Complex World.
Real Solutions.
Securing Success.

SESSION 314: ISO 27001—WHAT YOU NEED TO KNOW ABOUT RECENT CHANGES

Peter T. Davis
Principal, Peter Davis+Associates

ISACA

- IT Governance consulting
- CISA, CISSP, CMA, CMC, CISM, COBIT 5 FC, ITIL FC, PMP, SSGB, CGEIT, PRINCE2 FC, ISO 27001 LI/LA, ISO 20000 FC, ISO 27005/31000 RM, ISO 28000 FC
- 29 years IT security and audit experience
- Authored/co-authored 12 books
- *International Who's Who of Professionals*
- Contact information

ptdavis@pdaconsulting.com
www.pdaconsulting.com
(v) 416-907-4041
(f) 416-907-4851

Session Objectives

- Understand key differences
- Understand new requirements
- Understand added controls and deleted controls

Big Picture

- Evolution NOT Revolution
- Harmonization
- Much of the 2005 text and requirements still there, but moved around to fit the new headings
- Not as big a migration as BS 7799 to ISO 17799

+80%

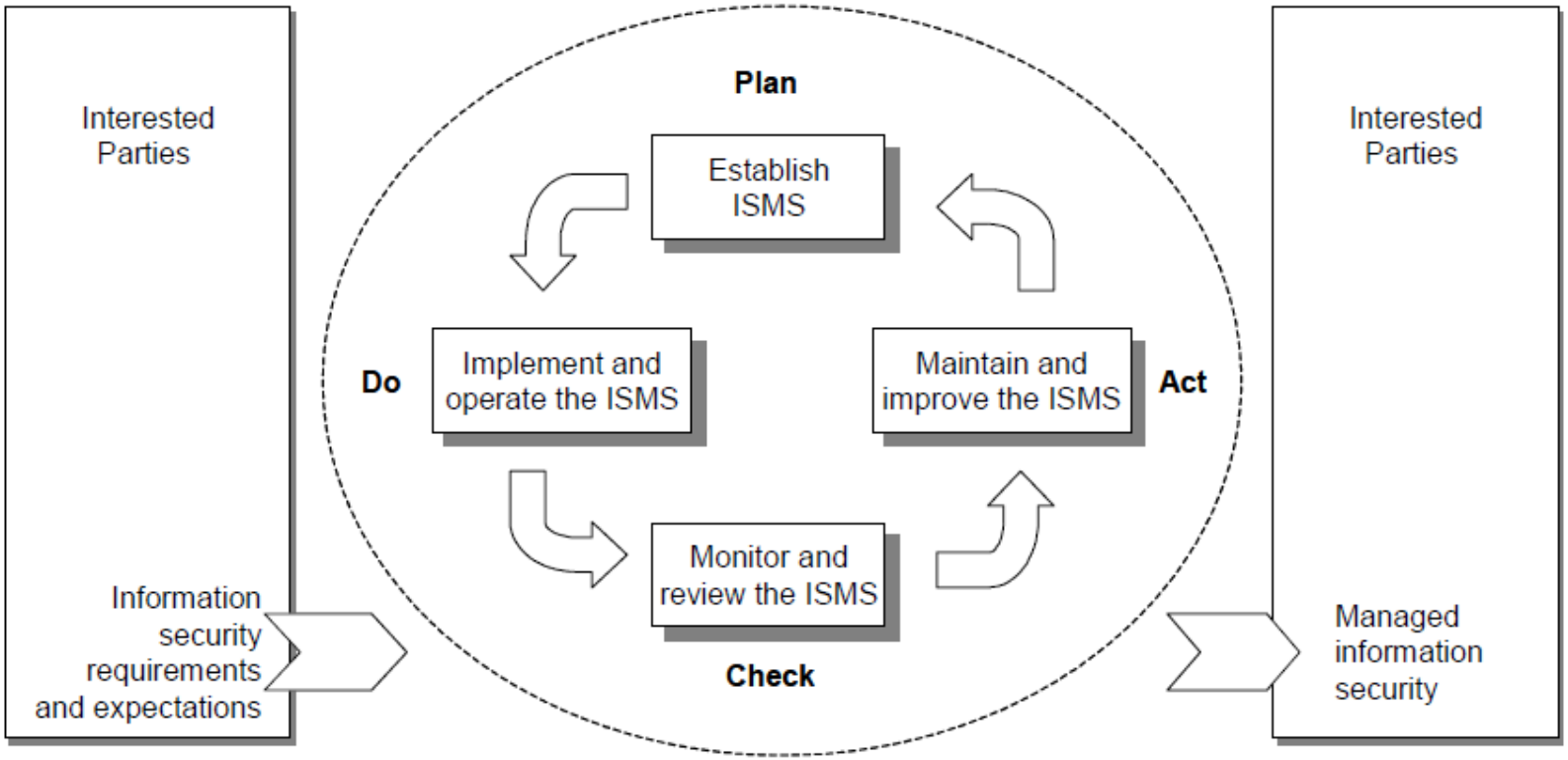


Figure 1 — PDCA model applied to ISMS processes

Source: ISO/IEC 27001:2005

5 Key Differences

- Written in accordance with Annex SL
- ISO 27002 is no longer a normative reference
- Definitions removed and relocated to ISO 27000
- Changes to terminology; e.g., IS policy is used rather than ISMS policy
- Requirements for Management Commitment revised and presented in the Leadership Clause

4 More Differences

- Preventive action replaced with “actions to address risks and opportunities” and features earlier in the standard
- Risk assessment requirements more general and align with ISO 31000
- SoA requirements are similar but more clarity on the determination of controls by the risk treatment process
- Greater emphasis on setting the objectives, monitoring performance and metrics

New Document Structure

- Developed using Annex SL
  - For standard writers
  - Provides standardized text suitable for all MS standards
- New structure to become common for all MS standards
- Want to standardize terminology and requirements for fundamental MS requirements

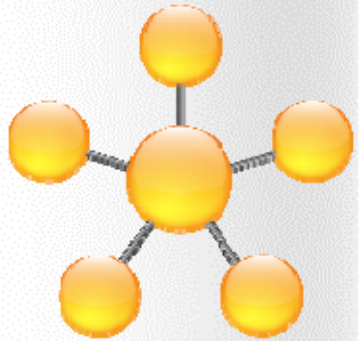


Table of Contents

2005		2013	
0	Introduction	0	Introduction
1	Scope	1	Scope
2	Normative References	2	Normative References
3	Terms and Definitions	3	Terms and Definitions
4	Information Security Management System	4	Context of the Organization
5	Management Responsibility	5	Leadership
6	Internal ISMS Audit	6	Planning
7	Management Review of the ISMS	7	Support

Table of Contents

2005		2013	
8	ISMS Improvement	8	Operation
		9	Performance Evaluation
		10	Improvement
A	Control Objectives and Controls	A	Control Objectives and Controls
B	OECD Principles and this International Standard		
C	Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard		

3 Terms and Definitions

- All definitions removed
- Relevant definitions moved to ISO 27000
- Promotes consistency of terms and definitions across the ISO 27000 suite

4 Context of the Organization

- Relates to the context of the organization—Determine external and internal issues
- Clear requirement to consider interested parties
- Context determines IS policy and objectives and how the organization will consider risk and the effect of risk on its business
- Requirements of interested parties may include legal and regulatory requirements and contractual obligations

External Context

- Social, cultural, political, legal, regulatory, financial, technological, economic, natural & competitive environment (international, national, regional, or local)
- Key drivers & trends having impact on the objectives of the organization
- Relationships with, and perceptions & values of, external stakeholders

Internal Context

- Organization's culture
- Governance, organizational structure, roles & accountabilities
- Policies and objectives and the strategies in place to achieve them
- Capital in terms of resources & knowledge (e.g., money, time, people, processes, systems and technologies)
- Informal & formal info systems, info flows & decision making processes
- Adopted standards, guidelines & models
- Form & extent of contractual relationships
- Relationships with, and perceptions & values of, internal stakeholders

5 Leadership

- Summarizes the requirements specific to top management's role in the ISMS
- Outlines specific ways for management to demonstrate its commitment to the system. Examples include:
  - ensuring that the resources needed for the ISMS are available
  - communicating the importance of effective IS management and conforming to the ISMS requirements.
- ISMS policy renamed, but original policy requirements remain
- Requires that top management ensure responsibilities and authorities for roles relevant to IS are assigned and communicated

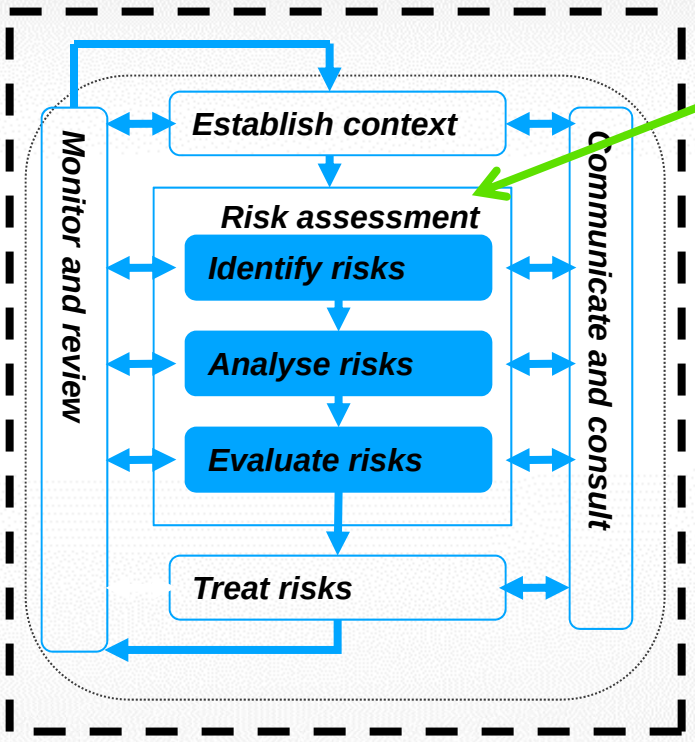
6 Planning

- Establishment of IS objectives and guiding principles for the ISMS
- When planning the ISMS, the context of the organization should be taken into account through the consideration of the risks and opportunities
- Organization's IS objectives must be clearly defined with plans in place to achieve them
- Risk assessment requirements more general and align with ISO 31000
- SoA requirements largely unchanged (name dropped)

Risk

- Risk Owner rather than Data Owner
- Only required to identify risks w.r.t. CIA
- Includes “upside risk” a.k.a Opportunities
- Risk treatment plan (RTP) used to create a SoA

Process for Managing Risk



Process for Managing Risk

Risk Treatment Plan

- Clause 6.1.3 describes how an organization can respond to risks with a RTP; an important part of this is choosing appropriate controls
- These controls, and control objectives, are listed in Annex A, although it is also possible in principle for organizations to pick other controls elsewhere

7 Support

- Required to establish, implement and maintain and continually improve an effective ISMS, including:
  - Resource requirements
  - Competence of people involved
  - Awareness of and communication with interested parties
  - Requirements for document management
- Refers to “documented information” rather than “documents and records”
- No longer a list of documents you need or particular names they must be given
- Puts emphasis on the content rather than the name

8 Operation

- Requires organizations to plan and control the operation of their IS requirements
- Will include:
  - Carrying out IS risk assessments at planned intervals
  - Implementing an IS RTP

9 Performance Evaluation

- Internal audits and management review key methods of reviewing the performance of the ISMS and tools for its continual improvement
- More specific requirements for measurement of effectiveness

10 Improvement

- Nonconformities of the ISMS have to be dealt with together with corrective actions to ensure they don't happen again
- As with all MS standards, continual improvement is a core requirement of the standard

Controls

2005		2013
Security Policy	Renamed	Information Security Policies
Security Organization	Renamed	How Information Security is Organized
Asset Management	Moved	Human Resources Security
Human Resources Security	Moved	Asset Management
Physical and Environmental Security	Renamed	Access Control and Managing User Access
Communications and Operations Management	Split	Cryptographic Technology
Access Control	Renamed	Physical Security of the Organisation's Sites and Equipment

Controls

2005		2013
Information Systems Acquisition, Development and Maintenance	Renamed	Operational Security
Information Security Incident Management	Moved	Secure Communications and Data Transfer
Business Continuity Management	Renamed	Secure Acquisition, Development and Support of Information Systems
Compliance	Unchanged	Security for Suppliers and Third Parties
		Information Security Incident Management
		Information Aspects of Business Continuity Management
		Compliance

Controls

- Number of controls reduced from 133 to 113
- Controls now in 14 groups (2005: 11 groups)
- Existing controls deleted or merged and some new controls added
- Some of the retained controls have been re-worded

Deleted Controls

A.6.1.1	Management commitment to information security
A.6.1.2	Information security coordination
A.6.1.4	Authorization process for information processing facilities
A.6.2.1	Identification of risks related to external parties
A.6.2.2	Addressing security when dealing with customers
A.10.2.1	Service delivery
A.10.7.4	Security of system documentation
A.10.10.2	Monitoring system use
A.10.10.5	Fault logging
A.11.4.2	User authentication for external connections
A.11.4.3	Equipment identification
A.11.4.4	Remote diagnostic and configuration port protection

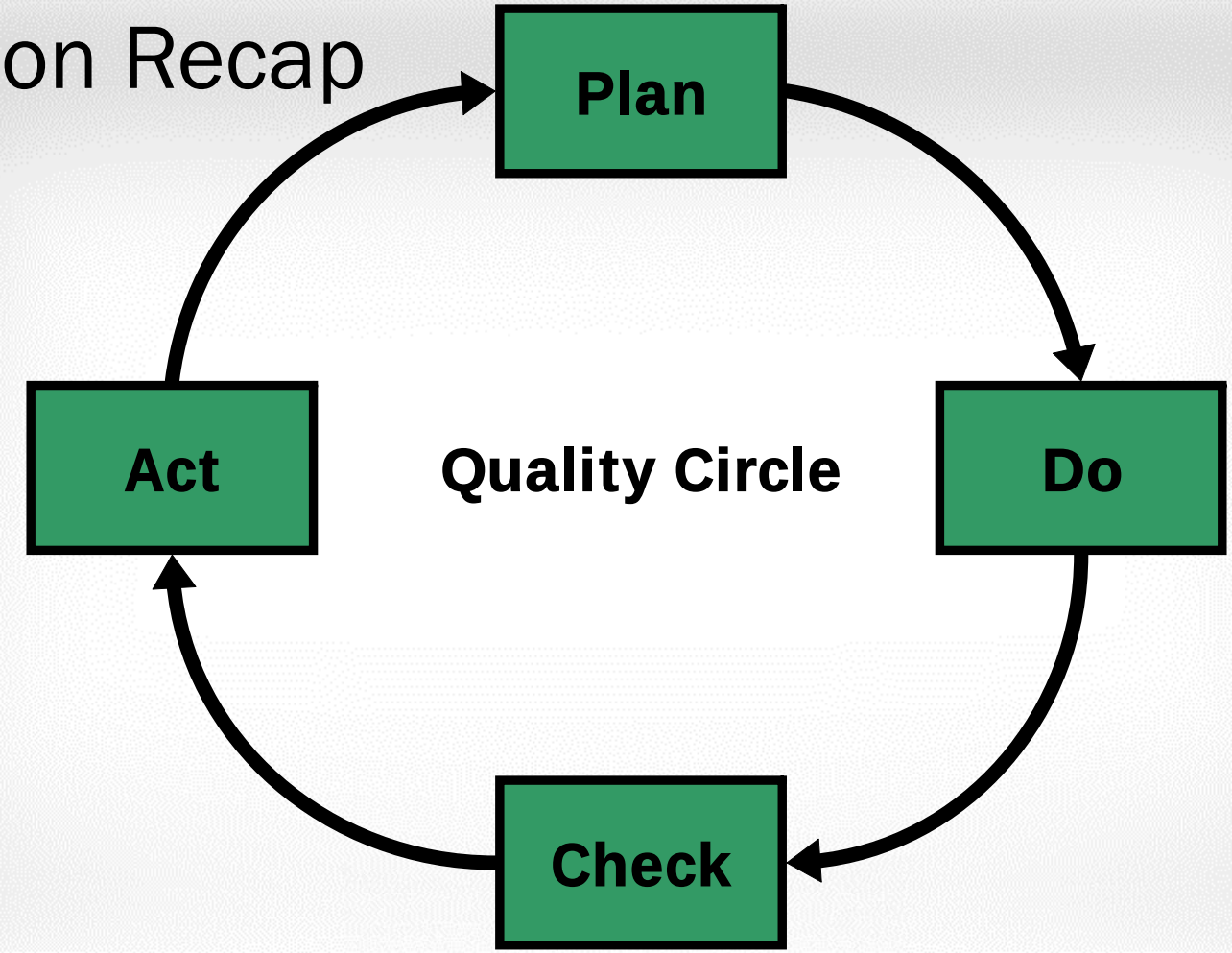
Deleted Controls

A.11.4.4	Remote diagnostic and configuration port protection
A.11.4.6	Network connection control
A.11.4.7	Network routing control
A.10.8.5	Business information systems
A.11.6.2	Sensitive system isolation
A.12.2.1	Input data validation
A.12.2.2	Control of internal processing
A.12.2.3	Message integrity
A.12.2.4	Output data validation
A.12.5.4	Information leakage
A.15.1.5	Prevention of misuse of information processing facilities
A.15.3.2	Protection of information systems audit tools

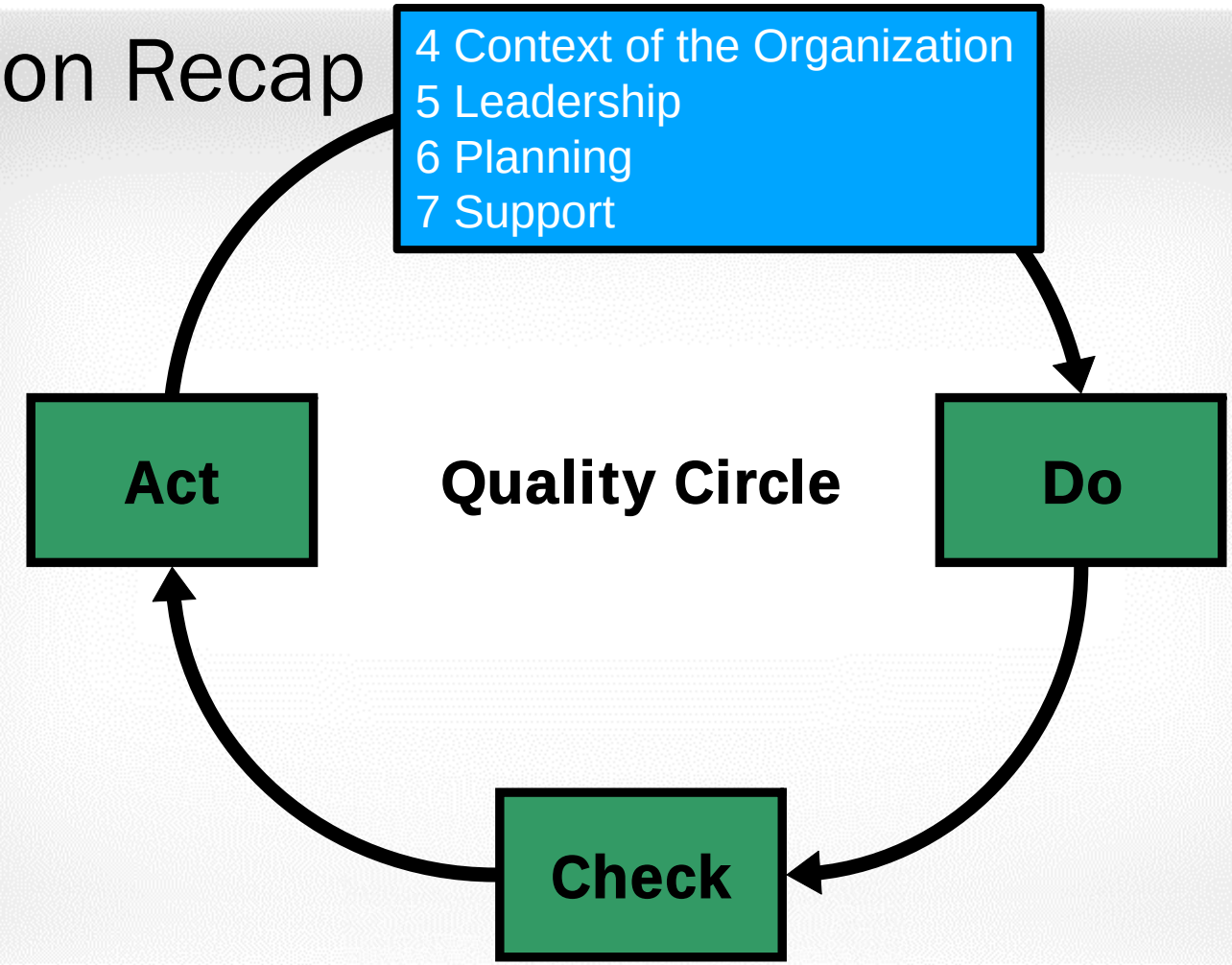
Added Controls

A.6.1.5	Information security in project management
A.12.6.2	Restrictions on software installation
A.14.2.1	Secure development policy
A.14.2.5	Secure system engineering principles
A.14.2.6	Secure development environment
A.14.2.8	System security testing
A.15.1.1	Information security policy for supplier relationships
A.15.1.3	Information and communication technology supply chain
A.16.1.4	Assessment of and decision on information security events
A.16.1.5	Response to information security incidents
A.17.2.1	Availability of information processing facilities

Session Recap

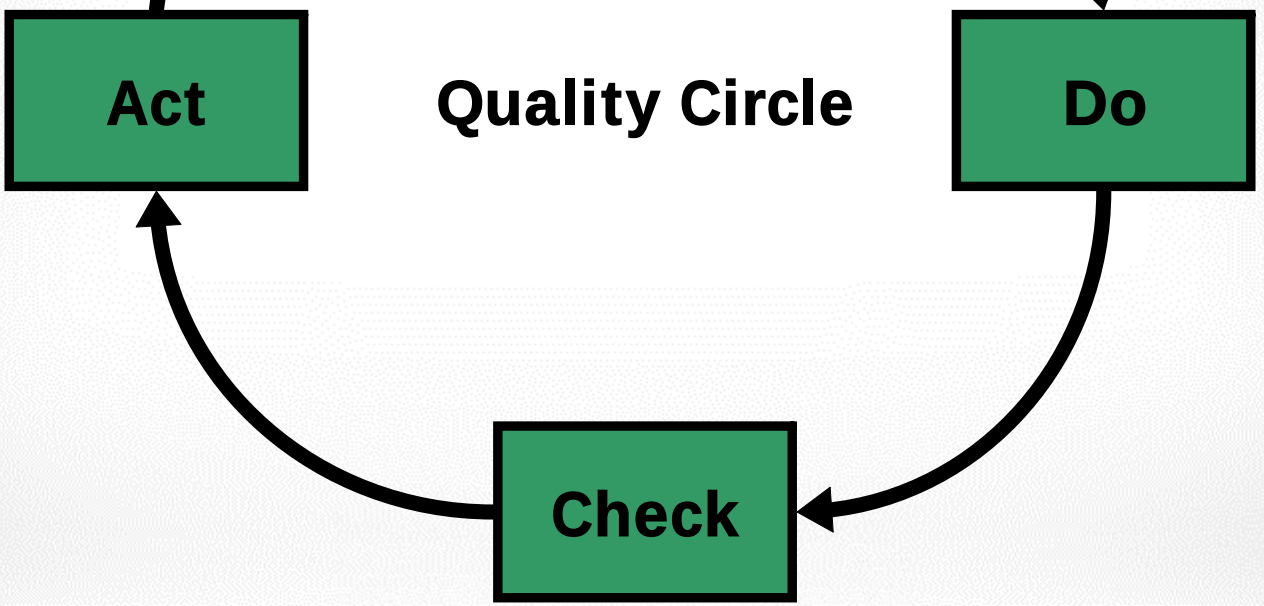


Session Recap

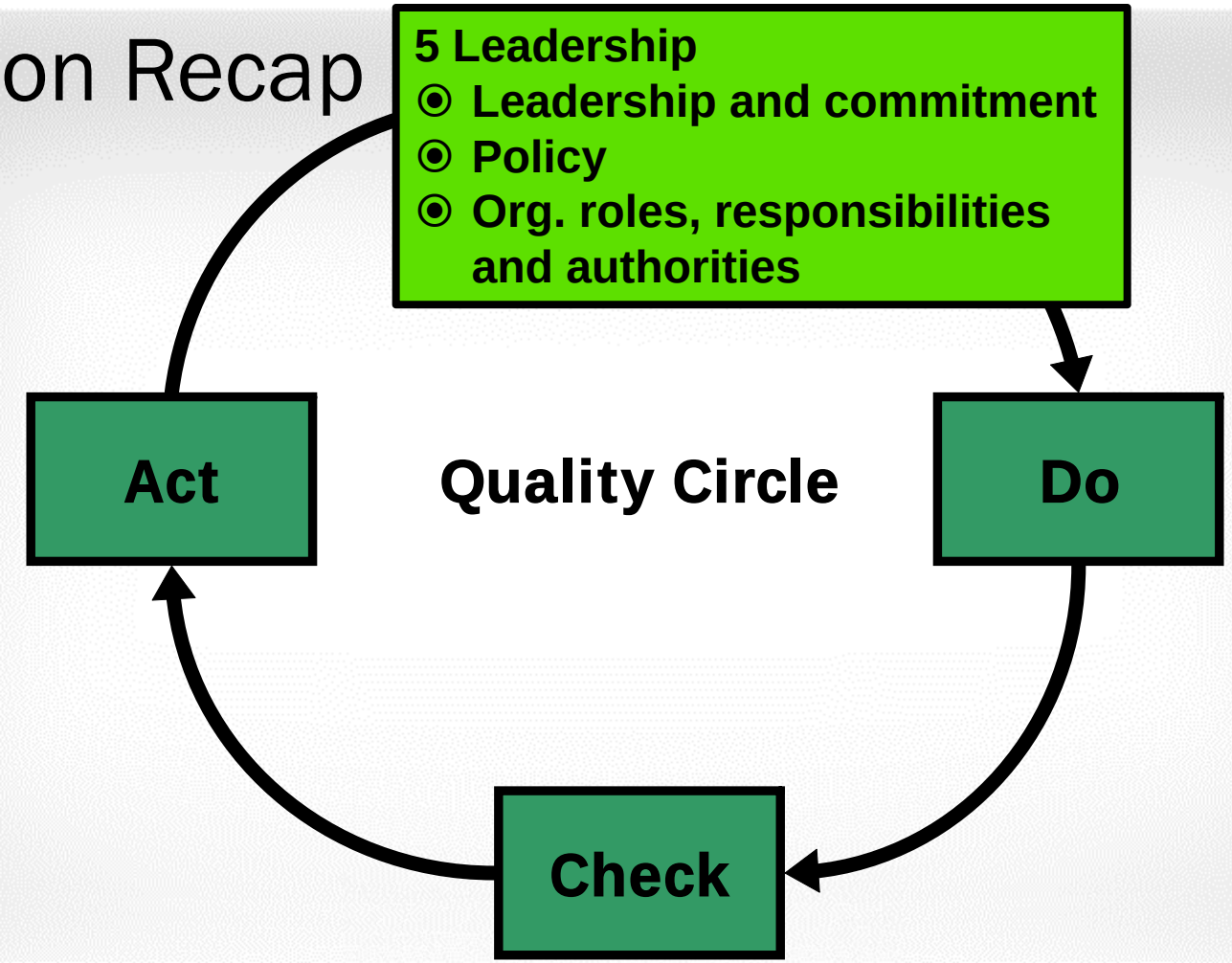


Session Recap

4 Context of the Organization
- **Understanding the organization and its context**
- **Expectations of interested parties**
- **Scope of ISMS**
- **ISMS**

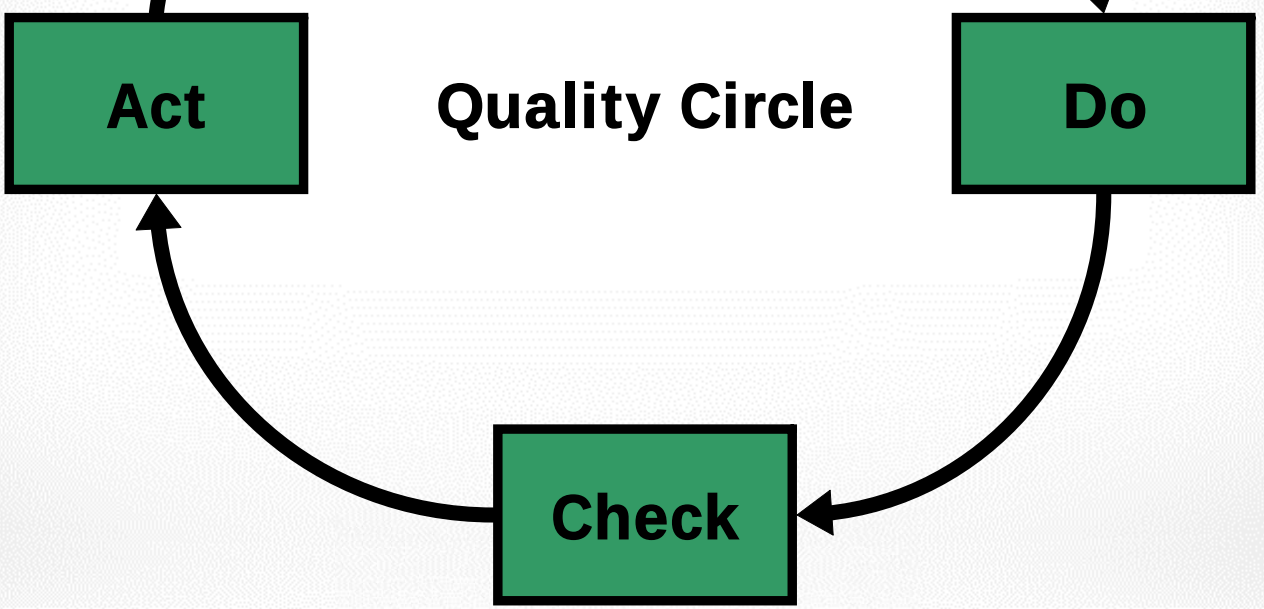


Session Recap

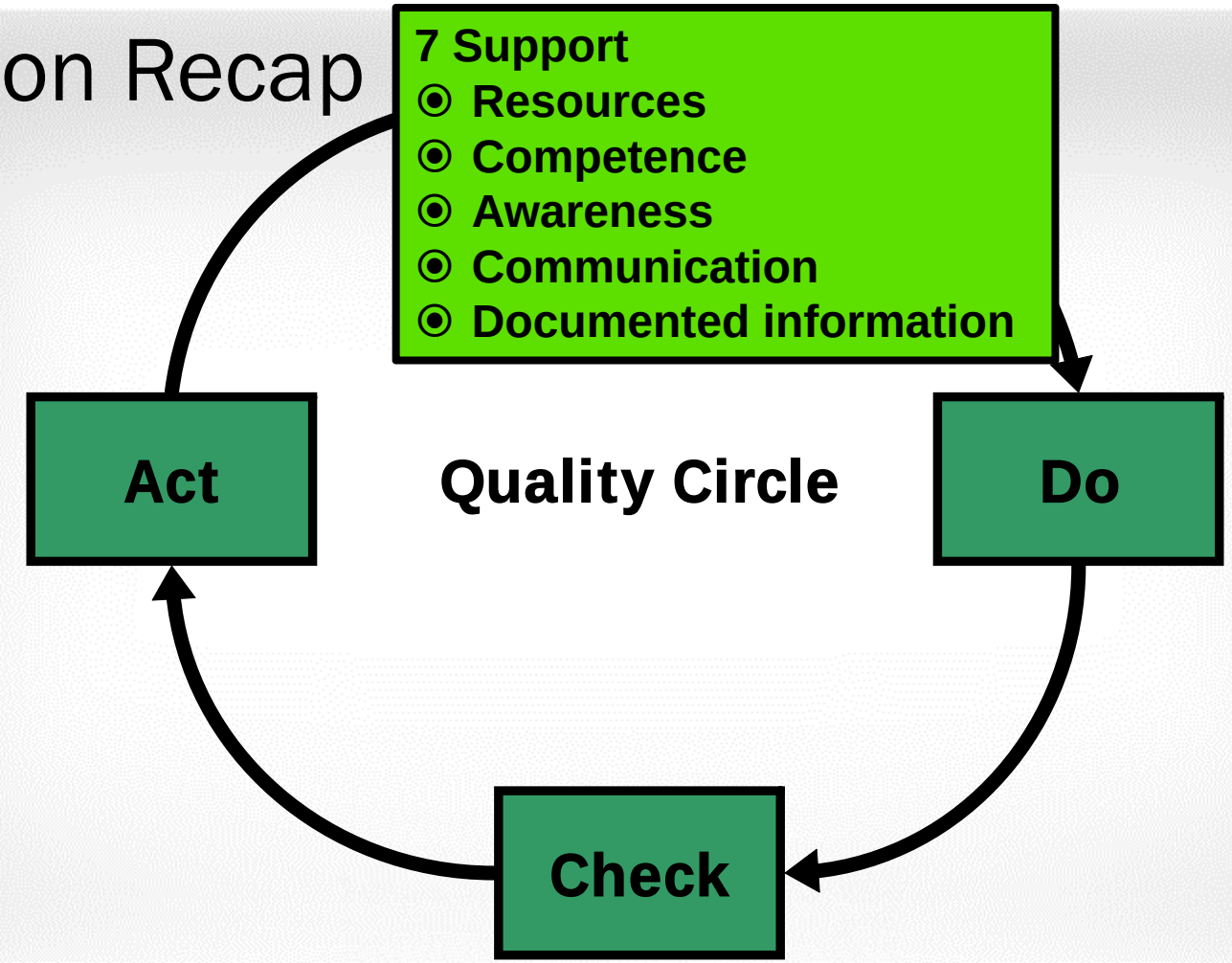


Session Recap

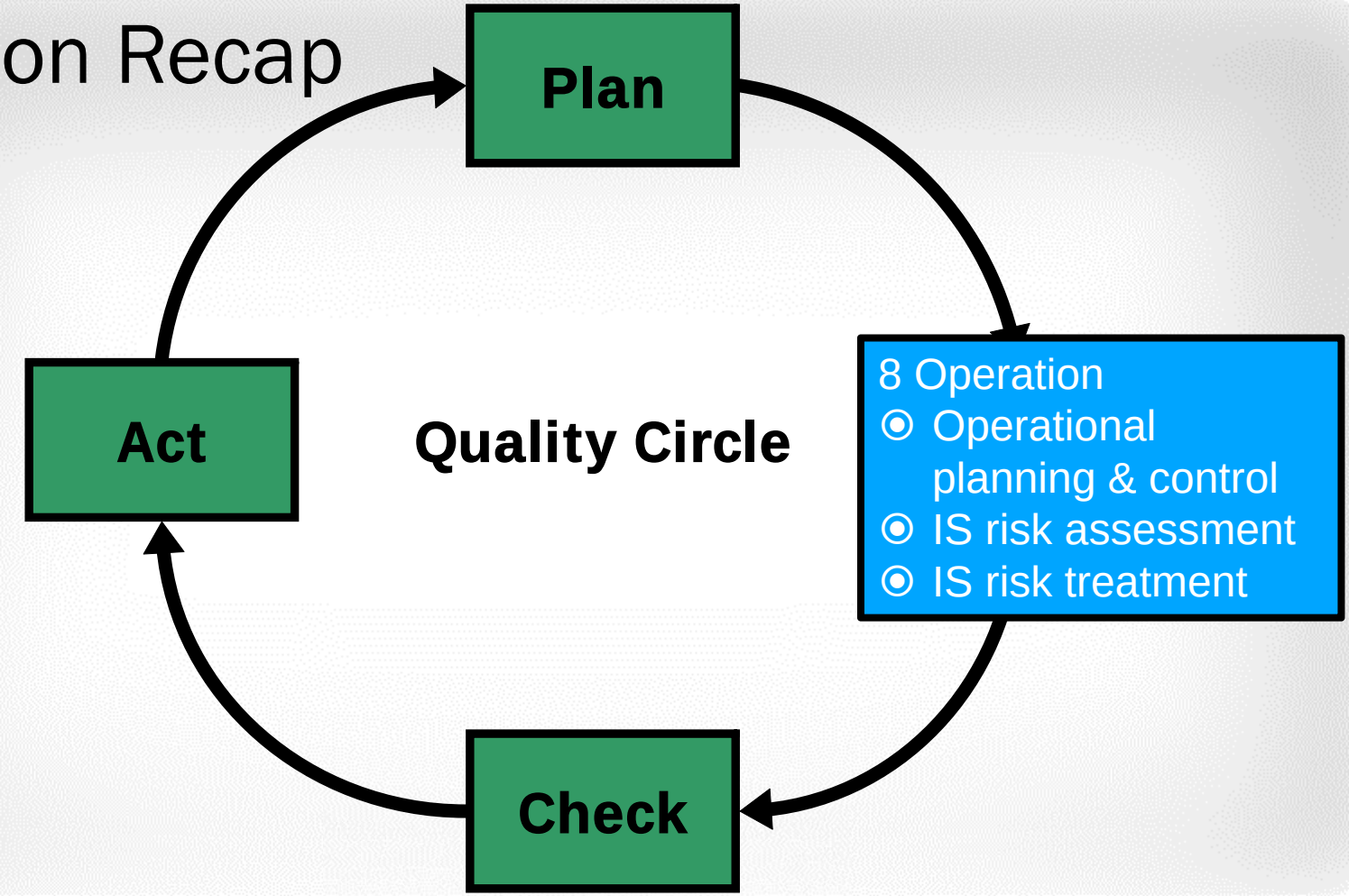
6 Planning
- **Actions to address risks and opportunities**
- **IS objectives and plans to achieve them**



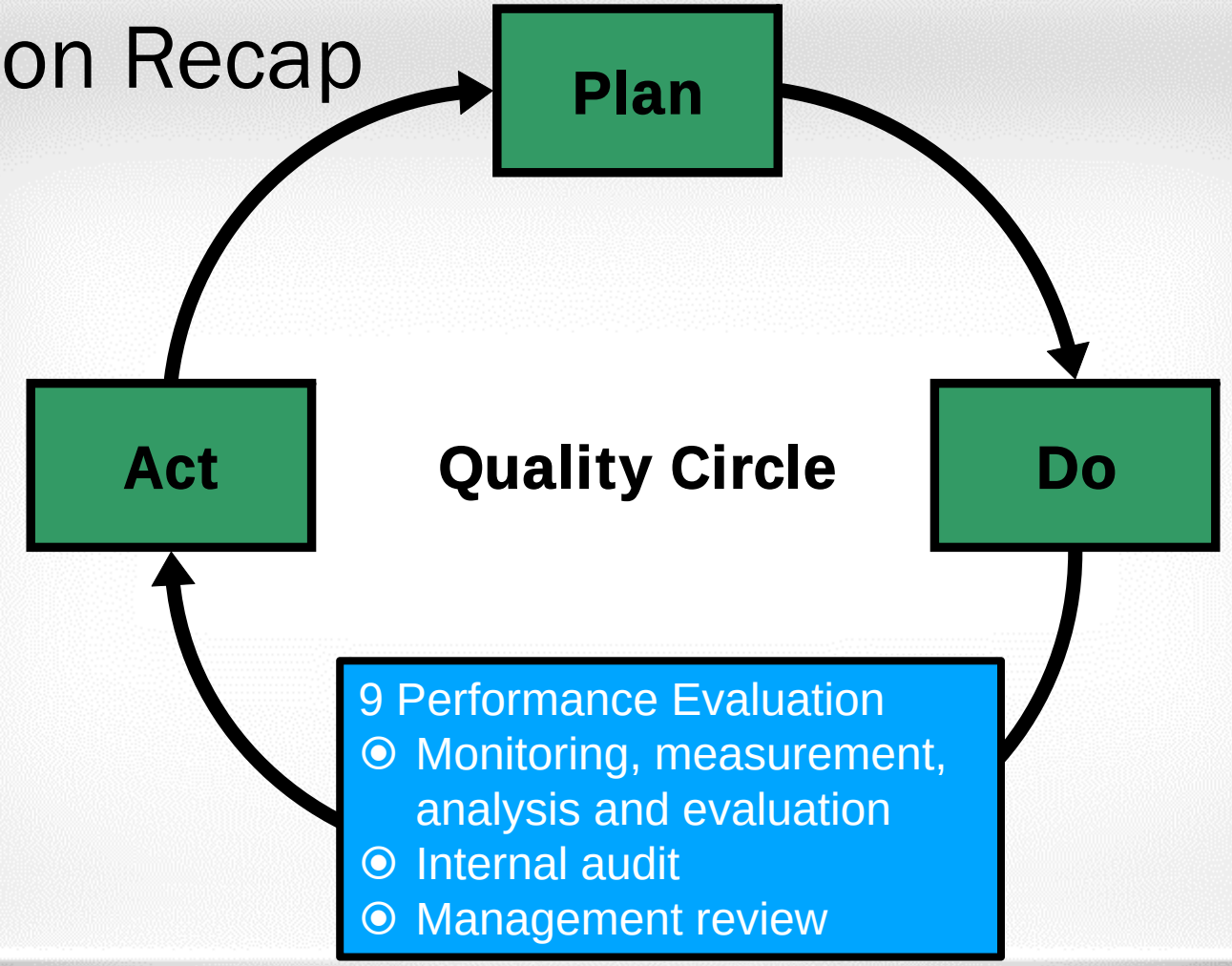
Session Recap



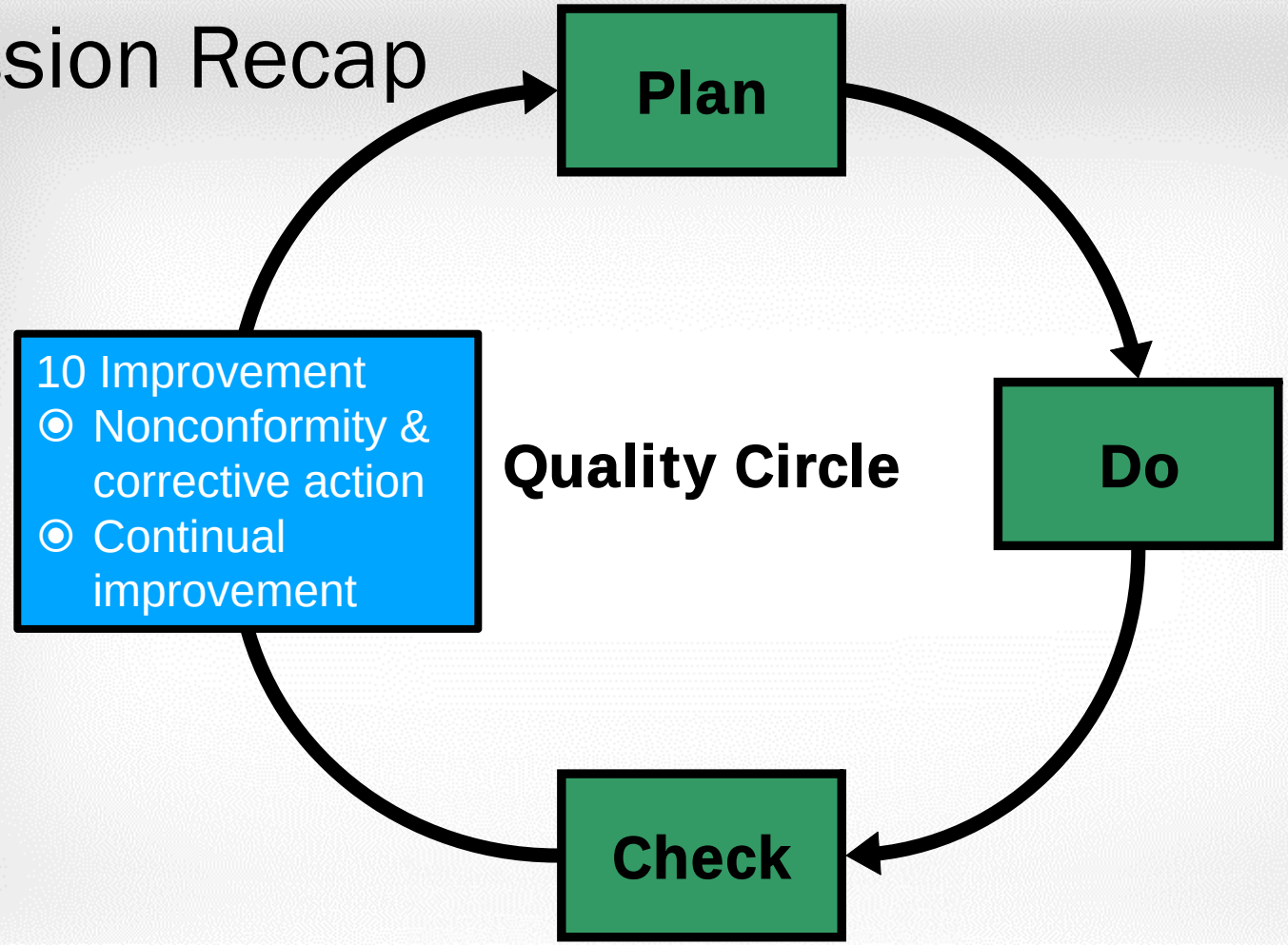
Session Recap



Session Recap



Session Recap



Take Home Thoughts

- Less descriptive and prescriptive
- Greater freedom in implementing
- Transition period for certified organizations

Standard Comparison (1/10)

ISO 27001:2005	ISO 27001:2013	Change
0.2 Process Approach	Eliminated from this new standard	PDCA Model was an explicit section in the older version unlike the newer one, which adopts this model all throughout the mandatory clauses, but does not occupy a separate and dedicated section in the standard.
1. Scope 1.1 General 1.2 Applications	These sub-sections are eliminated from this new standard	Sub Sections 1.1 General and 1.2 Application of older version are now merged into one section 1. Scope. The set of mandatory clauses in the old standard were from 4 to 8, which is now changed to 4 to 10 in the new version.

Standard Comparison (2/10)

ISO 27001:2005	ISO 27001:2013	Change
4. Information security management system	4. Context of the organization	ISMS is renamed as Context of the Organization
4.1. General Requirements	4.1. General Requirements	The Old standard talks about Documented ISMS, whereas the New one strongly focuses on understanding the context of business. Also, a reference to ISO31000 – the Risk Management standard is added.

Standard Comparison (3/10)

ISO 27001:2005	ISO 27001:2013	Change
4.2 Establishing and managing the ISMS	4.2. Understanding the needs and expectations of interested parties	The huge importance of interested parties, which can include shareholders, authorities (including legal and regulatory requirements), clients, partners, etc., is recognized in the new ISO 27001 – there is a separate clause that specifies that all the interested parties must be listed, together with all their requirements. This is definitely an excellent way of defining key inputs into the ISMS.

Standard Comparison (4/10)

ISO 27001:2005	ISO 27001:2013	Change
4.2.1 a) to j) Establish the ISMS	6.1. Actions to address risks and opportunities	**Risk assessment and treatment** Assets, vulnerabilities and threats are not the basis of risk assessment anymore! It is only required to identify the risks associated with the confidentiality, integrity and availability – although this might seem too radical of a change, the authors of the new standard wanted to allow more freedom in the way the risks are identified. However, the assets-vulnerabilities-threats methodology will remain as a best practice for a long time. The concept of determining the level of risk based on consequences and likelihood remains the same. Further, Risk Assessment Methodology does not need to be documented, although the risk assessment process needs to be defined in advance; the concept of asset owner is gone, too – a new term is used: “risk owners” – so the responsibility is pushed to a higher level.

Standard Comparison (5/10)

ISO 27001:2005	ISO 27001:2013	Change
4.3 Documentation Requirements	**Documented information (No Dedicated Sub-Section)4.3.** Determining the scope of the information security management system	The concepts of “documents” and “records” are merged together; so, now it is “documented information.” Consequently, all the rules that are required for documentation control are now valid for both documents and records; the rules themselves haven’t changed much from the old ISO 27001. The requirement in the old standard for documented procedures (Document control, Internal audit, Corrective action, Preventive action) is eliminated – however, the requirement for documenting the output from those processes remains in the new standard. Therefore, we don’t need to write all these procedures, but we are required to maintain all the records when managing documents, performing internal audits, and executing corrective actions. Also, the clause from the old standard where all the required documents are listed (4.3.1) is removed – now there is no central list of required documents.

Standard Comparison (6/10)

ISO 27001:2005	ISO 27001:2013	Change
	New Clause 4.4. Information security management system	
5. Management responsibility	**5. Leadership**	
5.1. Management Commitment	**5.1. Leadership and commitment**	Unlike the older version, the newer version talks only about the need of Leadership and Management's Commitment. Policy related clauses are moved to a separate sub-section.

Standard Comparison (7/10)

ISO 27001:2005	ISO 27001:2013	Change
5.2. Resource Management	**5.2. Policy**	This is a dedicated sub-section for the backbone document of ISMS; i.e., the IS Policy
	5.3. Organizational roles, responsibilities and authorities	New addition. An individual sub-section in the newer version.
6. Internal ISMS audits	6. Planning	PDCA not explained explicitly but embedded into the mandatory clauses in the newer version, with the mapping as under: P-6; D-7 & 8; C-9; A-10 It completely talks about, Risks, Opportunities, Information Security Risk Assessment and Treatment, unlike the older one which only focused on the ISMS mandated Internal Audits.

Standard Comparison (8/10)

ISO 27001:2005	ISO 27001:2013	Change
7. Management Review of the ISMS	9.3. Management Review 7. Support 7.1 Resources 7.2 Competence 7.3 Awareness 7.4 Communication 7.5 Documented Information	Unlike the older version, in this newer version, Management Review has been made a sub-section, of the Performance Evaluation Clause. 7· New clause in the new standard 7.4. This is also a new clause where all the requirements are summarized – what needs to be communicated, when, by whom, through which means, etc. This will help overcome the problem of information security being only an "IT thing" or "security thing" – the success of information security depends on both the IT side and the business side, and their overall understanding about the purpose of information protection. Hence this dedicated emphasis on Communication can be seen as a good change.

Standard Comparison (9/10)

ISO 27001:2005	ISO 27001:2013	Change
8. ISMS Improvement	8. Operations10.2 of the newer version	The Elaborated DO phase in the new version. Contains Risk Assessment Requirements However, the older version talked about CAPA, and continual improvement, the “ACT” phase

Standard Comparison (10/10)

ISO 27001:2005	ISO 27001:2013	Change
None	9. Performance Evaluation	The separate “CHECK” Phase, talking about, measurement, monitoring, analysis and evaluation along with Internal Audits and Management Reviews
None	10. Improvement	Talks about NCs, Corrective Actions and Continual Improvement. No Explicit mention of Preventive Actions.

Deleted Controls (1/9)

Control	Rationale
A.6.1.1 Management commitment to information security	Claimed that this is not a control but part of the ISO/IEC 27001 management commitment requirement
A.6.1.2 Information security coordination	Claimed removed as this deals with the establishment of an ISMS and guidance is to be found in ISO/IEC 27003
A.6.1.4 Authorisation process for information processing facilities	Appears no longer explicitly addressed, as it seems to be an aspect of A.6.1.1
A.6.2.1 Identification of risks related to external parties	Claimed that this is not a control but part of the ISO/IEC 27001 risk assessment/risk treatment requirements

Deleted Controls (2/9)

Control	Rationale
A.6.2.2 Addressing security when dealing with customers	Claimed that this is not a control but part of the ISO/IEC 27001 risk assessment/risk treatment requirements
A.10.2.1 Service delivery	No reason given
A.10.7.4 Security of system documentation	Claimed that this control has been removed on the grounds that system documentation is just another form of asset that requires protection. Its removal therefore requires consideration during risk assessment of whether such documents, should they fall into the wrong hands, present a source of risk.

Deleted Controls (3/9)

Control	Rationale
A.10.8.5 Business Information Systems	Claimed removed on the grounds that the control really relates to the whole standard reflecting and trying to do it more or less in a single control doesn't really work.
A.10.10.2 Monitoring system use	Appears considered to be part of Event Logging (A.12.4.1)
A.10.10.5 Fault logging	Now appears referenced in Event Logging (A.12.4.1)
A.11.4.2 User authentication for external connections	Claimed covered by access control (A.9.1.1)

Deleted Controls (4/9)

Control	Rationale
A.11.4.3 Equipment identification in networks	Appears covered by A.13.1.3
A.11.4.4 Remote Diagnostic and configuration port protection	Claimed that separate physical diagnostic ports are becoming rare and that protection is covered through access control (A.9.1.1) and segregation in networks control (A.13.1.3).
A.11.4.6 Network Connection control	Claimed covered by A.13.1.3
A.11.4.7 Network routing control	Claimed covered by A.13.1.3

Deleted Controls (5/9)

Control	Rationale
A.11.6.2 Sensitive system isolation	Claimed that in an interconnected world such a control defeats the objective. However, we note that it may still apply in certain cases.
A.12.2.1 Input data validation	Claimed that since this control was introduced, technology has moved on, and input data validation is just one small aspect of protecting web interfaces from attacks such as SQL injection. There are some remarks in the “Other Information” section of A.14.2.5, but the general understanding appears now is that such techniques lie firmly in the domain of professional software developers and are therefore outside the scope of ISO/IEC 27002.

Deleted Controls (6/9)

Control	Rationale
A.12.2.2 Control of internal processing	See A.14.2.5 and the explanation above.
A.12.2.3 Message integrity	Appears to be a duplication of material in A.13.2.1.
A.12.2.4 Output data validation	See A.14.2.5 and the explanation above.
A.12.5.4 Information leakage	Claimed that this control was deleted because it only covered part of the problem associated with information leakage, and indeed there is coverage elsewhere. For example, the term "leakage" appears in A.8.3.2, A.11.2.1, A.12.6.2 and A.13.2.4 as guidance and other information. Note., however, we note that the term "covert channel" does not appear in the DIS. Adware viruses, some of which are known to leak information, would be addressed by A.12.2.1.

Deleted Controls (7/9)

Control	Rationale
A.14.1.1 Including information security in the business continuity management process	There used to be five "controls" and now there are three. Two these (planning/RA and testing) map well onto two of these originals. The other three originals perhaps merit being called controls even less than everything else in the 2005 version; "principles" would be a more apt description. From our experience, this control is often just mapped to the BCP as a whole and therefore this control could be mapped to A.17.1.2.
A.14.1.3 Developing and implementing continuity plans including formation security.	For the reason cited above, this control could be mapped to A.17.1.2.

Deleted Controls (8/9)

Control	Rationale
A.14.1.4 Business continuity planning framework	For the reason cited above, this control could be mapped to A.17.1.2.
A.15.1.5 Prevention of misuse of information processing facilities	This control corresponds to a UK law and could be a remnant of the original BS7799:1995 standard which was completely UK centric. Its omission is effectively covered by the new A.18.2.1 which requires all relevant laws to be identified. Thus, in the UK, this control is effectively dealt with by that control. Moreover, there is mention of "warning banners" in A.9.4.2.

Deleted Controls (9/9)

Control	Rationale
A.15.3.2 Protection of information systems audit tools	Claimed that this control has been removed on the grounds that an audit tool is just another form of asset that requires protection. Its removal therefore requires consideration during risk assessment of whether such tools present a source of risk.

Copyright

- This session is the copyright of Peter Davis+Associates © 2013. All rights reserved.

ISACA