ISO 27001:2022
Internal Auditor Training

Simply leveraging Quality.

Primary Shareholders

<For training by DQS HK only>

DGQ
Deutsche Gesellschaft für Qualität

German Society of Quality since 1952

DIN

German Institute for Standardization since 1917

UL

Underwriters Laboratories since 1894

Note: **DIN** is the current international secretariat of ISO/IEC Joint Technical Committee JTC 1/SC 27, who develops International Standards of information security.

* All DQS ultimate shareholding organizations are registered as non-profit organizations.

DQS

Simply leveraging Quality.

- Issue the 1st ISO9001 certificate in Germany
- The 1st CB recognized by IATF for ISO/TS 16949 certification
- Issue the 1st IRIS certificate in the world
- A founding member of IQNet

Course Objectives

- To understand development of and changes to ISO 27001 standard
- To understand ISO 27001:2022 standard requirements
- To understand some best practices in ISMS implementation
- To develop expertise to implement ISMS according to ISO 27001
- To develop the basic expertise to plan and conduct internal audit

Evaluation

- Full Participation
- Assignments

Training Attendant Certificate

- Passing general evaluation

Training Completion Certificate

Discussions and Cases Studies

- To provide separately during the course

Course Agenda 課程安排

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops

Q&A

Evaluation

Forewords

- This training material is based on the author's understanding, to facilitate clients to understand the standard.
- This training material is not technically possible, nor intended to completely replace the original standard.
- The interpretation of standard may not be 100% precise due to the constraints of time and author's knowledge.
- For interpretation of regulations, you should refer to a lawyer.
- Please inform us if you find any mistake.
- The copyright of this material belongs to DQS HK and it is not allowed to copy, translate or propagate.

Forewords

ISO 27000 Serials Standards

- ISO/IEC 27000:2018, Overview and vocabulary
- ISO/IEC 27001:2013, ISMS Requirements
- ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC 27003:2017, ISMS implementation guidance
- ISO/IEC 27005:2018, Information security risk management
- ISO/IEC 27006:2015, Requirements for bodies providing audit and certification of ISMS
- ISO/IEC 27007:2020, Guidelines for ISMS auditing
- ISO/IEC TR 27008:2019,
  Guidelines for auditors on information security controls
- …

Development of ISMS standards

- 1990 Code of Best Practices by some companies
- …
- 2000 ISO 17799 Best Practices Code
- 2005 ISO 27001
- 2007-2012 ISO 27000 family
- 2013 Revised ISO 27001
- …
- 2018 Revised ISO 27000
- …
- 2022 Revised ISO 27002, ISO 27001 and ISO 27005

ISO 27001 vs ISO 27002

- ISO 27001 specifies the requirements for an ISMS.
- ISO 27002 is used as a reference, with guidance on the best practices in implementing ISO 27001.
- An organization can get a certification against ISO 27001, but not against ISO 27002.
- ISO 27002:2022 was released on Feb 15, 2022.
- The controls in ISO 27002 are stated with should as recommendations
- The controls in ISO 27001 are stated with shall as requirements

Transition

- Release of ISO 27001:2022 in Oct 2022
- The SOA, procedures and some other documents may need revisions
- Update and implement ISMS against the revised standard
- Internal Audit –> Management Review –> Transition Audit
- Transition Audit can be together with Surveillance Audit or Recertification Audit, with certain additional audit time
- The ISO 27001:2013 certification shall be transitioned to ISO 27001:2022 with certificate issued before Oct 31, 2025.

When should the Transition Audit planned?

Main Changes to ISO 27001:2022

- Standard title change

ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

ISO/IEC 27001:2013
Information technology — Security techniques — Information security management systems — Requirements

Main Changes to ISO 27001:2022

- Clause changes
  - ✓ Addition of 4.2 c)
  - ✓ Additional wording in 4.4 to emphasize processes and their interactions
  - ✓ Editorial revisions to Notes in Clause 6.1.3 c):
    - deleting control objectives, and
    - using “information security control” to replace “control”
  - ✓ Wording re-organization to Clause 6.1.3 d) to remove ambiguity
  - ✓ Addition of 6.3 Planning of Changes
  - ✓ Change in wording, such as the use of staff to replace employee, to include contracted or temporary staff.

Main Changes to ISO 27001:2022

- Clause changes

✓ Editorial changes to below clauses,
but no solid change in requirements

- 7.4 Communication
- 8.1 Operational planning and control
- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal Audit,
- 9.3 Management Review,
- 10 Improvement

Main Changes to ISO 27001:2022

- Annex A references to controls in ISO/IEC 27002:2022, including information of control title and control
- 114 controls in 14 clauses → 93 controls in 4 clauses
- 11 controls are new, 24 are merged from previous controls, and 58 are updated
- Control structure is revised
  - introduces “attribute” and “purpose” for each control and
  - no longer uses “objective” for a group of controls
- Improve Physical Security
- Include Data Protection and Cloud Security

Examples of ISMS related Regulations

- Sarbanes-Oxley Act (2002) – US
  It establishes sweeping auditing and financial regulations for public companies, with requirements for data security.

- HIPAA (1996) - US
  It protects the personal information related to activities of healthcare industry.

- Federal Information Security Management Act (2002) - US
  It imposes a series of processes for information system used by the Federal Government, its contractors or suppliers.

- GDPR (2018) (More details later) – EU

- Can you name an associated regulation in your country?

Examples of ISMS related Regulations – Industrial Associations

- PCI-DSS (Payment Card Industry Data Security Standard) (2004)

A series of technical and operational controls whose goal is to protect organizations against fraud and other threats related to credit cards.

- Basel II (2004)

Recommendations concerning banking legislations and regulations.

- COBIT (Control Objectives for Business and related Technology) (1994+)

A reference frame to manage the governance of information systems.

Forewords

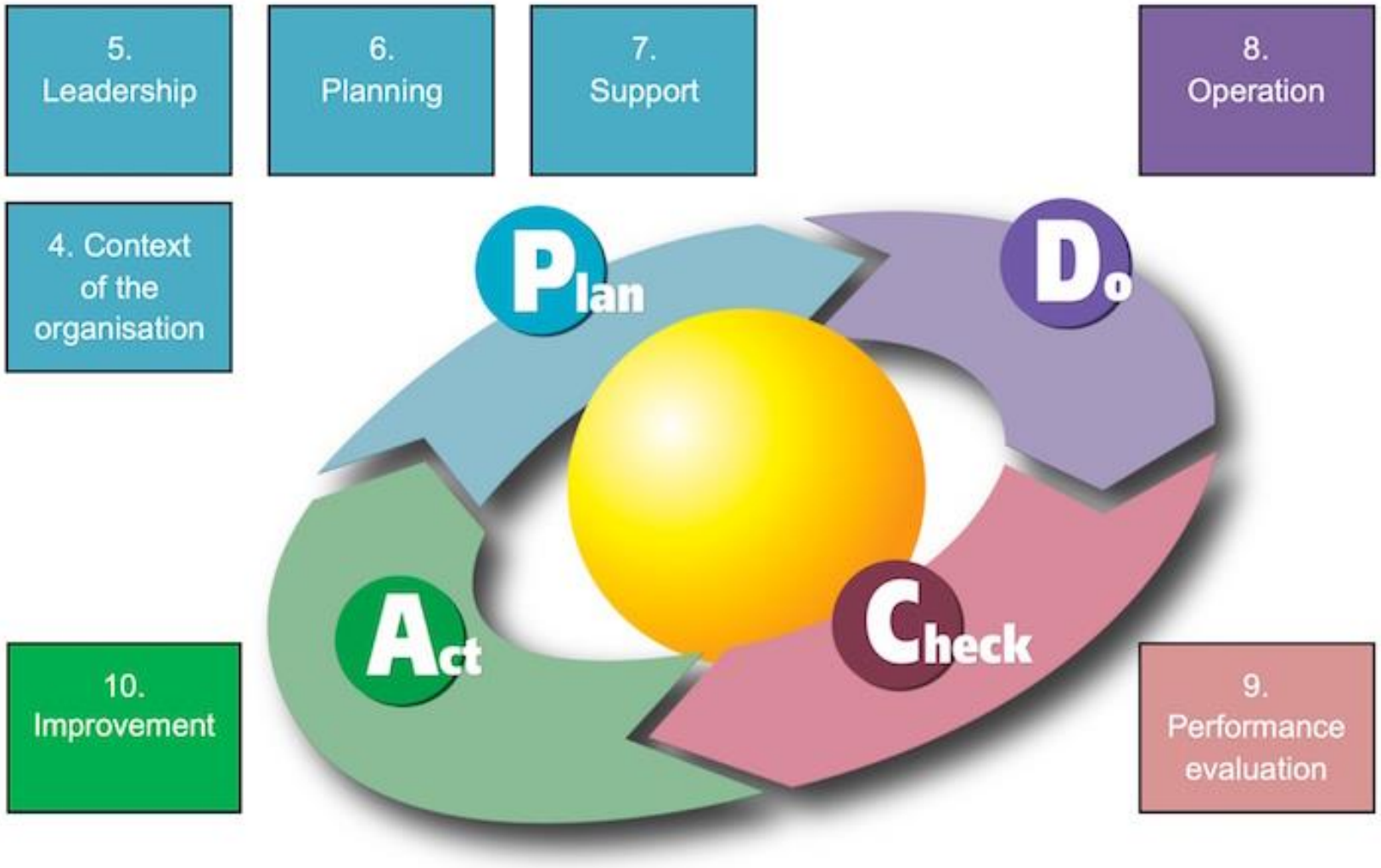
- Information security address the perspectives of:
  A) confidentiality ?
  B) integrity ?
  C) availability ?

- ISMS is part of and integrated with the organization's processes and overall management structure

- High-level structure is applied.
  It facilitates compatibility with other M.S. standards

High Level Structure

<For training by DQS HK only>



Course Agenda 課程安排

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops

Q&A

Evaluation

1. Scope

- It specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS within the context of the organization.
- It includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization
- Applicable to all organizations
- Exclusion of requirements (Clause 5-10) not acceptable

2. Normative references

- ISO/IEC 27000,
  Information technology — Security techniques — Information security management systems — Overview and vocabulary

Important Terms

- Defined in ISO/IEC 27000
- **Information Security**
  preservation of confidentiality, integrity and availability of information
- **Threat**
  potential cause of an information security incident that can result in damage to a system or harm to an organization
- **Vulnerability**
  weakness of an asset or control that can be exploited so that an event with a negative consequence occurs

3. Terms and Definitions

- **Event**
  occurrence or change of a particular set of circumstances

- **information security incident**
  single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations
  and threatening information security

Course Agenda 課程安排

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops

Q&A

Evaluation

4.1
Understanding the organization and its context

- The organization shall determine
  external and internal issues
  that are relevant to its purpose and
  that affect its ability to achieve the intended outcome(s)
  of its ISMS.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system; and

b) the requirements of these interested parties relevant to information security.

c) which of these requirements will be addressed through the ISMS.

Change

4.3 Determining the scope of the information security management system

- The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in **4.1**;

b) the requirements referred to in **4.2**; and

c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

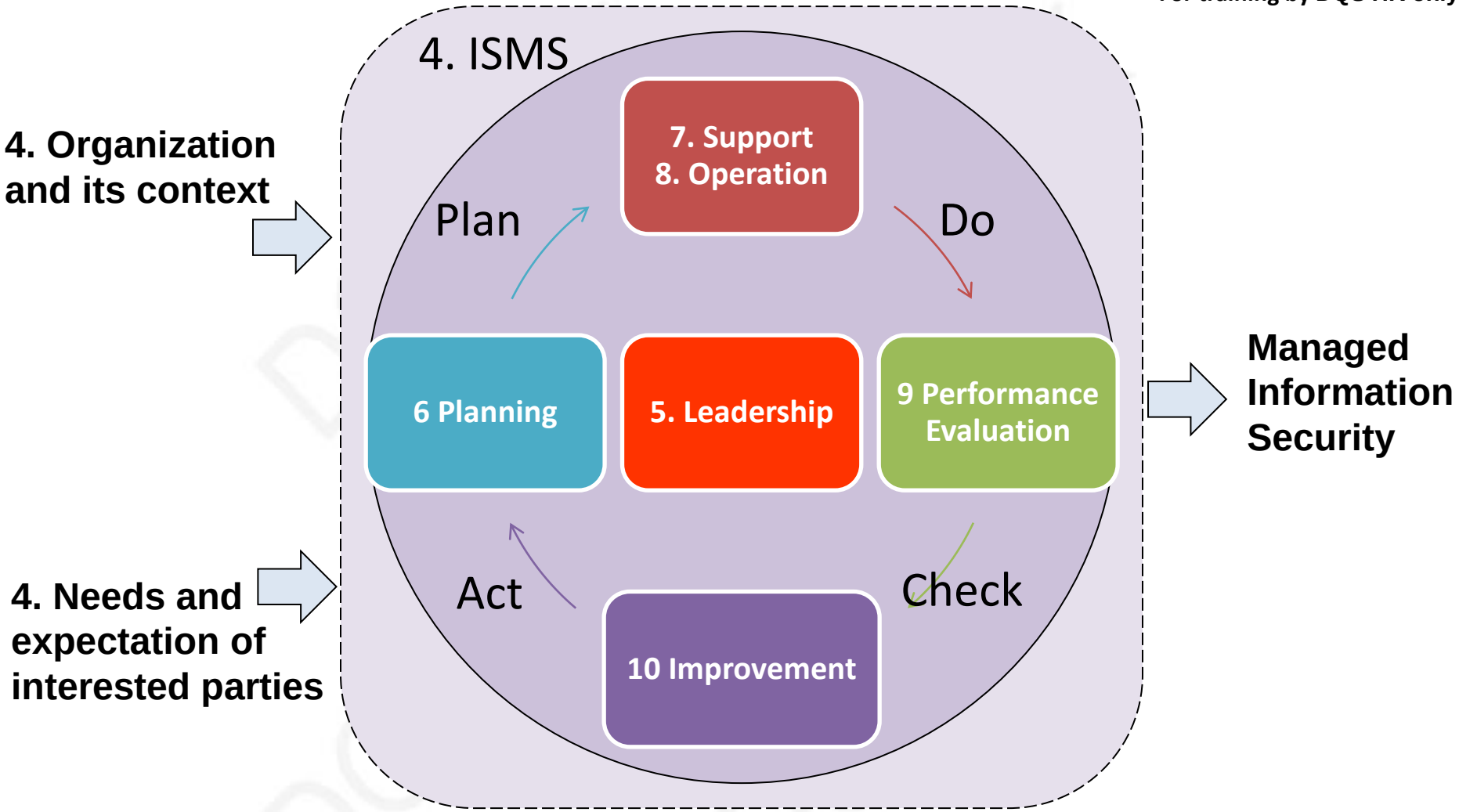
The scope shall be available as documented information.

4.4 Information security management system

- The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this International Standard.

Change

PDCA Cycle


4. Organization and its context
4. Needs and expectation of interested parties
4. ISMS
7. Support
8. Operation
Plan
Do
6 Planning
5. Leadership
9 Performance Evaluation
Act
Check
10 Improvement
Managed Information Security

Course Agenda 課程安排

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops

Q&A

Evaluation

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the ISMS by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of ISMS requirements into the organization's processes;

c) ensuring that the resources needed for ISMS are available;

d) communicating the importance of effective information security management and of conforming to the ISMS requirements;

5. Leadership

5.1

…

e) ensuring that the ISMS achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the ISMS;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security; and

d) includes a commitment to continual improvement of the ISMS.

5.2 Policy

The information security policy shall:

e) be available as documented information;

f) be communicated within the organization; and

g) be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management shall assign the responsibility and authority for:

a) ensuring that the ISMS conforms to the requirements of this International Standard; and

b) reporting on the performance of the ISMS to top management.

NOTE Top management may also assign responsibilities and authorities for reporting performance of the ISMS within the organization.

Course Agenda 課程安排

<For training by DQS HK only>

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops

Q&A

Evaluation

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the ISMS, the organization shall consider
the issues referred to in 4.1 and
the requirements referred to in 4.2 and determine
the risks and opportunities that need to be addressed to:

a) ensure the ISMS can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects; and

c) achieve continual improvement.

6.1.1 …

The organization shall plan:

d) actions to address these risks and opportunities; and

e) how to

1) integrate and implement the actions into its ISMS processes; and

2) evaluate the effectiveness of these actions.

6.1.2 Information security risk assessment

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:
   1) the risk acceptance criteria; and
   2) criteria for performing information security risk assessments;

a) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

6.1.2 …

c) identifies the information security risks:

1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS; and

2) identify the risk owners;

d) analyses the information security risks:

1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;

2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

3) determine the levels of risk;

6.1.2 …

e) evaluates the information security risks:

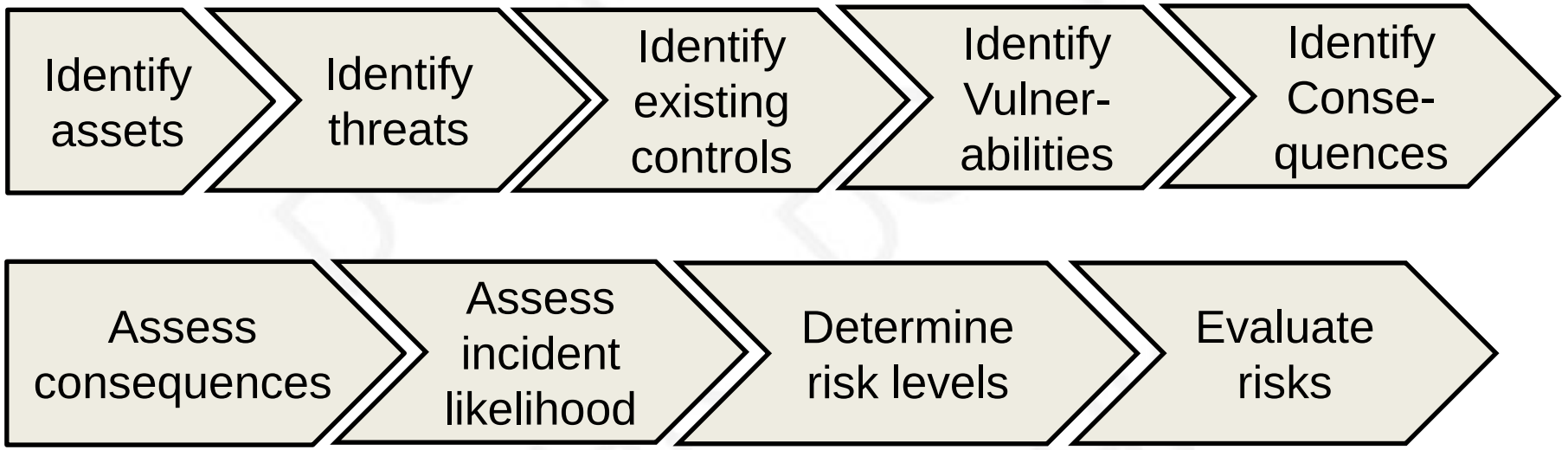
1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security risk assessment process.

Risk Assessment Process

- Typical Risk Assessment Process



6.1.3 Information security risk treatment

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

Note 1 Organizations can design controls as required, or identify them from any source.

6.1.3 …

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

Note 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.

Note 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.

editorial changes only

re-organized to remove ambiguity

6.1.3 …

c) …

d) produce a Statement of Applicability that contains:
- the necessary controls (see 6.1.3 b) and c));
- justification for inclusions,
- whether they are implemented or not, and
- the justification for excluding any of the Annex A controls.

e) formulate an information security risk treatment plan; and

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;
b) be measurable (if practicable);
c) take into account applicable information security requirements, and results from risk assessment and risk treatment;
d) be communicated; and
e) be updated as appropriate.

The organization shall retain documented information on the information security objectives.

6.2

...

When planning how to achieve its information security objectives, what shall be determined by the organization?

a) what will be done
b) what resources will be required
c) who will be responsible
d) when it will be completed
e) how the results will be evaluated

6.3 Planning of changes

When the organization determines the need for changes to the ISMS, the changes shall be carried out in a planned manner.

Addition of clause

Course Agenda 課程安排

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops

Q&A

Evaluation

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS.

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and

c) the implications of not conforming with the ISMS requirements.

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the ISMS including:

a) on what to communicate;
b) when to communicate;
c) with whom to communicate;
d) how to communicate.

Change

7.5 Documented information

7.5.1 General

The organization's ISMS shall include:

a) documented information required by this International Standard; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

NOTE
The extent of documented information for an ISMS can differ from one organization to another due to:

1) the size of organization and its type of activities, processes, products and services;

2) the complexity of processes and their interactions; and

3) the competence of persons.

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the ISMS and by this International Standard shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

7.5.3 Control of documented information

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including the preservation of legibility;

e) control of changes (e.g. version control); and

f) retention and disposition.

7.5.3 Control of documented information

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the ISMS, shall be identified as appropriate, and controlled.

NOTE Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

Course Agenda 課程安排

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops

Q&A

Evaluation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria.

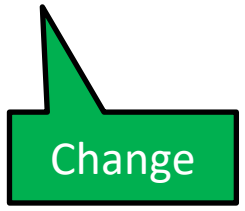
Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

editorial change to 8.1

8.1 Operational planning and control

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the ISMS are controlled.



8.2 Information security risk assessment

The organization shall perform
information security risk assessments
at planned intervals or
when significant changes are proposed or occur,
taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

Course Agenda 課程安排

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops

Q&A

Evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results.
The methods selected should produce comparable and reproducible results to beconsidered valid;

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated;

f) who shall analyse and evaluate these results.

editorial change to 9.1

9.1 Monitoring, measurement, analysis and evaluation

...

Documented information shall be available as evidence of the results.

The organization shall evaluate the information security performance and the effectiveness of the ISMS.

9.2 Internal audit

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to

1) the organization's own requirements for its ISMS;

2) the requirements of this document;

b) is effectively implemented and maintained.

editorial change to 9.2

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider

- the importance of the processes concerned and
- the results of previous audits.

9.2.2 Internal audit programme

…

The organization shall:

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management.

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

9.3 Management review

9.3.1 General

Top management shall review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

9.3.2 Management review inputs

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the ISMS;

c) changes in needs and expectations of interested parties that are relevant to the ISMS;

editorial change to 9.3

9.3.2 Management review inputs

The management review shall include consideration of:

…

d) feedback on the info. sec. performance, including trends in:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results;

4) fulfilment of information security objectives;

e) feedback from interested parties;

f) results of risk assessment and status of risk treatment plan;

g) opportunities for continual improvement.

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the ISMS.

Documented information shall be available as evidence of the results of management reviews.

Course Agenda 課程安排

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops

Q&A

Evaluation

10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the ISMS.

editorial change to 10

10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

1) take action to control and correct it;

2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of NC, in order that it does not recur or occur elsewhere, by:

1) reviewing the nonconformity;

2) determining the causes of the nonconformity; and

3) determining if similar NCs exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the ISMS, if necessary.

10.1 Nonconformity and corrective action

…

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Documented information shall be available as evidence of:

f) the nature of the nonconformities and any subsequent actions taken,

g) the results of any corrective action.

Course Agenda 課程安排

<For training by DQS HK only>

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops

Q&A

Evaluation

Main Changes to Annex A in ISO 27001:2022

- Control categories are reduced from 14 to 4:
  - ✓ 37 organizational controls (clause 5)
  - ✓ 8 people controls (clause 6)
  - ✓ 14 physical controls (clause 7)
  - ✓ 34 technological controls (clause 8)
- Number of controls decrease from 114 to 93.

Main Changes to Annex A in ISO 27001:2022

- 11 New Controls:
  - ✓ 5.7 Threat intelligence
  - ✓ 5.23 Information security for use of cloud services
  - ✓ 5.30 ICT readiness for business continuity
  - ✓ 7.4 Physical security monitoring
  - ✓ 8.9 Configuration management
  - ✓ 8.10 Information deletion
  - ✓ 8.11 Data masking
  - ✓ 8.12 Data leakage prevention
  - ✓ 8.16 Monitoring activities
  - ✓ 8.23 Web filtering
  - ✓ 8.28 Secure coding

Main Changes to Annex A in ISO 27001:2022

- Control 18.2.3 Technical Compliance Review
  was split into:
  - ✓ 5.3.6 –
    Compliance with policies, rules and standards for information security;
  - ✓ 8.8 –
    Management of technical vulnerabilities
- 57 controls have been merged into 24 controls
- 58 controls are updated
- Any original control is excluded?

Annex A

- Determine the applicable controls and exclusions based primarily on the outcome of risk assessment

- Can an organization apply additional security objectives and controls and include them in the Statement of Applicability?

Course Agenda 課程安排

<For training by DQS HK only>

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops (separated documents)

Q&A

Evaluation

Course Agenda 課程安排

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops

Q&A

Evaluation

Course Agenda 課程安排

<For training by DQS HK only>

Forewords

- **Scope, References, Terms**
- **Context of the organization**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance evaluation**
- **Improvement**

Annex

Workshops (ebbed in each section)

Q&A

Evaluation

Annex A

(normative)

Information security controls reference

The information security controls listed in **Table A.1** are directly derived from and aligned with those listed in ISO/IEC 27002:2022, Clauses 5 to 8, and shall be used in context with **6.1.3**.

Table A.1 - Information security controls

(Separated document)

Thanks !

Simply leveraging Quality.

DQS HK

德國體系認證集團 成員

www.dqsglobal.com/en-hk/

Info.hk@dqs.de