

# ISO/IEC 21878:2018 (E)

## Information technology — Security techniques — Security guidelines for design and implementation of virtualized servers

---

### Contents

|         |   |
|---------|---|
|         | Foreword  |
|         | Introduction  |
| 1       | Scope   |
| 2       | Normative references                                |
| 3       | Terms and definitions                               |
| 4       | Symbols and abbreviated terms                       |
| 5       | Overview of server virtualization                   |
| 5.1     | Types of server virtualization                      |
| 5.2     | Components of a VS                                  |
| 5.3     | Technical considerations                            |
| 5.3.1   | General   |
| 5.3.2   | Exclusions  |
| 5.3.2.1 | Vendor attestation                                  |
| 5.3.2.2 | Operating environment                               |
| 6       | Overview of security threats and risks              |
| 6.1     | General   |
| 6.2     | Common threats                                      |
| 6.3     | VS-specific risks                                   |
| 6.3.1   | General   |
| 6.3.2   | VM risks  |
| 6.3.3   | Hypervisor risks                                    |
| 6.3.4   | Operational risks related to implementation         |
| 6.3.5   | Cloud Services risks                                |
| 7       | Recommendations for secure VS lifecycle             |
| 7.1     | General   |
| 7.2     | Initial preparation phase                           |
| 7.3     | Planning and design phase                           |
| 7.4     | Implementation phase                                |
| 7.5     | Disposition phase                                   |
| 8       | Planning and design phase: security considerations  |
| 8.1     | General   |
| 8.2     | Security considerations and satisfying requirements |
| 9       | Implementation phase: security checklist            |
| 9.1     | General   |
| 9.2     | Security checklist and vulnerability exposure       |
| Annex A | (informative) Risk assessment for VSs               |
| A.1     | General   |
| A.2     | Risk assessment matrix                              |
| A.3     | Likelihood rating                                   |
| A.4     | Impact rating                                       |
| A.5     | Risk matrix   |

**Annex B (informative) Guidelines for implementing security checklist items in Table 2**

- B.1** Have the policies and controls which prevent uncontrolled proliferation of VMs been implemented?
- B.2** Are the sensitive data within the VM being protected?
- B.3** Are the security measures implemented for offline and dormant VMs?
- B.4** Are the security measures implemented for pre-configured (Golden Image) VM and active VMs?
- B.5** Is the visibility over traffic and controls in virtual networks ensured?
- B.6** Are controls and policies to prevent resource exhaustion implemented?
- B.7** Are measures taken to ensure the security of the hypervisor?
- B.8** Are the measures to prevent unauthorized access to the hypervisor implemented?
- B.9** Are the controls and policies to prevent account or service hijacking implemented?
- B.10** Are security measures for proper and secure segregation of workload on physical hosts implemented?
- B.11** Are measures taken to ensure the security of the cloud service provider API?
- B.12** Are there automated processes in place to monitor patch releases and apply them to hypervisor software and Guest OS software modules?

Page count: 22