## Statement of Applicability

Current as of:
Sep-16

Legend (for Selected Controls and Reasons for controls selection)
**LR**: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

| ISO 27001:2005 Controls | | | Current Controls | Remarks (Justification for exclusion) | Selected Controls and Reasons for selection | | | | Remarks (Overview of implementation) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | LR | CO | BR/BP | RRA | |
| Clause | Sec | Control Objective/Control | | | | | | | |
| 5. Security Policy | 5.1 | Information Security Policy | | | | | | | |
| | 5.1.1 | Information Security Policy Document | * | Existing controls | | | * | * | highlight the importance of having secured communications while doing business online |
| | 5.1.2 | Review of Information Security Policy | * | SOC | | | * | | 1. Internal review by IT Security Office and CIO. 2. Reviews by company committees, |
| 6. Organization of Information security | 6.1 | Internal Organization | | | | | | | |
| | 6.1.1 | Management Commitment to information security | * | Existing controls | | | * | | Management should approve the information security policy, assign security roles and co-ordinate and review the implementation of security across the DELL company |
| | 6.1.2 | Information security Co-ordination | | | | | | | |
| | 6.1.3 | Allocation of information security Responsibilities | * | Existing controls | | * | * | * | heads of department are responsible for information security within their departments |
| | 6.1.4 | Authorization process for Information Processing facilities | | | | | | | |
| | 6.1.5 | Confidentiality agreements | | | | | | | |
| | 6.1.6 | Contact with authorities | * | Existing controls | * | | | | Appropriate contacts shall be maintained with local law enforcement authorities, emergency support staff and service providers. |
| | 6.1.7 | Contact with special interest groups | | | | | | | |
| | 6.1.8 | Independent review of information security | | | | | | | |
| | 6.2 | External Parties | | | | | | | |
| | 6.2.1 | Identification of risk related to external parties | | | | | | | |
| | 6.2.2 | Addressing security when dealing with customers | | | | | | | |
| | 6.2.3 | Addressing security in third party agreements | * | 'Existing controls | | * | * | * | Agreements with third parties involving accessing, processing, communicating or managing the DELL company information, or information systems, should cover all relevant security requirements, and be covered in contractual arrangements |
| 7. Asset Management | 7.1 | Responsibility for Assets | | | | | | | |
| | 7.1.1 | Inventory of assets | * | Existing controls | * | | * | | Risk Assessment Report And Asset Register |
| | 7.1.2 | Ownership of Assets | | | | | | | |
| | 7.1.3 | Acceptable use of assets | | | | | | | |
| | 7.2 | Information classification | | | | | | | |
| | 7.2.1 | Classification Guidelines | * | Existing controls | | | * | | 1.Information and information system security classification 2. Mandatory |
| | 7.2.2 | Information Labeling and Handling | * | Unnecessary Process | | | | | |

## Statement of Applicability

Current as of:
Sep-16

Legend (for Selected Controls and Reasons for controls selection)
**LR**: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

| ISO 27001:2005 Controls | | | Current Controls | Remarks (Justification for exclusion) | Selected Controls and Reasons for selection | | | | Remarks (Overview of implementation) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | LR | CO | BR/BP | RRA | |
| Clause | Sec | Control Objective/Control | | | | | | | |
| | | | | | | | | | |
| 8. Human Resource Security | 8.1 | Prior to Employment | | | | | | | |
| | 8.1.1 | Roles and Responsibilities | | | | | | | |
| | 8.1.2 | Screening | * | Existing controls | | * | * | | have formal interviews |
| | 8.1.3 | Terms and conditions of employment | | | | | | | |
| | 8.2 | During Employment | | | | | | | |
| | 8.2.1 | Management Responsibility | * | Existing controls | * | | * | | development of policies is the responsibility of the Chief Information Security Officer.   DELL senior management and executive Director of risk management and safty service provide |
| | 8.2.2 | Information security awareness, education and training | * | Existing controls | * | * | * | | Managers must provide ongoing information security |
| | 8.2.3 | Disciplinary process | | | | | | | |
| | 8.3 | Termination or change of employment | | | | | | | |
| | 8.3.1 | Termination responsibility | * | Existing controls | * | | * | | according to he document of return on Assets and procedure |
| | 8.3.2 | Return of assets | | | | | | | |
| | 8.3.3 | Removal of access rights | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| 9. Physical and Environmental Security | 9.1 | Secure Areas | | | | | | | |
| | 9.1.1 | Physical security Perimeter | ■ | Existing controls | | ■ | | | |
| | 9.1.2 | Physical entry controls | ■ | Existing controls | | ■ | | ■ | Implement swipe card on all data centers and established visitor control logs |
| | 9.1.3 | Securing offices, rooms and facilities | ■ | Existing controls | | | | ■ | |
| | 9.1.4 | Protecting against external and environmental threats | ■ | Existing controls | | | | | |
| | 9.1.5 | Working in secure areas | ■ | Existing controls | | | | | Policy created |
| | 9.1.6 | Public access, delivery and loading areas | ■ | Existing controls | | | | | |
| | 9.2 | Equipment security | | | | | | | |
| | 9.2.1 | Equipment sitting and protection | ■ | Existing controls | | ■ | | ■ | |
| | 9.2.2 | Support utilities | ■ | Existing controls | | | | ■ | |
| | 9.2.3 | Cabling security | ■ | Existing controls | | ■ | | | |
| | 9.2.4 | Equipment Maintenance | ■ | Existing controls | | ■ | | ■ | Formalized PM mechanism |
| | 9.2.5 | Security of equipment off-premises | ■ | Existing controls | | | | | |
| | 9.2.6 | Secure disposal or reuse of equipment | | | | | | | Implemented procedure |
| | 9.2.7 | Removal of Property | ■ | Existing controls.  Use of gate pass. | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | 10.1 | Operational Procedures and responsibilities | | | | | | | |

# Statement of Applicability

Current as of:
Sep-16

Legend (for Selected Controls and Reasons for controls selection)
**LR**: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

| ISO 27001:2005 Controls | | | Current Controls | Remarks (Justification for exclusion) | Selected Controls and Reasons for selection | | | | Remarks (Overview of implementation) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | LR | CO | BR/BP | RRA | |
| **Clause** | **Sec** | **Control Objective/Control** | | | | | | | |
| 10. Communications and Operations Management | 10.1.1 | Documented operating Procedures | * | Existing controls | | | | | Information Custodians must ensure that approved operating procedures and standards are:<br>□ Documented;<br>□ Consistent with government policies;<br>□ Reviewed and updated annually; |
| | 10.1.2 | Change Management | | | | | | | |
| | 10.1.3 | Segregation of Duties | | | | | | | |
| | 10.1.4 | Separation of development and Operations facilities | | | | | | | |
| | 10.2 | Third Party Service Delivery Management | | | | | | | |
| | 10.2.1 | Service Delivery | | | | | | | |
| | 10.2.2 | Monitoring and review of third party services | | | | | | | |
| | 10.2.3 | Manage changes to the third party services | | | | | | | |
| | 10.3 | System Planning and Acceptance | | | | | | | |
| | 10.3.1 | Capacity management | yes | | | | * | * | Resource capacity management - for implementing capacity management processes by:<br>□ Documenting capacity requirements and capacity planning processes, |
| | 10.3.2 | System acceptance | | | | | | | |
| | 10.4 | Protection against Malicious and Mobile Code | | | | | | | |
| | 10.4.1 | Controls against malicious code | * | Existing controls | | | | * | The Chief Information Security Officer must ensure processes are implemented to:<br>□ Maintain a critical incident management plan to identify and respond to malicious code incidents |
| | 10.4.2 | Controls against Mobile code | | | | | | | |
| | 10.5 | Back-Up | | | | | | | |
| | 10.5.1 | Information Backup | * | Existing controls | | | | * | Safeguarding backup facilities and media -<br>□ Using encryption to protect the backed up information;<br>□ Using digital signatures to protect the integrity of the information;<br>□ Physical and environmental security;<br>□ Access controls; |
| | 10.6 | Network Security Management | | | | | | | |
| | 10.6.1 | Network controls | | | | | | | |
| | 10.6.2 | Security of Network services | | | | | | | |
| | 10.7 | Media Handling | | | | | | | |
| | 10.7.1 | Management of removable media | | | | | | | |
| | 10.7.2 | Disposal of Media | | | | | | | |
| | 10.7.3 | Information handling procedures | | | | | | | |
| | 10.7.4 | Security of system documentation | * | Existing controls | * | | * | * | □ Establish lists of users authorized to access system documentation |

## Statement of Applicability

Current as of:
Sep-16

Legend (for Selected Controls and Reasons for controls selection)
**LR**: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

| ISO 27001:2005 Controls | | | Current Controls | Remarks (Justification for exclusion) | Selected Controls and Reasons for selection | | | | Remarks (Overview of implementation) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | LR | CO | BR/BP | RRA | |
| Clause | Sec | Control Objective/Control | | | | | | | |
| | 10.8 | Exchange of Information | | | | | | | |
| | 10.8.1 | Information exchange policies and procedures | * | Existing controls | | | | * | The Chief Information Security Officer of DELL must document and implement procedures to protect information from interception, copying, misrouting and destruction when being transmitted electronically or verbally. |
| | 10.8.2 | Exchange agreements | | | | | | | |
| | 10.8.3 | Physical media in transit | | | | | | | |
| | 10.8.4 | Electronic Messaging | | | | | | | |
| | 10.8.5 | Business Information systems | * | Existing controls | | | * | * | Implement procedures to restrict access to information in interconnected internal administrative and productivity information systems that support government such as e-mail, calendars and financial systems. |
| | 10.9 | Electronic Commerce Services | | | | | | | |
| | 10.9.1 | Electronic Commerce | | | | | | | |
| | 10.9.2 | On-Line transactions | * | Existing controls | * | | * | * | transaction management are responsible for ensuring that information systems used for processing payment card transactions or connected to payment card transaction processing systems comply with the Payment Card Industry Data Security Standard. |
| | 10.9.3 | Publicly available information | | | | | | | |
| | 10.10 | Monitoring | | | | | | | |
| | 10.10.1 | Audit logging | | | | | | | |
| | 10.10.2 | Monitoring system use | * | Existing controls | * | | * | * | Process management ensure that the use of information systems can be monitored to detect activities including: authorized and unauthorized accesses, system alerts and failures System Admin must implement, manage and monitor logging systems for: |
| | 10.10.3 | Protection of log information | | | | | | | |
| | 10.10.4 | Administrator and operator logs | | | | | | | |
| | 10.10.5 | Fault logging | * | | | | * | | Authentication administrator must Reporting and logging faults and Analysis, resolution and corrective action. |
| | 10.10.6 | Clock synchronization | | | | | | | |
| | | | | | | | | | |
| | 11.1 | Business Requirement for Access Control | | | | | | | |
| | 11.1.1 | Access control Policy | | | | | | | |
| | 11.2 | User Access Management | | | | | | | |
| | 11.2.1 | User Registration | | | | | | | |

## Statement of Applicability

Current as of:
Sep-16

Legend (for Selected Controls and Reasons for controls selection)
**LR**: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

| ISO 27001:2005 Controls | | | Current Controls | Remarks (Justification for exclusion) | Selected Controls and Reasons for selection | | | | Remarks (Overview of implementation) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | LR | CO | BR/BP | RRA | |
| **Clause** | **Sec** | **Control Objective/Control** | | | | | | | |
| 11. Access control | 11.2.2 | Privilege Measurement | | | | | | | |
| | 11.2.3 | User password management | | | | | | | |
| | 11.2.4 | Review of user access rights | | | | | | | |
| | 11.3 | User Responsibilities | | | | | | | |
| | 11.3.1 | Password Use | | | | | | | |
| | 11.3.2 | Unattended user equipment | | | | | | | |
| | 11.3.3 | Clear Desk and Clear Screen Policy | | | | | | | |
| | 11.4 | Network Access control | | | | | | | |
| | 11.4.1 | Policy on use of network services | | | | | | | |
| | 11.4.2 | User authentication for external connections | | | | | | | |
| | 11.4.3 | Equipment identification in networks | | | | | | | |
| | 11.4.4 | Remote diagnostic and configuration port protection | | | | | | | |
| | 11.4.5 | Segregation in networks | | | | | | | |
| | 11.4.6 | Network connection control | | | | | | | |
| | 11.4.7 | Network Routing control | | | | | | | |
| | 11.5 | Operating System Access Control | | | | | | | |
| | 11.5.1 | Secure Log-on procedures | | | | | | | |
| | 11.5.2 | User identification and authentication | | | | | | | |
| | 11.5.3 | Password Management system | | | | | | | |
| | 11.5.4 | Use of system utilities | | | | | | | |
| | 11.5.5 | Session Time-out | | | | | | | |
| | 11.5.6 | Limitation of connection time | | | | | | | |
| | 11.6 | Application access control | | | | | | | |
| | 11.6.1 | Information access restriction | | | | | | | |
| | 11.6.2 | Sensitive system isolation | | | | | | | |
| | 11.7 | Mobile Computing and Teleworking | | | | | | | |
| | 11.7.1 | Mobile computing and communication | | | | | | | |
| | 11.7.2 | Teleworking | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| 12. Information Systems Acquisition Development and | 12.1 | Security Requirements of Information Systems | | | | | | | |
| | 12.1.1 | Security requirement analysis and specifications | | | | | | | |
| | 12.2 | Correct Processing in Applications | | | | | | | |
| | 12.2.1 | Input data validation | | | | | | | |
| | 12.2.2 | Control of internal processing | | | | | | | |
| | 12.2.3 | Message integrity | | | | | | | |
| | 12.2.4 | Output data validation | | | | | | | |
| | 12.3 | Cryptographic controls | | | | | | | |
| | 12.3.1 | Policy on the use of cryptographic controls | | | | | | | |
| | 12.3.2 | Key Management | | | | | | | |
| | 12.4 | Security of System Files | | | | | | | |
| | 12.4.1 | Control of Operational software | | | | | | | |
| | 12.4.2 | Protection of system test data | | | | | | | |

**Statement of Applicability**

Current as of:
Sep-16

Legend (for Selected Controls and Reasons for controls selection)
**LR**: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

| ISO 27001:2005 Controls | | | Current Controls | Remarks (Justification for exclusion) | Selected Controls and Reasons for selection | | | | Remarks (Overview of implementation) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | LR | CO | BR/BP | RRA | |
| Clause | Sec | Control Objective/Control | | | | | | | |
| Development and Maintenance | 12.4.3 | Access control to program source library | | | | | | | |
| | 12.5 | Security in Development & Support Processes | | | | | | | |
| | 12.5.1 | Change Control Procedures | | | | | | | |
| | 12.5.2 | Technical review of applications after Operating system changes | | | | | | | |
| | 12.5.3 | Restrictions on changes to software packages | | | | | | | |
| | 12.5.4 | Information Leakage | | | | | | | |
| | 12.5.5 | Outsourced Software Development | | | | | | | |
| | 12.6 | Technical Vulnerability Management | | | | | | | |
| | 12.6.1 | Control of technical vulnerabilities | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| 13. Information Security Incident Management | 13.1 | Reporting Information Security Events and Weaknesses | | | | | | | |
| | 13.1.1 | Reporting Information security events | | | | | | | |
| | 13.1.2 | Reporting security weaknesses | | | | | | | |
| | 13.2 | Management of Information Security Incidents and Improvements | | | | | | | |
| | 13.2.1 | Responsibilities and Procedures | | | | | | | |
| | 13.2.2 | Learning for Information security incidents | | | | | | | |
| | 13.2.3 | Collection of evidence | | | | | | | |
| | | | | | | | | | |
| 14. Business Continuity Management | 14.1 | Information Security Aspects of Business Continuity Management | | | | | | | |
| | 14.1.1 | Including Information Security in Business continuity management process | | | | | | | |
| | 14.1.2 | Business continuity and Risk Assessment | | | | | | | |
| | 14.1.3 | developing and implementing continuity plans including information security | | | | | | | |
| | 14.1.4 | Business continuity planning framework | | | | | | | |
| | 14.1.5 | Testing, maintaining and re-assessing business continuity plans | | | | | | | |
| | | | | | | | | | |
| 15. Compliance | 15.1 | Compliance with Legal Requirements | | | | | | | |
| | 15.1.1 | Identification of applicable legislations | | | | | | | |
| | 15.1.2 | Intellectual Property Rights ( IPR) | | | | | | | |
| | 15.1.3 | Protection of organizational records | | | | | | | |
| | 15.1.4 | Data Protection and privacy of personal information | | | | | | | |
| | 15.1.5 | Prevention of misuse of information processing facilities | | | | | | | |
| | 15.1.6 | Regulation of cryptographic controls | | | | | | | |
| | 15.2 | Compliance with Security Policies and Standards and Technical compliance | | | | | | | |

# Statement of Applicability

Current as of:
Sep-16

Legend (for Selected Controls and Reasons for controls selection)
**LR**: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

| ISO 27001:2005 Controls | | | Current Controls | Remarks (Justification for exclusion) | Selected Controls and Reasons for selection | | | | Remarks (Overview of implementation) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | LR | CO | BR/BP | RRA | |
| **Clause** | **Sec** | **Control Objective/Control** | | | | | | | |
| | 15.2.1 | Compliance with security policy | | | | | | | |
| | 15.2.2 | Technical compliance checking | | | | | | | |
| | 15.3 | Information System Audit Considerations | | | | | | | |
| | 15.3.1 | Information System Audit controls | | | | | | | |
| | 15.3.2 | Protection of information system audit tools | | | | | | | |
| | | | | | | | | | |