มีอะไรใหม่ในมาตรฐาน ?

ISO 22301:2019

Business Continuity Management System

17.03.2020

Speaker Profile

วิทยากร : นิจิรา วัฒนพันธุ์

ตำแหน่ง : Consultant

บริษัท : ACinfotec Co., Ltd.

ประสบการณ์ :

- ที่ปรึกษามาตรฐาน ISO 22301 ให้ธนาคารในประเทศ
- ที่ปรึกษามาตรฐาน ISO 22301 ให้หน่วยงานภาครัฐ ภาคเอกชน และหน่วยงานโครงสร้างพื้นฐานที่สำคัญของประเทศ
- ที่ปรึกษามาตรฐาน ISO 20000 ให้หน่วยงานภาคเอกชน

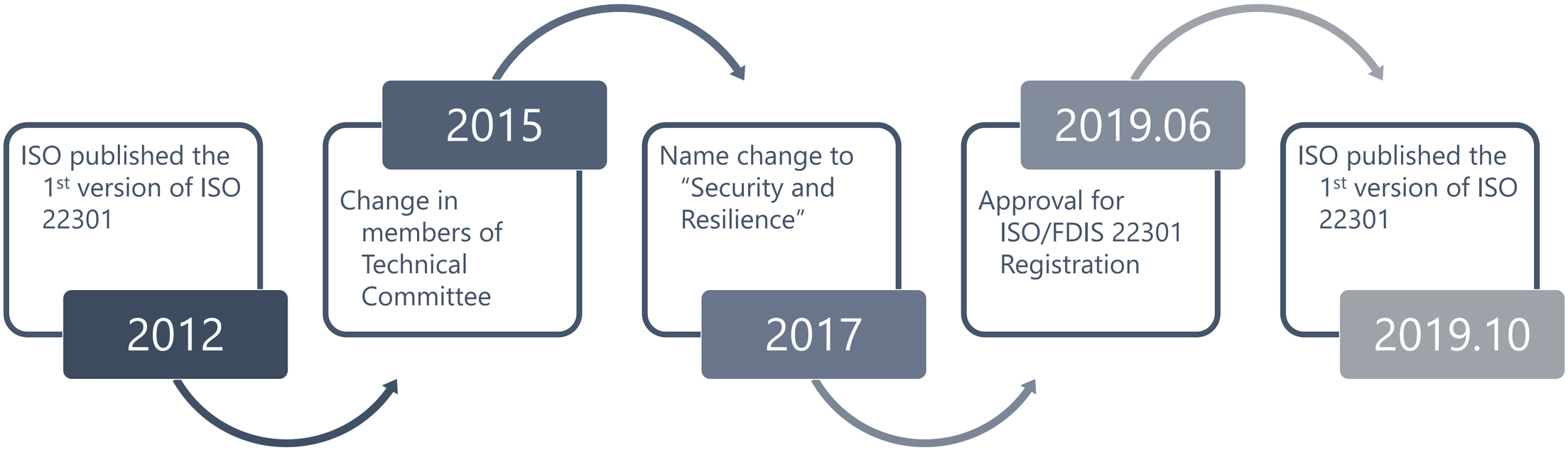
ประกาศนียบัตร :

- PECB Certified ISO 22301 Lead Implementer
- PECB Certified ISO/IEC 20000 Lead Auditor
- PECB Certified ISO/IEC 27032 Provisional Cybersecurity Manager
- PECB Certified Trainer
- ITIL 4 Foundation

Agenda

- Timeline of ISO 22301:2019 Publication
- ISO 22301 Second Edition 2019-10
- ISO 22301 Version 2019 and 2012
- Minimum Documentation Requirements
- Key Changes in ISO 22301:2019

Timeline of ISO 22301:2019 Publication



ISO 22301 Second Edition 2019-10

INTERNATIONAL STANDARD

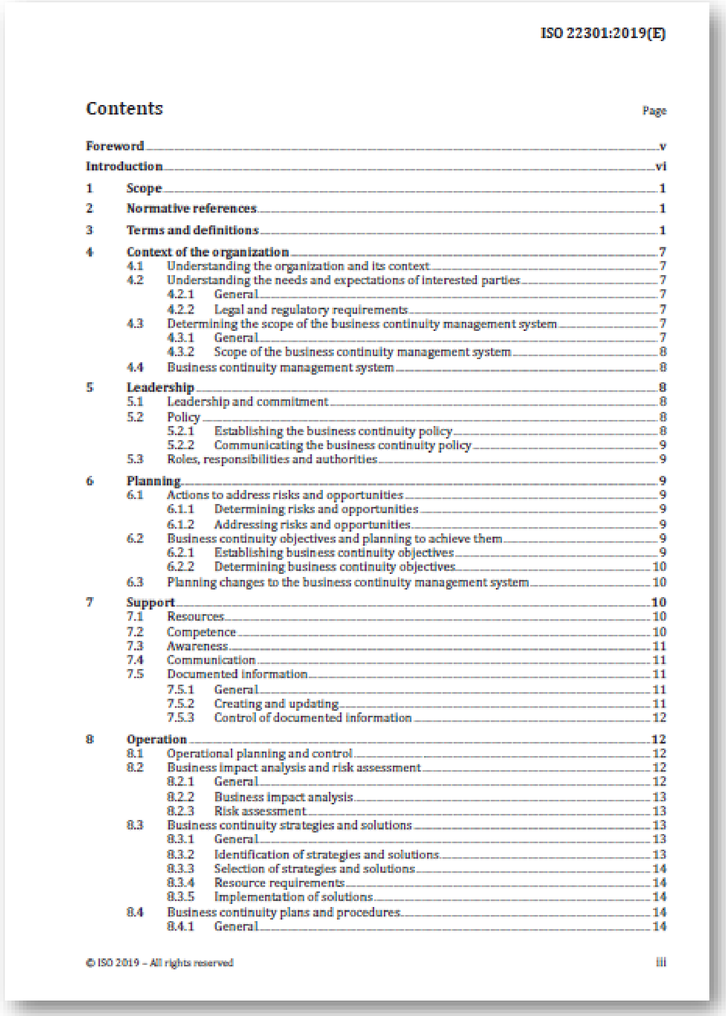
ISO 22301

Second edition
2019-10

Security and resilience — Business continuity management systems — Requirements

Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences

Reference number
ISO 22301:2019(E)



Contents Page

Clause 1 – Clause 10

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

Introduction
Clause 1: Scope
Clause 2: Normative references
Clause 3: Terms & definitions

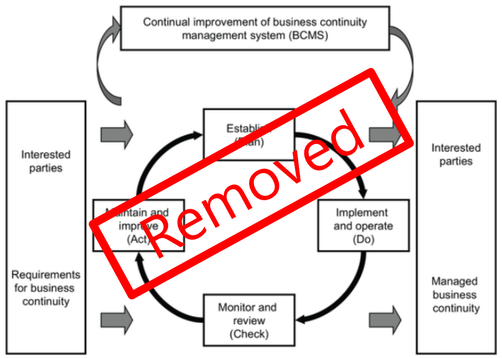
ISO 22301 Version 2019 and 2012

ISO 22301:2019	ISO 22301:2012
Introduction	0 Introduction
1 Scope	1 Scope
2 Normative references	2 Normative references
3 Terms and definitions	3 Terms and definitions

Introduction & Clause 1 – Clause 3

Introduction

- Following verbal forms are used:
  - “shall” indicates a requirement (ข้อกำหนด)
  - “should” indicates a recommendation (คำแนะนำ)
  - “may” indicates a permission (การอนุญาต)
  - “can” indicates a possibility or a capability (ความเป็นไปได้หรือความสามารถ)
- Graph of PDCA Cycles has been removed



Introduction & Clause 1 – Clause 3

Clause 1: Scope

- No significant change in content

Clause 2: Normative Reference

- Link to ISO 22300, *Security and resilience – Vocabulary*

Introduction & Clause 1 – Clause 3

Clause 3: Terms and definitions

- Changes in terminology (reduction from 55 to 31)
- Sample of changes in Terms

New
Disruption
Impact

Modified
Activity
Audit
Business continuity
Business continuity plan
Business impact analysis
Corrective action
Incident
Prioritized activity
Production and service

Removed
Business continuity management
Business continuity management system
Business continuity programme
Document
Event
Exercise
Infrastructure
Internal audit
Production and service
MAO, MTPD* and MBCO
Mutual aid agreement

Removed
Performance evaluation
Personnel
Procedure
Product and service
RTO*, RPO
Risk appetize
Risk assessment
Risk management
Testing
Verification
Work environment

*included in sub-clause 8.2.2 note of d) and e)

Clause 4: Context of the organization

ISO 22301 Version 2019 and 2012

ISO 22301:2019	ISO 22301:2012
4 Context of the organization	4 Context of the organization
4.1 Understanding the organization and its context	4.1 Understanding of the organization and its context
4.2 Understanding the needs and expectations of interested parties	4.2 Understanding the needs and expectations of interested parties
4.2.1 General	4.2.1 General
4.2.2 Legal and regulatory requirements	4.2.2 Legal and regulatory requirements
4.3 Determining the scope of the business continuity management system	4.3 Determining the scope of the business continuity management system
4.3.1 General	4.3.1 General
4.3.2 Scope of the business continuity management system	4.3.2 Scope of BCMS
4.4 Business continuity management system	4.4 Business continuity management system

Clause 4: Context of organization

ISO 22301:2019	
4 Context of the organization	
4.1 Understanding the organization and its context	Simplified with less prescriptive - Exclude requirement to document this process
4.2 Understanding the needs and expectations of interested parties	Simplified - Remove communication of new or changed legal & regulatory to affected employees and other interested parties
4.2.1 General	
4.2.2 Legal and regulatory requirements	

4.3 Determining the scope of the business continuity management system	Simplified
	- Scope determination
	  - Add 'take into account location of organization '
	  - Remove 'consideration of needs & interests of interested parties (customers, investors, etc.)'

4.3.1 General	
4.3.2 Scope of the business continuity management system	
4.4 Business continuity management system	No change

Clause 5: Leadership

ISO 22301 Version 2019 and 2012

ISO 22301:2019	ISO 22301:2012
5 Leadership	5 Leadership
5.1 Leadership and commitment	5.1 Leadership and commitment 5.2 Management commitment
5.2 Policy	5.3 Policy
5.2.1 Establishing the business continuity policy	
5.2.2 Communicating the business continuity policy	
5.3 Roles, responsibilities and authorities	5.4 Organizational roles, responsibilities and authorities

Clause 5: Leadership

ISO 22301:2019	
5 Leadership	
5.1 Leadership and commitment	Merged 5.1 and 5.2 to become 5.1 - Remove requirement for evidence of top management commitment
5.2 Policy	Divided to 2 sub-clauses - No significant change
5.2.1 Establishing the business continuity policy	
5.2.2 Communicating the business continuity policy	
5.3 Roles, responsibilities and authorities	Renamed - No significant change

Clause 6: Planning

Comparison ISO 22301 Version 2019 and 2012

ISO 22301:2019	ISO 22301:2012
6 Planning	6 Planning
6.1 Actions to address risks and opportunities	6.1 Actions to address risks and opportunities
6.1.1 Determining risks and opportunities	
6.1.2 Addressing risks and opportunities	
6.2 Business continuity objectives and planning to achieve them	6.2 Business continuity objectives and plans to achieve them
6.2.1 Establishing business continuity objectives	
6.2.2 Determining business continuity objectives	
6.3 Planning changes to the business continuity management system	

Clause 6: Planning

ISO 22301:2019	
6 Planning	
6.1 Actions to address risks and opportunities	Divided to 2 sub-clauses - No significant change - Include note to clarify risk in 6.1 and 8.2
6.1.1 Determining risks and opportunities	
6.1.2 Addressing risks and opportunities	
6.2 Business continuity objectives and planning to achieve them	Renamed Divided to 2 sub-clauses - Refer 'organization' shall establish BC objective not 'top management' - State that BC objectives shall be communicated
6.2.1 Establishing business continuity objectives	
6.2.2 Determining business continuity objectives	
6.3 Planning changes to the business continuity management system	New requirement - Require organizations make changes to BCMS in planned manner

Clause 6: Planning

Clause 6.3: Planning changes to the business continuity management system

When planning changes to BCMS, the organization shall consider:

- The purpose of the changes and their potential consequences
- The integrity of the BCMS
- The availability of resources
- The allocation or reallocation of responsibilities and authorities

Clause 7: Support

Comparison ISO 22301 Version 2019 and 2012

ISO 22301:2019	ISO 22301:2012
7 Support	7 Support
7.1 Resources	7.1 Resources
7.2 Competence	7.2 Competence
7.3 Awareness	7.3 Awareness
7.4 Communication	7.4 Communication
7.5 Documented information	7.5 Documented information
7.5.1 General	7.5.1 General
7.5.2 Creating and updating	7.5.2 Creating and updating
7.5.3 Control of documented information	7.5.3 Control of documented information

Clause 7: Support

ISO 22301:2019	
7 Support	
7.1 Resources	- No significant change
7.2 Competence	- No significant change
7.3 Awareness	Slightly modified - Emphasize of employees' awareness of their R&R before, during, and after disruptions
7.4 Communication	Simplified with less prescriptive - Remove 'establishment', 'implementation', and 'maintenance' of communication procedures
7.5 Documented information	Divided 7.5.3 into 2 sub-clauses - No significant change
7.5.1 General	
7.5.2 Creating and updating	
7.5.3 Control of documented information	

Clause 8: Operation

Comparison ISO 22301 Version 2019 and 2012

ISO 22301:2019	ISO 22301:2012
8 Operation	8 Operation
8.1 Operational planning and control	8.1 Operational planning and control
8.2 Business impact analysis and risk assessment	8.2 Business impact analysis and risk assessment
8.2.1 General	8.2.1 General
8.2.2 Business impact analysis	8.2.2 Business impact analysis
8.2.3 Risk assessment	8.2.3 Risk assessment

Clause 8: Operation

ISO 22301:2019	
8 Operation	
8.1 Operational planning and control	Slightly modified - Add ‘supply chain’ that need to be controlled
8.2 Business impact analysis and risk assessment	
8.2.1 General	Simplified with less prescriptive
8.2.2 Business impact analysis	Modified - Enhance to include notes for ‘MTPD’ and ‘RTO’
8.2.3 Risk assessment	Simplified with less prescriptive - Include note to clarify risk in 8.2 and 6.1

Comparison ISO 22301 Version 2019 and 2012

ISO 22301:2019	ISO 22301:2012
8.3 Business continuity strategies and solutions	8.3 Business continuity strategy
8.3.1 General	
8.3.2 Identification of strategies and solutions	8.3.1 Determination and selection 8.3.3 Protection and mitigation
8.3.3 Selection of strategies and solutions	8.3.1 Determination and selection
8.3.4 Resource requirements	8.3.2 Establishing resource requirements
8.3.5 Implementation of solutions	

Clause 8: Operation

ISO 22301:2019	
8.3 Business continuity strategies and solutions	Renamed
8.3.1 General	No significant change,
8.3.2 Identification of strategies and solutions	Rewritten - Combine part of 8.3.1 and 8.3.3 of version 2012 - Remove ‘evaluation of business continuity capabilities of suppliers’
8.3.3 Selection of strategies and solutions	Rewritten - Part of 8.3.1 of version 2012 - Add ‘consider associated costs and benefits’
8.3.4 Resource requirements	Rewritten - 8.3.2 of version 2012
8.3.5 Implementation of solutions	New requirement

Clause 8: Operation

Clause 8.3.5: Implementation of solutions

The organization shall implement and maintain selected business continuity solutions so they can be activated when needed.

Comparison ISO 22301 Version 2019 and 2012

ISO 22301:2019	ISO 22301:2012
8.4 Business continuity plans and procedures	8.4 Establish and implement business continuity procedures
8.4.1 General	8.4.1 General
8.4.2 Response structure	8.4.2 Incident response structure
8.4.3 Warning and communication	8.4.3 Warning and communication
8.4.4 Business continuity plans	8.4.4 Business continuity plans
8.4.5 Recovery	8.4.5 Recovery
8.5 Exercise programme	8.5 Exercising and testing
8.6 Evaluation of business continuity documentation and capabilities	

Clause 8: Operation

ISO 22301:2019	
8.4 Business continuity plans and procedures	Renamed
8.4.1 General	No significant change
8.4.2 Response structure	Renamed & rewritten by dividing to 4 sub-clauses - Add ‘roles & responsibilities’ of working teams with dependencies - Add ‘alternate personnel’
8.4.3 Warning and communication	Divided into 2 sub-clauses - Add ‘documentation of communication procedures’
8.4.4 Business continuity plans	Divided into 3 sub-clauses
8.4.5 Recovery	No significant change
8.5 Exercise programme	Renamed - Similar to version 2012
8.6 Evaluation of business continuity documentation and capabilities	- Move content of 9.1.2 to be 8.6 and renamed - Add requirement ‘to update documentation and procedures in a timely manner’

Clause 9: Performance evaluation

Comparison ISO 22301 Version 2019 and 2012

ISO 22301:2019	ISO 22301:2012
9 Performance evaluation	9 Performance evaluation
9.1 Monitoring, measurement, analysis and evaluation	9.1 Monitoring, measurement, analysis and evaluation
	9.1.1 General
	9.1.2 Evaluation of business continuity procedures
9.2 Internal audit	9.2 Internal audit
9.2.1 General	
9.2.2 Audit programme(s)	
9.3 Management review	9.3 Management review
9.3.1 General	
9.3.2 Management review input	
9.3.3 Management review output	

Clause 9: Performance evaluation

ISO 22301:2019	
9 Performance evaluation	
9.1 Monitoring, measurement, analysis and evaluation	Simplified - Delete procedures for setting of performance metrics - Clause 9.1.2 of version 2012 moved to Clause 8.6 of version 2019
9.2 Internal audit	Divided to 2 sub-clauses - Modify by replacing 'relevant management' with 'relevant managers' in audit results reporting
9.2.1 General	
9.2.2 Audit programme(s)	
9.3 Management review	Divided to 3 sub-clauses - Management review input includes new requirements (feedback from interested parties, information from BIA and RA, lesson learned from near-misses and disruptions, output from 8.6) - Management review output includes new requirements (improve BCMS efficiency and effectiveness)
9.3.1 General	
9.3.2 Management review input	
9.3.3 Management review output	

Clause 10: Improvement

Comparison ISO 22301 Version 2019 and 2012

ISO 22301:2019	ISO 22301:2012
10 Improvement	10 Improvement
10.1 Nonconformity and corrective action	10.1 Nonconformity and corrective action
10.2 Continual improvement	10.2 Continual improvement

Clause 10: Improvement

ISO 22301:2019	
10 Improvement	
10.1 Nonconformity and corrective action	Divided to 3 sub-clauses - Similar to version 2012
10.2 Continual improvement	Modified - Specify requirement to consider result of analysis, evaluations and outputs from management review, as part of continual improvement

ISO 22301:2019 Minimum Documentation Requirements

ISO 22301:2019 Clauses	Minimum Documentation Requirements
4.2.2	Legal and regulatory requirements
4.3.1	Scope of BCMS
4.3.2	Exclusions
5.2.2	Policy
6.2.1	Business Continuity Objectives
7.2	Evidence of competence
7.5.1	Documented information required by this document as well as documented information, determined by the organization, as being necessary for the effectiveness of the BCMS
7.5.3	Documented information of external origin determined by the organization to be necessary
8.1	Information to the extent necessary to have confidence that the processes have been carried out as planned

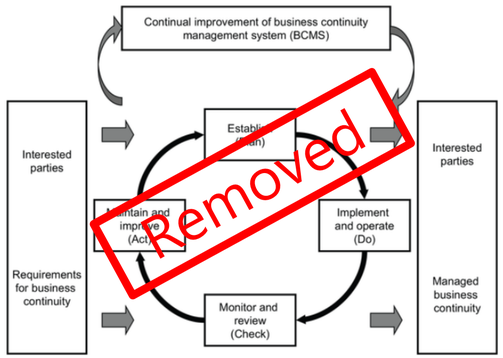
ISO 22301:2019 Clauses	Minimum Documentation Requirements
8.4.1	Business continuity plans and procedures
8.4.2	Documented procedures to guide their actions
8.4.3	Procedures for warning and communication Communications from interested parties Details of the disruption
8.4.4	Business continuity plans and procedures
8.4.5	Processes for recovery
8.5	Formalized post-exercise reports
9.1	Evidence of results
9.2.1	Audit programme(s) and audit results
9.3.3	Results of management reviews
10.1.3	Nature of the nonconformities and any subsequent actions taken Results of any corrective action

Key Changes in ISO 22301:2019

- Graph of PDCA Cycles has been removed
- Terms and Definitions clause has been modified (redefined, removed, added)
- '*Risk Appetite*' references have been removed
- Less documentation requirements
- Clause 6.3 *Planning changes to the BCMS*, new clause to ensure changes are accounted for
- Clause 8 *Operation,* simplified and reorder content

Risk Appetite: amount and type of risk that an organization is willing to pursue or retain

Removed



References

- ISO 22300:2018 Security and resilience - Vocabulary
- ISO 22301:2019 Security and resilience - Business Continuity Management Systems - Requirements
- PECB: Certified ISO 22301 Transition
- BSI: Transition to ISO 22301:2019
- BSI: Understanding the requirements of ISO 22301:2012 and ISO 22301:2019 Mapping Guide
- https://advisera.com/27001academy/blog/2019/12/02/iso-22301-2019-vs-iso-22301-2012-key-changes-infographic/

Q & A

THANK YOU

For more information, contact: **ACinfotec Consulting Services**

02-670-8980-3 | services@acinfotec.com | www.acinfotec.com


Consulting


Training


Assessment


Solutions

ACINFOTEC > DRIVING BUSINESS EXCELLENCE