SUSE Linux Enterprise Server 12 – Product Requirement Document (PRD)

Zero Outage Industry Standard

Version	1.00
Date	09.03.2018
Status	Released

Important:
This PRD is elaborated by members of the Zero Outage Industry Standard association as a proof-of-concept and not a publication of SUSE. It should be understood as a demonstration example not providing any binding statement about SUSE and its product. Refer to chapter 4 for more detail.

Imprint

Publisher

Zero Outage Industry Standard Ltd.
20-22 Bedford Row
London, WC1R 4JS

Version	Date	Status
1.00	09.03.2018	Released

Contact	Phone / Fax	E-Mail
www.zero-outage.com		

Change History

Version	Stand	Editor	Changes / Commentary
0.1	10.11.2017	Ralph Roth, Walter Sedlacek	First draft (based on Version 1.00 of the Template)
0.2	30.10.2017	Ralph Roth	Initial version sent out for review.
0.90	01.03.2018	Dr. Eberhard von Faber	Final Draft
1.00	09.03.2018	Dr. Eberhard von Faber	Prepared for web publishing

Table of Contents

List of Figures

List of Tables

1 Preface

Nowadays, IT services are the outcome of complex value chains or supply networks which consist of multiple corporations each delivering a specific contribution to the IT service finally consumed by a user organization and end users. Hence, IT services are composed of different technical components from different sources. Moreover, different corporations are involved to build, operate and maintain these components and composite IT systems built using these components.

IT services need to be secure. Each technical component may contain vulnerabilities and each activity relating to the development, production, operation or maintenance of technical components may cause vulnerabilities which could be exploited by adversaries. It is hence required that all participants in the supplier network cooperate in order to provide a secure integrated whole. Transparency about security objectives and meeting them is the basis for this.

A so-called Product Requirement Document (PRD) provides the security specification which needs to be agreed between the supplying party and the consuming party. The role and use of the PRD and the procedures for managing security in a supplier network are summarized in another paper published by the Zero Outage Industry Standard association. Refer to [6].[1] The idea is shown in Figure 1. In the example, the final composite IT service has 16 security aspects. Three of them are covered by the product or IT services from the supplying party. The consuming party learns from the PRD which security aspects or measures are provided (black) and which require additional consideration (blue) in order to make the final composite IT service a secure one.

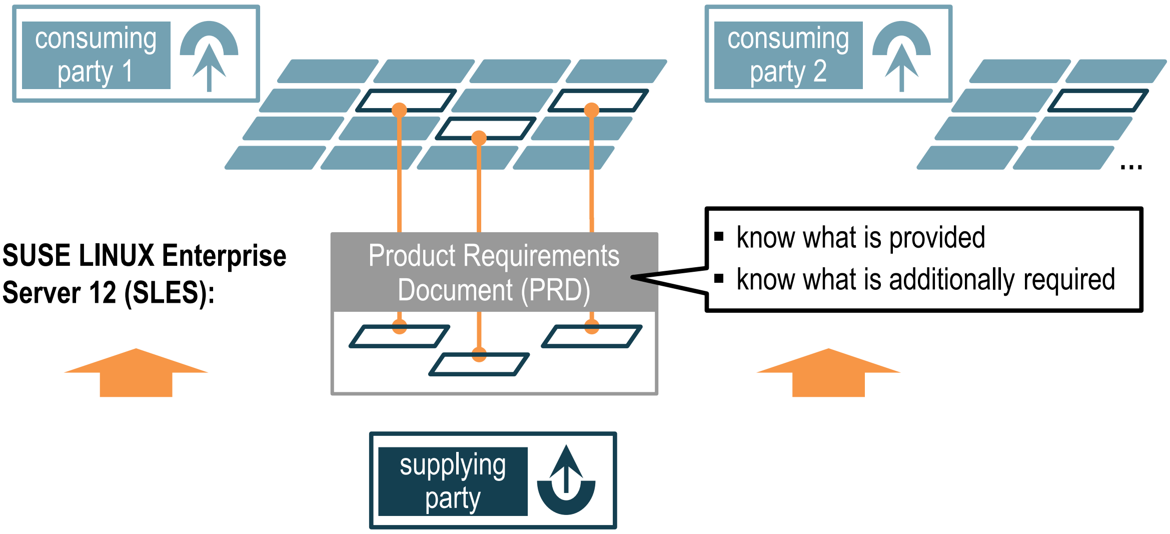
consuming party 1
consuming party 2
...
SUSE LINUX Enterprise Server 12 (SLES):
Product Requirements Document (PRD)
▪ know what is provided
▪ know what is additionally required
supplying party

Figure 1: Function of the Product Requirements Document (PRD)

A PRD is a means to exchange security relevant information between supplying and consuming parties in a little formalized way fostering its reuse.

[1] Managing security in the supplier network – Third Party Integration Model; Zero Outage Industry Standard, Release 2 about Security, August 2017, zero-outage.com/security

2 Specification of the IT service

2.1 Overview

This document (PRD) is produced to provide a detailed requirement and or specification for the

SUSE LINUX Enterprise Server 12 Operating System

also referred to as “SLES” and “IT service” in the following. The PRD defines business, non-functional and technical requirements with respect to security. This Section 2.1 provides an overview only, details are provided in Section 2.2.

The “specification of the IT service” comprises a description of the IT service (functions, components, value, usage, activities in ITSM – IT Service Management etc.) and the context in which it is intended to be used (context information, environment).

SUSE Linux Enterprise Server (SLES) is a world-class, secure open source server operating system, built to power physical, virtual and cloud-based mission-critical workloads. The operating system further raises the bar in helping organizations to accelerate innovation, enhance system reliability, meet tough security requirements and adapt to new technologies. SUSE Linux Enterprise Server provides the infrastructure foundation that enables organizations to deploy latest container innovations, adapt to new hardware architectures, maximize service up-time, increase virtualization, and implement enterprise-ready solutions out-of-the-box with proven security and optimized performance.

2.2 Detailed specification of the IT service

SUSE Linux Enterprise Server 12 is a world-class, secure open source server operating system, built to power physical, virtual and cloud-based mission-critical workloads. SUSE Linux Enterprise Server 12 is a modular, general-purpose operating system and runs on all major processor architectures.

SUSE LINUX Enterprise Server 12 Operating System (SLES)

- SLES comprises software of an operating system including software tools supporting the installation, configuration and management of the operating system.
  - Software components may originate from multiple sources (developers) but are provided by SUSE.
  - SUSE takes responsibility for SLES comprising multiple software components including optional ones.
- SLES supports traditional, single-instance installations and virtualization environments as well.
  - SLES can be used in form of a traditional installation and in virtualized environments as an image as well.
  - SLES comprises the latest open source virtualization technologies, Xen and KVM. With these hypervisors, multiple virtual machines (VMs) can be provisioned, de-provisioned, installed, monitored and managed on a single physical system.
- SLES comes as a service.

  - If available, updates (patches) are provided and distributed for SLES including all software components it consists of.
  - SLES includes a vulnerability notification service, also known as the provisioning of CERT advisories, i.e. users are informed about software errors, their consequences and recommended solutions (patches), mitigation and/or workarounds.
  - SUSE Customer Center (SCC) is a portal to centrally manage the user's SUSE subscriptions, access software updates and contact SUSE Customer Support. Using the Subscription Management Tool (SMT) large user organizations centrally receive patches and updates for their SUSE Linux Enterprise software.

SUSE Linux Enterprise Server 12 is installed, operated and maintained by the consuming party. This means that the following activities are not part of SLES:

- Development of final profile and selection and configuration of the final installation of SLES (though SUSE provides guidance and tools to perform these tasks).
- Hardening and creation of images (though SUSE provides guidance and tools to perform these tasks).
- Provisioning including installation and final configuration (though SUSE provides guidance and tools to perform these tasks).
- Operations and maintenance including monitoring, updating (patching), trouble shooting etc.

Disclaimer: Details may depend on the contract between SUSE and the consuming party. This PRD explains the variety of options available.

3 Security Requirements

Figure 2 summarizes the main deliverables from this PRD (which are provided in this section). This PRD tells the following about SLES:

1. It is indicated which areas (in the *ESARIS Security Taxonomy*) are covered by security measures implemented by SLES. If the consuming party also uses the *ESARIS Security Taxonomy*, it can easily identify own security standards which are relevant for SLES. (This is the basis for a later comparison.)
2. The individual security measures implemented by SLES are described. This allows the consuming party to compare own expectations and requirements with the security measures stipulated in this PRD. (This influences the purchasing decision.)
3. The PRD also provides guidance to securely use SLES, e.g. how to appropriately configure the product. (This ensures that the consuming party becomes aware about its own contribution. This is important to achieve the necessary level of security, but the consuming party may also learn that further expenditures are required.)
4. In general, the PRD also helps to securely integrate SLES in the final IT production environment. (This is important for the consuming party since the supplying party could only anticipate the IT environment and assume its typical characteristics. It's up to the consuming party to verify possible assumptions and to build the environment properly.)

These are necessary conditions for Zero Outage though they are, obviously, not sufficient alone.

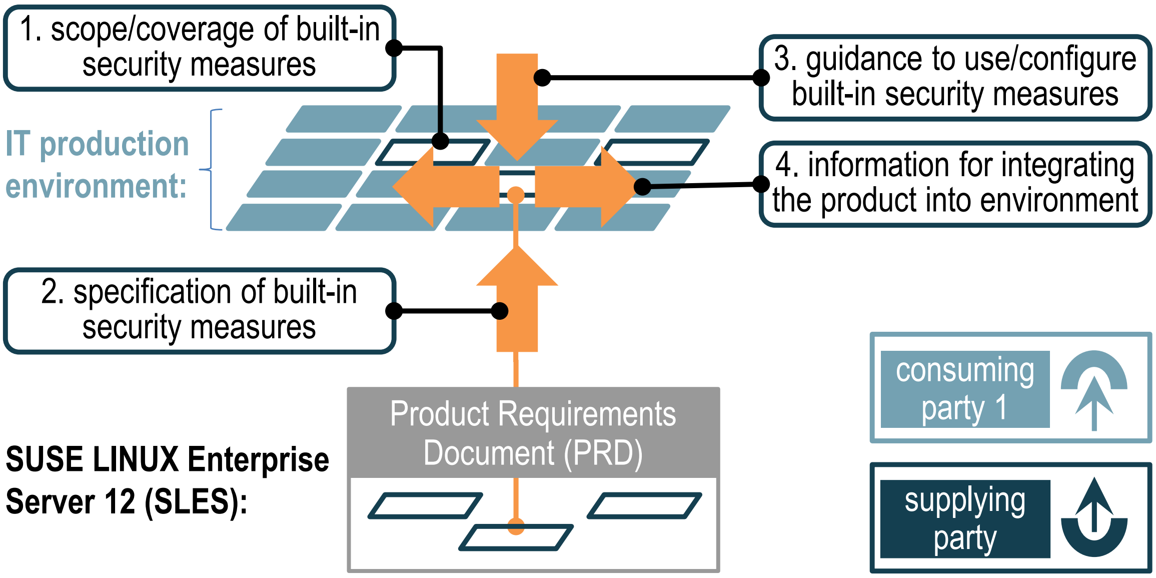
1. scope/coverage of built-in security measures
IT production environment:
2. specification of built-in security measures
3. guidance to use/configure built-in security measures
4. information for integrating the product into environment
SUSE LINUX Enterprise Server 12 (SLES):
Product Requirements Document (PRD)
consuming party 1
supplying party

Figure 2: Summary of deliverables from this PRD

3.1 Summary of security requirements

The “IT service” *SUSE LINUX Enterprise Server 12 Operating System* (SLES) is characterized as follows:

1. SLES is primarily software implementing state-of-the-art security measures of an operating system.
2. SLES is developed in a secure manner to ensure that security requirements are identified beforehand and implemented appropriately in the software.
3. SLES includes the provisioning of updates (also called patches) for the live time of the release to correct errors and to respond to requirements which occurred in the meantime.
4. The updates (patches) are developed using the same development standards applied for the original release of SLES.
5. The updates (patches) are distributed with appropriate guidance and securely to ensure their authenticity.
6. The default installation of the original release of SLES meets basic hardening standards. Several tools are part of SLES that are used to configure SLES to meet security requirements.
7. SLES can be installed as a traditional dedicated system and in a shared, virtualized computing environment as well. SLES supports the necessary profiles to ensure its secure use in shared, virtualized computing environments: The Hypervisors KVM and XEN are included.

Disclaimer: The measures or practices regarding the secure development only refer to the SLES software package (comprising software from multiple sources) and to software components developed by SUSE.

The security parts of SLES and their relation to security standards and areas in the *ESARIS Security Taxonomy* is shown in Figure 3.

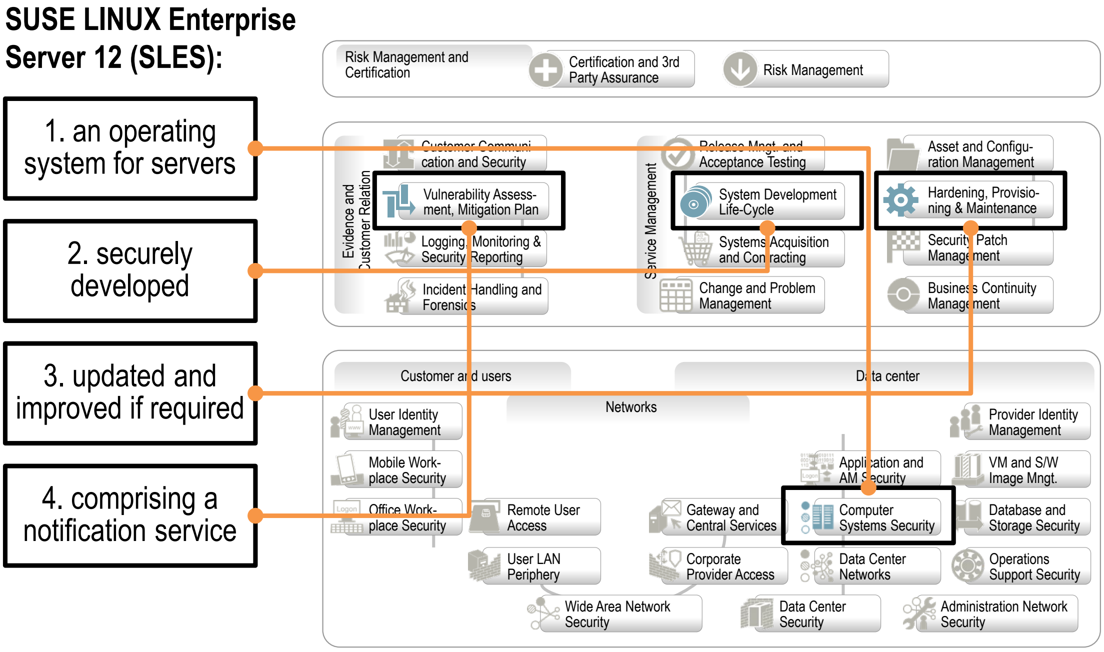
SUSE LINUX Enterprise Server 12 (SLES):
1. an operating system for servers
2. securely developed
3. updated and improved if required
4. comprising a notification service
Risk Management and Certification
Certification and 3rd Party Assurance
Risk Management
Evidence and Customer Relation
Customer Communication and Security
Vulnerability Assessment, Mitigation Plan
Logging, Monitoring & Security Reporting
Incident Handling and Forensics
Service Management
Release Mngt. and Acceptance Testing
System Development Life-Cycle
Systems Acquisition and Contracting
Change and Problem Management
Asset and Configuration Management
Hardening, Provisioning & Maintenance
Security Patch Management
Business Continuity Management
Customer and users
Data center
Networks
User Identity Management
Mobile Workplace Security
Office Workplace Security
Remote User Access
User LAN Periphery
Wide Area Network Security
Gateway and Central Services
Corporate Provider Access
Application and AM Security
Computer Systems Security
Data Center Networks
Data Center Security
Provider Identity Management
VM and S/W Image Mngt.
Database and Storage Security
Operations Support Security
Administration Network Security

Figure 3: SLES and areas in the *ESARIS Security Taxonomy*

3.2 Security requirements and responsibilities

In this chapter security measures are defined which need to be implemented by the IT service. The identification of the security measures relevant for the IT service subject to this PRD is conducted in three steps. **First**, areas (topics) are identified based on the specification of the IT service given in Chapter 2. The whole set of areas is provided by the ESARIS Security Taxonomy and its description given in [5]. **Second**, appropriate security standards are identified specifying security measures in the areas just selected. **Thirdly**, security measures relevant for the IT service are taken from those security standards and brought into a form meeting the requirements of this PRD with respect to level of detail etc. Fourth, the responsibility for implementing the security measure appropriately is assign to the supplying party, the consuming party or both.

3.2.1 Selection of security areas (topics)

The *ESARIS Security Taxonomy* supports the identification of security measures that are relevant for the IT service being provisioned. In the first step the relevant security areas/standards are identified using the specification of the IT service given in Chapter 2. The result is shown in the table below:

Table 1: Identification of security areas

Scope of SLES	Area relevant for SLES	
▪ SLES is primarily software of an operating system. ▪ SLES can be used in form of a traditional installation and in virtualized environments as an image as well. ▪ SLES provides built-in support for virtualization using KVM and XEN and includes those components.	CSS	SLES should therefore implement the security measures defined in *Computer Systems Security (CSS).*
▪ SLES is developed in a secure manner. ▪ SLES includes user guidance for secure installation and configuration.	SDL	SLES should therefore developed according to *System Development Life-Cycle (SDL).*
▪ SLES supports a secure default installation meeting basic hardening standards. ▪ SLES includes the provisioning of updates and makes patching possible without reboot.	HPM	SLES should therefore comprise security services relating to *Hardening, Provisioning & Maintenance (HPM).*
▪ SLES comprises software components from multiple sources which may require to be updated (patched).	VAM	SLES should therefore comprise security services relating to *Vulnerability Assessment and Mitigation Planning (VAM)*

3.2.2 Identification of security standards

This PRD uses the specification of the *ESARIS Security Taxonomy*[2] provided as a *Zero Outage Industry Standard* and the definition of security objectives contained therein. In addition, internal security standards of members of the *Zero Outage Industry Standard* association were used which are not made available to the public. The methodology used for creating this PRD[3] does not prescribe any specific security standard today. It only defines the level of detail of the specification which follows.

3.2.3 Definition of security measures implemented by SLES

In this PRD and the model behind it, the term security measure is uniquely used for every specification regarding security that need to be observed/met by the supplying party to provision the IT services or by the consuming party to securely use the IT service. The selected security measures cover the requirements meeting the IT service, without causing undue responsibilities to either party (supplier or consumer of the IT service), also hindering to provide technical progress and implementation of the IT service. Should the level of details be too high the delivery might be impacted due to the parties not being

[2] ESARIS Security Taxonomy – Synopsis, Scope and Content; Zero Outage Industry Standard, Release 1 about Security, February 2017, zero-outage.com/security [5]

[3] Managing security in the supplier network – Third Party Integration Model; Zero Outage Industry Standard, Release 2 about Security, August 2017, zero-outage.com/security [6]

able meeting their requirements. Should the level of details be too low holes in the end-to-end supply chain might occur.

The specification below is organized as follows:

- The security objectives defined by the Zero Outage Industry Standard[4] are used first.
- Additional detail is provided if necessary taken from the sources mentioned above.

Computer Systems Security (CSS)

Security measure SM1: The change of configurations and settings which have a potential effect on multiple users or comprehensive services or whole subsystems requires authorization. That is, access to all administrative functions of operating systems, hypervisors, etc., requires authorization. Users who are not intended to perform administrative tasks do not have administrative privileges.
Further detail regarding SM1 for clarification:

- Access Rights and Permissions
  Access rights to files and directories are controlled through user ownerships and permissions based on group memberships and access control lists to allow or deny access of users. To restrict access or protect information against unauthorized modifications, file and directory ownerships and access permissions are appropriately set on system files and system directories. This applies to all general purpose operation systems.
  SLES implements the standard UNIX access model DAC (Discretionary Access Control). This allows for compartments based on the model owner (UID), group (GID) and others/everybody.
- User Areas and Compartments
  All users have a defined user space or area on the operating system which prevents them from accessing other system areas or other areas of users. The user area also provides a boundary that prevents users from attempting to access system files, process of different users or escalate privilege to higher user levels.
  SLES implements the standard UNIX access model DAC (Discretionary Access Control). This allows for compartments based on the model owner (UID), group (GID) and others/everybody.
- Console and Local Access
  User access after authentication and authorization to the console, or other forms of local access is controlled to ensure that only required access is granted, as this level of access is seldom needed.
- Administrative Access
  Administrative access to the computer systems is provided in a secure way. Administrators are authenticated to allow for appropriate assignment of user roles and permissions (entitlements) to access information or to run commands and applications on the computer systems. Depending on the required level of security, different means are used basing the authentication on items the user to be authenticated knows (like password, PIN) or is in possession of (token like security smartcard, one time password generator, etc.).
  SLES delivers tools for secure administration of the operating system (e.g. SSH).

[4] ESARIS Security Taxonomy – Synopsis, Scope and Content; Zero Outage Industry Standard, Release 1 about Security, February 2017, zero-outage.com/security [5]

- [Responsibility of consuming party R1]: Administrative access refers to every access with higher privileges, namely those affecting the security configuration of SLES. The consuming party is responsible to use and configure the above security mechanisms in a way that SLES meets the security policies defined by the consuming party for its environment.

Security measure SM2: Malware can break the integrity of computer systems and thereby undermine the security achieved by other security measures. Means are provided that verify the integrity of software components, installed ones and updates (patches), and to scan for malware.
Further detail regarding SM2 for clarification:

- System and File Integrity
  System and file level checking of the file system ensures that all data stored on the storage device maintain its integrity and is not corrupted or manipulated. The integrity of important system files (usually executable binaries or configuration files) and files for permission control (such as Set User ID (SUID) and Set Group ID (SGID) in UNIX) is verified to prevent unauthorized or malicious modifications where applicable.
  SLES includes tools like Tripwire and Aide ensuring that modification of files and binaries are detectable. The scan for modified files is carried out on a regular basis.
  Using the above means, incorrect configurations and tampering with the configuration and other settings of operating systems and virtualization software can be detected so that corrective measures can be initiated.
- Malware scanning
  SLES comes with the open source anti-virus engine ClamAV. ClamAV has a limited set of scanning capabilities and limited performance compared to third party products. Hence, expect ClamAV to only provide basic protection.
- [Responsibility of consuming party R2]: Malware and virus scanning solutions are not installed and maintained by a standard installation of SLES itself. SUSE, however, provides with SLES various solutions for malware scanning, root kit detection or compromising of the SLES system itself. Also third party solutions exist, but it is the responsibility of the consuming party to choose the proper solution for their use case and implement and maintain it properly.

Security measure SM3: Computer systems communicate with other IT systems which they do not control. As a result, the operating system controls inbound and outbound traffic and decide which protocols and services can be used and by which applications.
Further detail regarding SM3 for clarification:

- SLES supports the usage of different network interfaces. It is the responsibility of the consuming party to provide the required setup of network cards to support such functionality and also to setup and configure the network stack to ensure this functionality.
- [Responsibility of consuming party R3]: Prevent interference: Through an appropriate configuration, the consuming party must ensure separation of network interfaces or isolation of customer data communication, communication with storage, and access for administration, respectively. Computer systems that do require direct access to the Internet may have an additional and separate interface for this purpose.
- [Responsibility of consuming party R4]: SLES comprise a firewall. The firewall service is to be installed by default. Whenever SLES is used in a network environment, the consuming party can use the kernel functions that allow the manipulation of network

packets to maintain a separation between internal and external network areas. The Linux netfilter framework provides the means to establish an effective firewall that keeps different networks apart. The consuming party must choose default settings that deny any traffic which is not allowed by rules. The firewall must be configured for the consuming party and their network traffic and protocols.[5]

Security measure SM4: Different applications that simultaneously run on one computer system (typically virtual machines (VMs) each comprising one or more applications and an operating system) are securely separated which allows for the sharing of resources without an unwanted or illegal flow of information or any other illegal interference between them.

Further detail regarding SM4 for clarification:

- Hardening and Basic Configuration
  Hardened configuration for the virtualization host (especially the hypervisor KVM or XEN) is available. Only the minimum services required by the virtualization host are configured to allow the host to maximize the available resources, and reduce the number of services which can be accessed by the Virtual Machines (VM), and thereby reduce possible vulnerabilities in software and hardware devices which might be exploited.
- Isolation of Virtual Machines and Communication
  All virtual machines device related functionality is restricted to a level which the virtual machine needs or must use to interact with the physical hardware. The virtualization host (especially the hypervisor) restricts the device functionality of its hosted Virtual Machines (VM) to the required extent to reduce the probability of virtual hardware and device based attacks. This includes that Virtual Machines (VM) are prevented to interfere with others in an unauthorized way and that communication is separated as required.

Security measure SM5: The access to and the communication with any virtualization software (hypervisor or virtual machine monitor) shall strictly be controlled and only be accessible by authorized operations personnel (administrators).

Further detail regarding SM5 for clarification:

- Console and Administrative Access
  Administrative access to the virtualization host (especially the hypervisor) is limited. Due to the security implications (capability to manage physical resources and Virtual Machines (VM), start and stop VM etc.) administrative access to the hypervisor is strictly restricted.
  [Responsibility of consuming party R5]: Administrative access refers to every access with higher privileges, namely those affecting the security configuration of SLES. The consuming party is responsible to use and configure the above security mechanisms in a way that SLES meets the security policies defined by the consuming party for its environment.

[5] See also https://www.suse.com/documentation/sles-12/book_hardening/data/sec_sec_prot_general_ports.html and https://www.suse.com/documentation/sles-12/book_hardening/data/sec_sec_prot_general_disable_xinetd_services.html

Security measure SM6: Virtual machines that are no longer needed on a physical machine shall immediately be deleted from the computer system. Local resources such as main memory are cleaned from residual data before being assigned to another virtual machine. However, the virtual machine file system images might be retained on centralized storage (e.g., NAS or SAN) for archival purposes or for restarting the virtual machine at a later time if required by the contractual agreements with the customer.

System Development Life-Cycle (SDL)

The System Development Life-Cycle is a process for developing demonstrably reliable and secure software and IT systems. It includes activities performed with the goal that software and IT systems respond to needs by providing the required functionality correctly and nothing more. That means that requirements are implemented correctly without introducing vulnerabilities. Specific security measures include the following:

Security measure SM7: The discussion and comprehension of security requirements is done before the appropriate management decisions and plans be made. Risks are continuously be analyzed so that security design issues can be detected and fixed before coding is committed, if possible. Processes and plans are established to tackle new security vulnerabilities or critical situations.

Security measure SM8: The design and implementation is arranged and controlled in a structured way for ensuring that requirements are met and flaws prevented. Secure-coding best practices are applied as well as proven testing processes and procedures.

Security measure SM9: A final security review and testing is conducted before delivery. Instructions for customers are included in the service package, which are sufficient managing the secure configuration and deployment of the software.

Security measure SM10: The development environment is protected and appropriate tools are used in order to prevent manipulation, espionage or any other adverse impact on the development and manufacturing process and its results.

SLES comprises software from multiple sources (developers). Therefore, the measures or practices regarding the secure development only refer to the SLES software package (comprising software from multiple sources) and to software components developed by SUSE.

Hardening, Provisioning and Maintenance (HPM)

Hardening comprises all methods applied to ICT systems, software and components that reduce the possibility of vulnerabilities and susceptibility to attacks. Provisioning comprises all methods of deployment and activation of ICT service including conception, installation, configuration, and approval. Maintenance comprises technical support to ensure continued operation and actuality, including the help desk.

[Responsibility of consuming party R6]: Only those versions of software and IT systems are used which are approved for IT production (at least by the manufacturer). They should only be used within the period of the active manufacturer support.

Included with SUSE Linux Enterprise Server, AppArmor is an application security tool designed to provide an easy-to-use security framework for applications. AppArmor security policies, called “profiles”, completely define which system resources and files can be accessed by each application. SELinux is an advanced technology for securing Linux systems.

Security measure SM11: Test data sets, software components installed for testing, default data sets and default (or initial) accounts or passwords and the like are removed from IT systems before switching to IT service delivery for customers. Such software or data may remain on the IT systems if necessary for a (power-on or regular) self-test.
Further detail regarding SM11 for clarification:

- Default installation of packages does not install test and sample data. Test and sample data are offered as add-on packages (e.g. tomcat.rpm and tomcat-samples.rpm).
- The default installation shall only include the packages needed for the operating system itself to run. All other software is optional and shall only be installed if actually needed. The graphical user interface is not to be installed. Where possible console-only versions of the packages required shall be installed. If that is not available there should be an alternative to replace it.

Security measure SM12: Software and IT systems configured in a way that reduces the possibility of vulnerabilities and susceptibility to attacks. One means to achieve this is the so-called system hardening, in which, for example, software components or services that are not required or never to be used are removed. IT systems should be assigned to classes which express different levels of control, trustworthiness and attack potential, depending on the network zone in which they are operated. For instance, IT systems in the DMZ and in the Data Center LAN may belong to different classes and may be treated differently.
Further detail regarding SM12 for clarification:

- Hardening center in YaST: The hardening center should be enabled by default. It shall make clearly visible if settings deviate from the defaults.

[Responsibility of consuming party R7]: Software and IT systems are configured in a way that applicable security policies are met. Software and IT systems run with the least possible privileges as appropriate.
Further detail regarding R7 for clarification:

- Using e.g. YaST, the consuming party determines the finally installed software depending on its needs according to applicable policies.

Security measure SM13: Maintenance comprises technical support aimed at ensuring that operations remain functional and are updated. Help desk services frequently are the access point for standard maintenance. Maintenance-related tasks are organized in a way that the overall state of security is upheld and no configurations exist that compromise security. Maintenance is performed in a manner that the confidentiality, the integrity and the availability of user data is ensured.
Further detail regarding SM13 for clarification:

- The concreate services provided by SUSE may depend on the contract between SUSE and the consuming party.

Vulnerability Assessment and Mitigation Planning (VAM)

SLES includes a vulnerability notification service, also known as the provisioning of CERT advisories, i.e. users are informed about software errors, their consequences and recommended solutions (patches), mitigation and/or workarounds.

Security measure SM14: Security relevant information about vulnerabilities is continually gathered from different sources (developers of used software). A vulnerability notification service is provided helping users to understand vulnerabilities and initiate counteraction such as the implementation of updates (patches).

Further detail regarding SM14 for clarification:

- SUSE provides security fixes via a subscription service. The same is true for the notifications just mentioned.
- [Responsibility of consuming party R8]: It is the responsibility of the consuming party to subscribe to this service and to apply the fixes in a timely manner to secure an updated secure system.

3.2.4 Assignment of responsibilities

The above specification assigns the responsibility for appropriately implementing a security measure to the supplying party, the consuming party or both. This assignment is necessary to provide transparency and set expectations. If the responsibility is assigned to the supplying party, it knows what to implement and provide. The PRD is also used to inform the consumer. By means of the PRD, the consuming party is exactly informed about the level of security and how it is achieved. The PRD can also be used to make a purchasing decision and to differentiate offers (market transparency with respect to security). The consuming party usually uses this information to ensure it meets the next level in the supply chain.

In the event the supplied IT service (specified in this PRD) does not meet the requirements of the consuming party (in the next level in the supply chain), the party should implement additional security measures (not defined in this PRD) to meet or exceed the requirements.

If security measures are modified from its original specification, this is indicated in the security measures' specification by making a reference to section 3.3 providing the details.

In the event that the consuming party is assigned any responsibility to implement security measures or to contribute to their appropriate implementation or use,

- this is marked using "**[Responsibility of consuming party Rx]"** in section 3.2.3.
- In these cases, guidance from the supplying party may be required. Such guidance is given (or referred to) in section 3.4.

3.3 Amendments and rationale

Readers of this PRD might be familiar with the security standards used to specify the security measures for the IT service in section 3.2 of this PRD. If a security measure has been modified from its specification the changes are documented below. More detail is provided about the differences, and a rationale is given as to why the original source needed to be changed whilst meeting the security objective.

This example of a PRD uses the specifications published as a *Zero Outage Industry Standard* and internal security standards of members of the *Zero Outage Industry Standard* association not made available to the public. Refer to section 3.2.2. As result, possible amendments are also not made public with this sample PRD.

3.4 Guidance to the consuming party

Usually, the consuming party is required to observe guidance for the IT service to be securely used. Such guidance is provided in this section. It is provided by the supplying party to the consuming party to ensure the effectiveness of already built-in security measures which comprise e.g. the provision of a specific scenario, the performance of specific actions or similar. Providing a secure configuration is one example which requires appropriate guidance. Checking for manipulations or replacement after shipment (receive) is another. It may also be necessary that the consuming party provides additional security services which are assigned to the consuming party in section 3.2. In this case a summary is given in form of guidance.

The consuming party must contribute to the security of using SLES. Major areas of activity are marked as **[Responsibility of consuming party Rx]** in section 3.2.3. There are 8 such areas in this PRD.

The following concrete guidance is part of SLES helping the consuming party to appropriately use the product and contribute to its security as indicated above:

The **Security Guide**[6] introduces basic concepts of system security, covering both local and network security aspects. It shows how to use the product inherent security software like AppArmor or the auditing system that reliably collects information about any security-relevant events. It covers extensive documentation about the authentication mechanisms available on Linux, such as NIS or LDAP. It deals with aspects of local security like access control lists, encryption and intrusion detection. In the network security part you learn how to secure computers with firewalls and masquerading, and how to set up virtual private networks (VPN). This guide shows how to use security software like AppArmor or the auditing system that collects information about security-relevant events.

The **Security and Hardening Guide**[7] deals with the particulars of installing and setting up a secure SUSE Linux Enterprise Server, and additional post-installation processes required to further secure and harden that installation. It supports the administrator with security-related choices and decisions.

[6] Security Guide, SUSE Linux Enterprise Server 12 SP3; SUSE LLC, January 08, 2018, https://www.suse.com/documentation/sles-12/index.html[1]

[7] Security and Hardening Guide, SUSE Linux Enterprise Server 12 SP3; SUSE LLC, September 01, 2017, https://www.suse.com/documentation/sles-12/index.html [2]

The guide about **Supported Virtualization Technologies**[8] offers an introduction to setting up and managing virtualization with KVM (Kernel-based Virtual Machine), Xen, and Linux Containers (LXC) on SUSE Linux Enterprise Server. The first part introduces the different virtualization solutions by describing their requirements, their installations and SUSE's support status. The second part deals with managing VM Guests and VM Host Servers with libvirt. The following parts describe various administration tasks and practices and the last three parts deal with hypervisor-specific topics.

The guide on **system analysis and tuning**[9] is for administrators and covers problem detection, resolution and optimization. Find how to inspect and optimize your system by means of monitoring tools and how to efficiently manage resources. Also contains an overview of common problems and solutions and of additional help and documentation resources.

An overview of security related certifications for SLES can be found here:
https://www.suse.com/de-de/support/security/certifications.

4 Role and use of this product requirement document

4.1 Status of document and version history

This PRD has been developed as a proof-of-concept implementation of a concept for managing security in a supplier network[10]. **This version is a first draft, mainly for demonstration purposes.** It may or may not be updated to reflect the progress made with SLES.

4.2 Legal disclaimer

Though this document specifies SLES, **binding statements are not provided by this PRD**. This PRD is intended to demonstrate how the Zero Outage concept for managing security in a supplier network can be put into practice. SLES has been selected for this purpose for the following reasons. SLES is widely availability and know. The nature of the business model of SUSE is an excellent example since it combines technology with selected services where the collaboration between the supplying party and the consuming party is badly required to ensure an appropriate level of security.

[8] SUSE Linux Enterprise Server: Supported Virtualization Technologies; SUSE LLC, Technical White Paper, 2013; the more detailed Virtualization guide is also available at https://www.suse.com/documentation/sles-12/index.html [3]

[9] SUSE Linux Enterprise Server 12: System Analysis and Tuning Guide; SUSE LLC, August 15, 2017, https://www.suse.com/documentation/sles-12/index.html [4]

[10] Managing security in the supplier network – Third Party Integration Model; Zero Outage Industry Standard, Release 2 about Security, August 2017, zero-outage.com/security [6]

4.3 Confidentiality

This PRD is not classified and will be made available on the Internet.

A References and Applicable Documents

[1] Security Guide, SUSE Linux Enterprise Server 12 SP3; SUSE LLC, January 08, 2018, https://www.suse.com/documentation/sles-12/index.html

[2] Security and Hardening Guide, SUSE Linux Enterprise Server 12 SP3; SUSE LLC, September 01, 2017, https://www.suse.com/documentation/sles-12/index.html

[3] SUSE Linux Enterprise Server: Supported Virtualization Technologies; SUSE LLC, Technical White Paper, 2013; the more detailed Virtualization guide is also available at https://www.suse.com/documentation/sles-12/index.html

[4] SUSE Linux Enterprise Server 12: System Analysis and Tuning Guide; SUSE LLC, August 15, 2017, https://www.suse.com/documentation/sles-12/index.html

[5] ESARIS Security Taxonomy – Synopsis, Scope and Content; Zero Outage Industry Standard, Release 1 about Security, February 2017, zero-outage.com/security

[6] Managing security in the supplier network – Third Party Integration Model; Zero Outage Industry Standard, Release 2 about Security, August 2017, zero-outage.com/security

[7] Eberhard von Faber and Wolfgang Behnsen: Secure ICT Service Provisioning for Cloud, Mobile and Beyond, ESARIS: The Answer to the Demands of Industrialized IT Production Balancing Between Buyers and Providers, 2017, ISBN- 978-3-658-16481-2

B List of Abbreviations

ESARIS	Enterprise Security Architecture for Reliable ICT Services
ICT	Information and Communication Technology (IT and TC)
ISO	International Organization for Standardization
IT	Information Technology (here also uses for ICT)
TC	Communication Technology
SLES	SUSE Linux Enterprise Server