

DIFFÉRENCES ET MISES À JOUR 17799 :2000 – 17799 :2005

Entre la version de la norme ISO/IEC 17799 publiée en 2000 qui est l'équivalent du BS7799, et celle qui vient d'être publiée, quelques différences et mises à jours ont eu lieu.

1.1. TABLEAU DE DIFFERENCES

ISO 17799:2000	ISO 17799:2005
Contents	Contents Page
Foreword	Foreword
Introduction What Is Information Security? Why Information Security Is Needed How To Establish Security Requirements Assessing Security Risks Selecting Controls Information Security Starting Point Critical Success Fact Ors Developing Your Own Guidelines	0 Introduction 0.1 What Is Information Security? 0.2 Why Information Security Is Needed? 0.3 How To Establish Security Requirements 0.4 Assessing Security Risks 0.5 Selecting Controls 0.6 Information Security Starting Point 0.7 Critical Success Factors 0.8 Developing Your Own Guidelines
1 Scope	1 Scope
2 Terms And Definitions	2 Terms And Definitions
–	3 Structure Of This Standard 3.1 Clauses 3.2 Main Security Categories
–	4 Risk Assessment And Treatment 4.1 Assessing Security Risks 4.2 Treating Security Risks
3 Security Policy 3.1 Information Security Policy	5 Security Policy 5.1 Information Security Policy
4 Organizational Security 4.1 Information Security Infrastructure 4.2 Security Of Third Party Access 4.3 Outsourcing	6 Organization of Information Security 6.1 Internal Organization 6.2 External Parties
5 Asset Classification And Control 5.1 Accountability For Assets 5.2 Information Classification	7 Asset Management 7.1 Responsibility For Assets 7.2 Information Classification
6 Personnel Security 6.1 Security In Job Definition And Resourcing 6.2 User Training 6.3 Responding To Security Incidents And	8 Human Resources Security 8.1 Prior To Employment 8.2 During Employment 8.3 Termination Or Change Of Employment

Malfunctions	
7 Physical And Environmental Security 7.1 Secure Areas 7.2 Equipment Security 7.3 General Controls	9 Physical And Environmental Security 9.1 Secure Areas 9.2 Equipment Security
8 Communications And Operations Management 8.1 Operational Procedures And Responsibilities 8.2 System Planning And Acceptance 8.3 Protection Against Malicious Software 8.4 Housekeeping 8.5 Network Management 8.6 Media Handling And Security 8.7 Exchanges Of Information And Software	10 Communications And Operations Management 10.1 Operational Procedures And Responsibilities 10.2 Third Party Service Delivery Management 10.3 System Planning And Acceptance 10.4 Protection Against Malicious And Mobile Code 10.5 Back-Up 10.6 Network Security Management 10.7 Media Handling 10.8 Exchange Of Information 10.9 Electronic Commerce Services 10.10 Monitoring
9 Access Control 9.1 Business Requirement For Access Control 9.2 User Access Management 9.3 User Responsibilities 9.4 Network Access Control 9.5 Operating System Access Control 9.6 Application Access Control 9.7 Monitoring System Access And Use 9.8 Mobile Computing And Teleworking	11 Access Control 11.1 Business Requirement For Access Control 11.2 User Access Management 11.3 User Responsibilities 11.4 Network Access Control 11.5 Operating System Access Control 11.6 Application And Information Access Control 11.7 Mobile Computing And Teleworking
10 Systems Development And Maintenance 10.1 Security Requirements Of Systems 10.2 Security In Application Systems 10.3 Cryptographic Controls 10.4 Security Of System Files 10.5 Security In Development And Support Processes	12 Information Systems Acquisition, Development And Maintenance 12.1 Security Requirements Of Information Systems 12.2 Correct Processing In Applications 12.3 Cryptographic Controls 12.4 Security Of System Files 12.5 Security In Development And Support Processes 12.6 Technical Vulnerability Management
—	13 Information Security Incident Management 13.1 Reporting Information Security Events And Weaknesses 13.2 Management Of Information Security Incidents And Improvements

11 Business Continuity Management 11.1 Aspects Of Business Continuity Management	14 Business Continuity Management 14.1 Information Security Aspects Of Business Continuity Management
12 Compliance 12.1 Compliance With Legal Requirements 12.2 Reviews Of Security Policy And Technical Compliance 12.3 System Audit Considerations	15 Compliance 15.1 Compliance With Legal Requirements 15.2 Compliance With Security Policies And Standards, And Technical Compliance 15.3 Information Systems Audit Considerations
–	Bibliography
–	Index

1.2. ANALYSE DES DIFFERENCES

Bien que de grandes sections de la norme version 2000 aient été conservées, la norme version 2005 introduit plusieurs nouveaux éléments :

Deux domaines qui n'existaient pas dans la norme version 2000 ont été ajoutés à la norme version 2005 :

- **Risk Assessment And Treatment**
- **Information Security Incident Management**

Plusieurs domaines de la norme voient leur titre modifié au passage à la seconde édition de la norme ISO/IEC 17799 :

- **Organizational Security** devient **Organization of Information Security** : l'organisation de la sécurité se penche maintenant sur la sécurité de l'information au sens large
- **Asset Classification and Control** devient **Asset Management** : le contrôle et la classification des assets devient la gestion des assets au sens large
- **Personnel Security** devient **Human Resources Security** : la sécurité des personnes devient la sécurité des ressources humaines. La section est entièrement refondue en trois axes : avant l'embauche, pendant le travail, après ou suite à un changement de poste.
- **System Development and Maintenance** devient **Information Systems Acquisition, Development and Maintenance**, la norme prend ici aussi une orientation vers les systèmes d'information au sens large.