

# ISO 28001:2007-10 (E)

## Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	2
4	Field of application .....	5
4.1	Statement of application .....	5
4.2	Business partners .....	5
4.3	Internationally accepted certificates or approvals .....	5
4.4	Business partners exempt from security declaration requirement .....	6
4.5	Security reviews of business partners .....	6
5	Supply chain security process .....	6
5.1	General .....	6
5.2	Identification of the scope of security assessment .....	6
5.3	Conduction of the security assessment .....	7
5.4	Development of the supply chain security plan .....	8
5.5	Execution of the supply chain security plan .....	8
5.6	Documentation and monitoring of the supply chain security process .....	8
5.7	Actions required after a security incident .....	8
5.8	Protection of the security information .....	9
Annex A (informative)	Supply chain security process .....	10
A.1	General .....	10
A.2	Identification of the scope of the security assessment .....	10
A.3	Conduction of the security assessment .....	11
A.4	Development of the security plan .....	15
A.5	Execution of the security plan .....	17
A.6	Documentation and monitoring of the security process .....	17
A.7	Continual improvement .....	17
Annex B (informative)	Methodology for security risk assessment and development of countermeasures .....	18
B.1	General .....	18
B.2	Step one - Consideration of the security threat scenarios .....	20
B.3	Step two - Classification of consequences .....	22
B.4	Step three - Classification of likelihood of security incidents .....	23
B.5	Step four - Security incident scoring .....	24
B.6	Step five - Development of countermeasures .....	24
B.7	Step six - Implementation of countermeasures .....	25
B.8	Step seven - Evaluation of countermeasures .....	25
B.9	Step eight - Repetition of the process .....	25
B.10	Continuation of the process .....	25
Annex C (informative)	Guidance for obtaining advice and certification .....	26
C.1	General .....	26
Bibliography .....		27