

---

---

**Information technology – Network  
security —**

**Part 7:  
Guidelines for network virtualization  
security**

*Technologies de l'information — Sécurité des réseaux —*

*Partie 7: Lignes directrices pour la sécurité de la virtualisation des  
réseaux*

**Document Preview**

[ISO/IEC 27033-7:2023](https://standards.iteh.ai/catalog/standards/sist/75435c1a-2159-4810-b1bf-8c231d1a4951/iso-iec-27033-7-2023)

<https://standards.iteh.ai/catalog/standards/sist/75435c1a-2159-4810-b1bf-8c231d1a4951/iso-iec-27033-7-2023>



iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

[ISO/IEC 27033-7:2023](https://standards.iteh.ai/catalog/standards/sist/75435c1a-2159-4810-b1bf-8c231d1a4951/iso-iec-27033-7-2023)

<https://standards.iteh.ai/catalog/standards/sist/75435c1a-2159-4810-b1bf-8c231d1a4951/iso-iec-27033-7-2023>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

Foreword.....	iv
Introduction.....	v
<b>1 Scope.....</b>	<b>1</b>
<b>2 Normative references.....</b>	<b>1</b>
<b>3 Terms and definitions.....</b>	<b>1</b>
<b>4 Abbreviated terms.....</b>	<b>2</b>
<b>5 Overview.....</b>	<b>4</b>
5.1 General.....	4
5.2 Description of network virtualization.....	4
5.3 Security model.....	4
5.3.1 Model of network virtualization security.....	4
5.3.2 Network virtualization components.....	6
<b>6 Security threats.....</b>	<b>6</b>
<b>7 Security recommendations.....</b>	<b>7</b>
7.1 General.....	7
7.2 Confidentiality.....	7
7.3 Integrity.....	8
7.4 Availability.....	8
7.5 Authentication.....	8
7.6 Access control.....	8
7.7 Non-repudiation.....	9
<b>8 Security controls.....</b>	<b>9</b>
8.1 General.....	9
8.2 Virtual network infrastructure security.....	10
8.3 Virtual network function security.....	10
8.4 Virtual network management security.....	11
8.4.1 SDN controller security.....	11
8.4.2 NFV orchestrator security.....	12
<b>9 Design techniques and considerations.....</b>	<b>12</b>
9.1 Overview.....	12
9.2 Integrity protection of platform.....	13
9.3 Hardening for network virtualization.....	13
9.4 API authentication and authorization.....	13
9.5 Software defined security for virtual network.....	13
<b>Annex A (informative) Use cases of network virtualization.....</b>	<b>15</b>
<b>Annex B (informative) Detailed security threat description of network virtualization.....</b>	<b>18</b>
<b>Bibliography.....</b>	<b>22</b>

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at [www.iso.org/patents](http://www.iso.org/patents) and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*. <https://standards.iteh.ai> | <https://standards.iteh.ai/document/iso-iec-27033-7-2023>

A list of all parts in the ISO/IEC 27033 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at [www.iso.org/members.html](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

## Introduction

The purpose of this document is to address the key challenges and risks of network virtualization security. Network virtualization includes virtual network infrastructure, virtual network function, virtual control and resource management. This document aims to:

- 1) identify security risks of network virtualization;
- 2) propose a network virtualization security model;
- 3) propose security guidelines for virtual network infrastructure, virtual network function, virtual control and resource management.

This document intends to help stakeholders in understanding the main characteristics of network virtualization security. For example, this document can help software and hardware suppliers to securely design and develop products that implement network virtualization, and help operators to evaluate the security of these products and deploy them securely for network services. By proposing security guidelines, this document aims to help the industry to improve system security that is built on network virtualization technology.

The target audience can include the network equipment vendors, network operators, internet service providers and software service providers.

With the rapid development of IT technologies such as cloud computing, IT systems and communication systems are increasingly evolving with the adoption of virtualization technology. Virtualization enables systems to have high agility, flexibility and scalability with low cost, but at the same time, introduces many security challenges.

(<https://standards.iteh.ai>)  
Document Preview

<https://standards.iteh.ai>  
ISO/IEC 27033-7:2023

<https://standards.iteh.ai/catalog/standards/sist/75435c1a-2159-4810-b1bf-8c231d1a4951/iso-iec-27033-7-2023>



# Information technology – Network security —

## Part 7: Guidelines for network virtualization security

### 1 Scope

This document aims to identify security risks of network virtualization and proposes guidelines for the implementation of network virtualization security.

Overall, this document intends to considerably aid the comprehensive definition and implementation of security for any organization's virtualization environments. It is aimed at users and implementers who are responsible for the implementation and maintenance of the technical controls required to provide secure virtualization environments.

### 2 Normative references

There are no normative references in this document.

### 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at <https://www.iso.org/obp>

— IEC Electropedia: available at <https://www.electropedia.org/>

#### 3.1

##### **network virtualization**

technology that enables the creation of logically isolated network partitions over shared physical network infrastructures so that multiple heterogeneous virtual networks can simultaneously coexist over the shared infrastructures

Note 1 to entry: Network virtualization allows the aggregation of multiple resources and makes the aggregated resources appear as a single resource.

[SOURCE: ISO/IEC TR 29181-1:2012, 3.3]

#### 3.2

##### **network functions virtualization**

##### **NFV**

technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of multiple virtual networks can simultaneously coexist over the shared networks

Note 1 to entry: This includes the aggregation of multiple resources in a provider and appearing as a single resource.

[SOURCE: ISO/IEC TR 22417:2017, 3.8]

### 3.3 software-defined networking

set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner

[SOURCE: ITU-T Y.3300:2014, 3.2.1]

### 3.4 virtual machine

virtual data processing system that appears to be at the disposal of a particular user, but whose functions are accomplished by sharing the resources of a real data processing system

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.4564]

### 3.5 container

isolated execution environment for running software that uses a virtualized operating system kernel

[SOURCE: ISO/IEC 22123-1:2023, 3.12.4]

### 3.6 orchestrator

tool that enables DevOps personas or automation working on their behalf to pull images from registries, deploy those images into *containers* (3.5), and manage the running containers

[SOURCE: NIST SP 800-190]

### 3.7 service function chain

ordered set of abstract functions and ordering constraints that are applied to packets and/or frames and/or flows selected as a result of classification

[SOURCE: IETF RFC 7665, modified — removed “a service function chain defines an” at the beginning of the definition and replaced “must” with “are” in the definition.]

<https://standards.iteh.ai/catalog/standards/sist/75435c1a-2159-4810-b1bf-8c231d1a4951/iso-iec-27033-7-2023>

## 4 Abbreviated terms

The following abbreviated terms apply to this document.

5G	the fifth generation mobile network
AMF	access and mobility management function
API	application programming interface
AUSF	authentication server function
CDN	content delivery network
CIS	centre for internet security
DoS	denial of service
DDoS	distributed denial of service
HMAC	hash-based message authentication code
IDS	intrusion detection system



IPS	intrusion prevention system
MANO	management and orchestration
MFA	multi-factor authentication
NF	network function
NFV	network functions virtualization
NFVO	network function virtualization orchestrator
NRF	network repository function
NSSF	network slice selection function
OAM	operation and management
OMC	operation maintenance centre
OS	operating system
SD-WAN	software-defined wide-area network
SDN	software-defined networking
SFC	service function chain
SMF	session management function
UDM	unified data management
UPF	user plane function
vCPU	virtual CPU
VIM	virtualised infrastructure manager
vI/O	virtual I/O
VNF	virtualised network function
VNFM	virtualised network function manager
VM	virtual machine
vMemory	virtual memory
VMM	virtual machine manager
vRouter	virtual router
vSwitch	virtual switch
vWAF	virtual web application firewall
VxLAN	virtual extensible local area network
WAF	web application firewall

## 5 Overview

### 5.1 General

Network virtualization provides a novel solution for the development and deployment of IT systems and communication networks. It greatly reduces the cost of system maintenance, improves the utilization of resources (such as computing, storage and networking) and the flexibility of IT systems or networks. Cloud computing, the dominant platform for new IT systems and networks makes extensive use of network virtualization technology. ISO/IEC 22123-1 and ISO/IEC 22123-2 provide an overview of cloud computing and its concepts. ISO/IEC 22123-3 provides reference architecture for cloud computing. The typical use cases of network virtualization include but are not limited to software-defined wide-area network (SD-WAN), network slice, Virtual WAF and cloud CDN with centralized control, which are referred to in [Annex A](#).

With the adoption of network virtualization, new security challenges to IT and communication systems are introduced. Hence, traditional security protection solutions, which are often static, passive and isolated, would not be effective for virtualized systems. New security solutions, which are dynamic, proactive, coordinated and have intelligent management capability, are needed.

### 5.2 Description of network virtualization

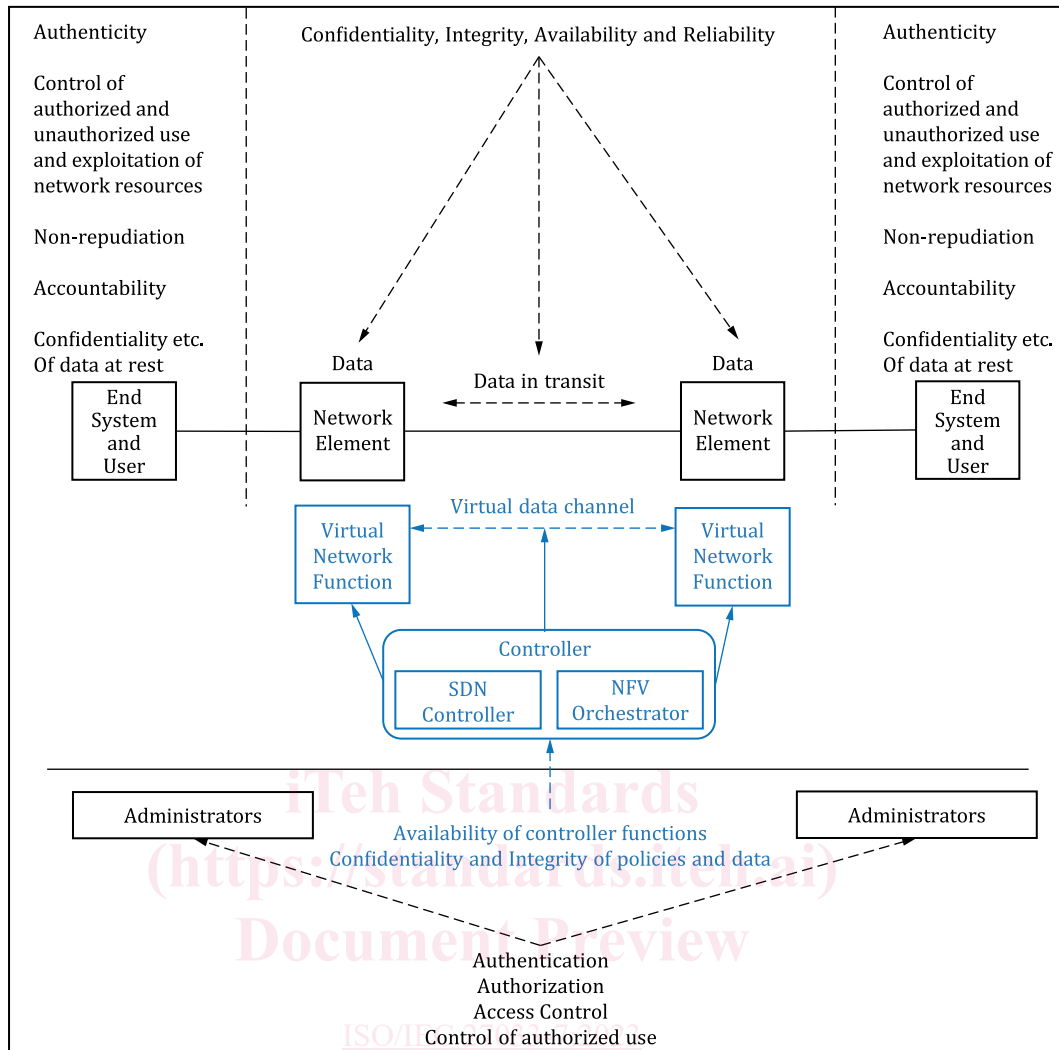
Network virtualization abstracts physical resources, such as computing, networking, memory and storage into standard and general-purpose entities. Each entity can be deployed with service functions under the control of an orchestrator. Through virtualization, the limitation of physical resources are broken, thus, the utilization of these resources are improved. The new virtual entities of these resources are no longer limited by the way their physical counterparts are deployed.

In this document, network virtualization includes virtual network function and virtual network connection. Virtual network function runs on virtual infrastructure (such as virtual computing, virtual storage and virtual networking) using virtualization technologies (such as virtual machines and containers). NFV is a common method to implement virtual network function. Virtual network connection is applied to connect functional units on demand. The resulting network called SDN is composed of virtual data links. An important characteristic of SDN is that all underlying resources can be centrally managed and provide a standard interface that support software programming based on the customer's requirements. The introduction of SDN and NFV solutions changes the network significantly: general-purpose hardware, virtual software function, programmable network connections and services. With SDN and NFV, the cost of network operation and maintenance is cut down, the utilization of resources (such as computing, storage and networking) is improved, the flexibility of the network and service logic is increased, and the time-to-market of new services is considerably decreased.

### 5.3 Security model

#### 5.3.1 Model of network virtualization security

ISO/IEC 27033-1 provides a conceptual model of network security for network security risk and management review. In general, network security includes three areas: security of the element, security of network connection and security of management. In network virtualization, the element is a virtual network function and the network connection is a virtual connection. This document further enhances this model according to the technical characteristic of network virtualization, as shown in [Figure 1](#).



**Figure 1 — A conceptual model of network virtualization security risk areas**

These changes brought about by network virtualization include:

- a) Centralized controllers are included. The NFV orchestrator is responsible for the allocation, scheduling and life cycle management of infrastructure and resources. The SDN controller is in charge of the management of network topology and virtual data links. The NFV orchestrator and SDN controller provide standard northbound API to support the scheduling of computing, network and storage resources in the system in a software programmable manner, and also provide collaborative, dynamic and optimized scheduling of network resources and services.
- b) Network elements are now virtual elements (as opposed to physical elements) whose behaviour is directed by the controller (NFV orchestrator). Network elements can be deployed or destroyed on demand as software, with service logic and functionality programmed to run on virtualized infrastructure (such as virtual machines and containers). ISO/IEC 21878 provides guidelines for design and implementation of virtualized servers.
- c) Data link has changed. Besides the physical data links, the adoption of new technologies such as SDN and SFC provides efficient virtualized data links according to applications' needs. New technologies can also improve the efficiency of data transmission inside the system and meet the transmission resiliency needs of cloud computing (such as load balancing and high reliability).