development of indicators	
4.5 Compliance obligations	5.2 Compliance policy		7.2.3 Training	8.3 Raising concerns	9.1.4 Compliance reporting	
4.6 Compliance risk assessment	5.3 Roles, responsibilities and authorities		7.3 Awareness	8.4 Investigation processes	9.1.5 Record-keeping	
	5.3.1 Governing body and top management		7.4 Communication		9.2 Internal audit.	
	5.3.2 Compliance function		7.5 Documented information		9.2.1 General	
	5.3.3 Management		7.5.1 General		9.2.2 Internal audit programme	
	5.3.4 Personnel		7.5.2 Creating and updating documented information		9.3 Management review	
			7.5.3 Control of documented information		9.3.1 General	
					9.3.2 Management review inputs	
					9.3.3 Management review results	
Annex A (informative) Guidance for the use of this document						
Bibliography						

ISO 37301:2021 Benefits

- Helps the organization consider all of their compliance requirements, compliance commitments and compliance obligations in order to be successful in the long term
- Helps the organization understand and adhere to the ever-changing and ever-increasing number of regulatory requirements while acknowledging the fundamental market drives



Management Systems Certifications in Hong Kong

Management Systems Standards	No. of Certificates
ISO 9001 :2015 Quality management systems	2102
ISO 14001 :2015 Environmental management systems	873
ISO 45001 :2018 Occupational health and safety management svstems	370
ISO/IEC 27001:2013 Information security management systems	158
ISO 22000:2018 Food safety management systems	114
ISO 50001 :2011&2018 Energy management systems	70
ISO 13485:2016 Medical devices Quality management systems	59
ISO/IEC 20000-1:2011&2018 Service management system requirements	31
ISO 28000:2007 Security management systems for the supply chain	11
ISO 22301 :2012&2019 Business continuity management systems	3
ISO 37001 :2016 Anti-bribery management systems	1

Source: The ISO Survey 2019 of Management System Standards Certifications

Management Systems Certification in Hong Kong

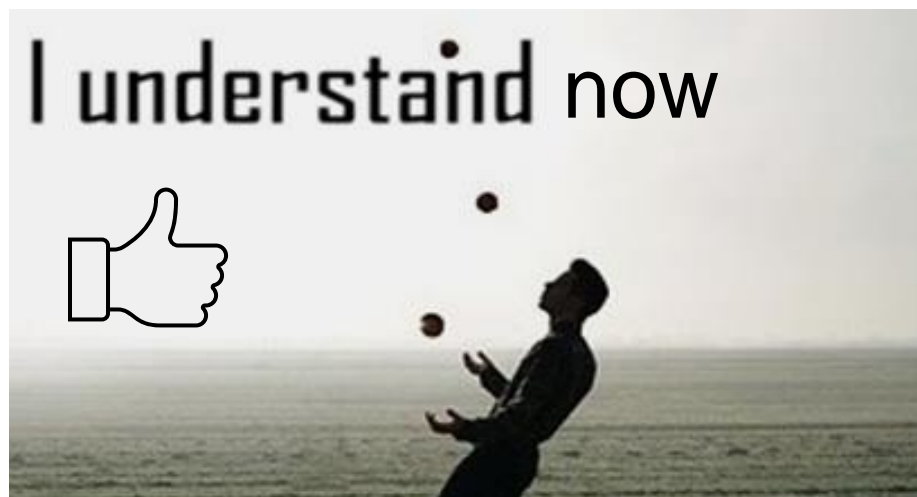
- There is No ISO 37301 (or ISO 19600) certificate in Hong Kong in the ISO Survey 2019

What?



Management Systems Certification in Hong Kong

- ISO 19600 (the predecessor of ISO 37301) provides a set of Guidelines for Compliance Management Systems but Not for certification
- And ISO 37301 is just released!



Management Systems Certification in Hong Kong

- But ISO 37301 (and ISO 19600) is a good basis and references for other Management Systems Standards **Examples**



Compliance Management Systems



Thanks!