Operations Security Evaluation of IaaS-Cloud Backend for Industry 4.0

Oliver Schluga[1], Elisabeth Bauer[1], Ani Bicaku[1,3], Silia Maksuti[1,3],
Markus Tauber[1] and Alexander Wöhrer[1,2]
[1]*University of Applied Sciences Burgenland, Eisenstadt, Austria*
[2]*Univeristy of Vienna, Vienna, Austria*
[3]*Luleå University of Technology, Luleå, Sweden*

Keywords: Cloud Computing, IaaS, ISO 27017, Security, Virtualization, OpenStack, VMware, Industry 4.0.

Abstract: The fast growing number of cloud based Infrastructure-as-a-Service instances raises the question, how the operations security depending on the underlying cloud computing infrastructure can be sustained and guaranteed. Security standards provide guidelines for information security controls applicable to the provision and use of the cloud services. The objectives of operations security are to support planning and sustaining of day-to-day processes that are critical with respect to security of information environments. In this work we provide a detailed analysis of ISO 27017 standard regarding security controls and investigate how well popular cloud platforms can cater for them. The resulting gap of support for individual security controls is furthermore compared with outcomes of recent cloud security research projects. Hence the contribution is twofold, first we identify a set of topics that still require research and development and secondly, as a practical output, we provide a comparison of popular industrial and open-source platforms focusing on private cloud environments, which are important for Industry 4.0 use cases.

1 INTRODUCTION

Following a current forecast (Gar, 2017) the cloud service market is projected to grow 18.5% in 2017 to total $260.2 billion, up from $219.6 billion in 2016. The highest growth arises from Infrastructure as a Service (IaaS), which is expected to show the fastest growth over the next five years. The reason for this is the shift away from legacy IT-systems to cloud-based services following the trend of organizations pursuing a digital business strategy. Another trend we see evolving is Industry 4.0 (Henning, 2013), with the goal to increase flexibility and automation in the production and provisioning of goods. Such an endeavor release strongly on flexible back-end services like the cloud. Initially, we expect a focus on private cloud environments due to security concerns, typical for manufacturing industry. Evolvement of trends will never the less be driven by novel service models derived from IaaS trends, which are also the drivers for guidelines and standards. The National Institute of Standards and Technology (NIST) (Mell et al., 2011) defines IaaS as the capability provided to the consumer to access resources (e.g., storage, networks, processing, etc.) and to deploy and run arbitrary software including operating systems and applications. The consumer has control over operating systems, storage and deployed applications but not to the underlying cloud infrastructure.Following this definition the cloud service provider is responsible to provide an elastic, reliable and secure IaaS platform for the cloud consumer. Additionally, because of the cloud computing architecture, IaaS can be used by other cloud services, like Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS). Regarding these, issues in IaaS may compromise the functionality of the overlying layers. As a result, apart from legal, contractual and technical concerns, security is one of the main topic in IaaS.

Operations security within IaaS involves planning and sustaining the day-to-day processes that are critical to keep data (virtual machines) and systems (virtualization platform) confidential, maintain the integrity and ensure their availability. Therefore, the most important aspect of operations security is that the operations themselves need to be repeatable, reliable and consistently performed. Additionally, operations security need to be measurable for representing and assessing the current state of an environment or for comparison purposes. To accomplish this, specific operations security related measurable metrics are used.

Schluga, O., Bauer, E., Bicaku, A., Maksuti, S., Tauber, M. and Wöhrer, A.
Operations Security Evaluation of IaaS-Cloud Backend for Industry 4.0.
DOI: 10.5220/0006683103920399
In *Proceedings of the 8th International Conference on Cloud Computing and Services Science (CLOSER 2018)*, pages 392-399
ISBN: 978-989-758-295-0

International standards development organisations, like NIST[1] , ENISA[2] or ISO[3], provide requirements, specifications, guidelines and characteristics which can be used consistently to ensure that processes and services are fit for their purpose. Additionally, most standards define metrics for measurement or assessment of processes and services. It is important to match those recommendations, which the environment manufacturing industry relies on. Our main contributions and preliminary results in this paper are:

- Deriving operations security metrics for IaaS in Industry 4.0
- Identification for research and development needs in operations security with respect to IaaS in Industry 4.0, considering ISO27017 standard
- A comparison of popular IaaS platforms (OpenStack and VMware) and an evaluation of their capability to support ISO27017 recommendations

2 RELATED WORK

Relevant research work is carried out to support organizations dealing with security considering existing standards and best practices. A general comparison of various security related standards and frameworks can be found at (Gao and Schneider, 2012). Disterer (Disterer, 2013) provides a detailed evaluation of the differences within ISO 270xx series considering ISO 27000, ISO 27001 and ISO 27002 standards. In addition the author provides an implementation of ISO 27001 certification from IT service management point of view. This work is based on ISO 27001 standard but considering operations security or ISO 27017.

Donevski et al. (Donevski et al., 2013) analyze the security assessment of virtual machines in OpenStack by addressing the security vulnerabilities from inside and outside the cloud. However, they do not address any specific security standard or best practice and do not consider the individual OpenStack components.

Majudar et al. (Majumdar et al., 2015) and Madi et.al (Madi et al., 2016) propose an approach in security compliance auditing for clouds with special focus on identity and access management. The auditing system is integrated into OpenStack by considering only the main modules. This work evaluates security regarding identity and access management extracted from different standards. The authors also include ISO 27017 in their evaluation but their research focus is only in auditing OpenStack. In comparison with this approach, we extract the operations security properties from ISO 27017 and evaluate their applicability on OpenStack and VMware.

Other existing works address security on VMware platform. Montesino and Fenz (Montesino and Fenz, 2011) analyze information security automation in respect to security standards and best practice guidelines. In addition they evaluate which existing tools can be used to support the automation by considering also VMware vSphere. In contrast with this work we evaluate operations security properties from ISO 27017 and their applicability on OpenStack and VMware.

Ryoo et al. (Ryoo et al., 2014) highlights the challenges between cloud security auditing and traditional IT security auditing via interviews with experienced cloud security auditors. This work analyzes the applicability of different standards including ISO 27017 operations security controls within an IaaS environment based on VMware vSphere. However, they do not consider specific properties of operation security and the applicability on OpenStack or VMware.

Research activities regarding the development of cloud computing has been very intense during the last years and several EU-funded projects have investigated relevant problems focusing on security in cloud. In the SECCRIT project, we have developed resilience components for clouds, policy driven security controller, techno-legal guidance and a cloud assurance evaluation methodology for aggregating and simplifying monitoring information related to high level security properties (Hudic et al., 2014), (Bicaku et al., 2016). PrismaCloud project brings novel security concepts, such as cryptographic concepts and methods to improve and guarantee the required security for sensitive data in the cloud (Bleikertz et al., 2015). Cumulus project has addressed security and privacy issues by developing a framework of models and tools to support the certification of security properties in the cloud based on the cloud trust protocol (Anisetti et al., 2015). Arrowhead project provides tools and methods for automation considering local clouds (Delsing, 2017).

The European Commission Community Research and Development Information Service (CORDIS[4]) lists additional research projects addressing cloud security: Coco-Cloud[5] analyses the secure and private exchange of data using cloud computing. TCLOUDS[6] focuses on the privacy and usability

[1] http://www.nist.gov/
[2] https://www.enisa.europa.eu/
[3] http://www.iso.org/iso/home.html
[4] http://cordis.europa.eu/
[5] http://www.coco-cloud.eu/
[6] http://www.tclouds-project.eu/

challenges of cross-border usage of personal data in communication with respect to data ownership. SERENITI analyses Networked Critical Infrastructures (NIC) and develops state-of-the-art techniques and tools in designing secure and resilient industrial Information and Communication Technologies (ICT).

3 OPERATIONS SECURITY

Industrial Control Systems (ICS) have been traditionally built as stand-alone systems, not connected to the outside world. The interconnection with the corporate network, wireless, mobile or cloud-based services make these systems potentially reachable from cyber-attacks. Therefore, each organization must understand the potential risks of a production environment which is no longer isolated from the Internet and puts the system at a risk of cyber-attacks. Thus, operations security is of utmost importance to be considered in Industry 4.0 applications. The application of operations security concepts supports the achievement of the following high-level security objectives: (i) reduce the operational vulnerability, (ii) protect the computing resources and information assets, (iii) balance of ease-of-use vs. system controls and balance of value of data vs business needs, and (iv) compliance with laws and organizational aspects.

Table 1 lists common security operations concepts identified by $(ISC)^2$ certifications in CISSP (Stewart et al., 2012). Combined, these practices help to prevent security incidents from occurring, and limit the scope of incidents that do occur.

Table 1: Basic Security Operations Concepts.

Security operations concept	Description
Need-To-Know	Grant users access to data they need
Least Privilege	Grant users only necessary privileges
Separation of Duties Two-Person Control	No single person has full control over a system
Job Rotation	Rotate of responsibilities between different persons
Mandatory vacations	Provides a form of peer review
Monitor special privileges	Monitor operations that require special access or elevated rights
Information Life Cycle Management	Marking, handling, storing and destroying data
Service Level Agreements	Agreement between organization and outside entity
Addressing Personal Safety	Controls enhancing personal safety, e.g. unlock locks when power is lost

Additionally, the elements listed in Table 2 are part of CISSPs security domain (Disterer, 2013) regarding security operations objectives. These elements cover security operations management tasks and they can be found within the ISO 270xx series.

Table 2: Security Operations Objectives.

Security operations objectives	Description
Provisioning and Managing Resources	Life cycle management of Hardware, software, physical, virtual or cloud-based assets
Configuration Management	Keeps a system in a secure consistent state
Change Management	Prohibit unauthorized changes
Patch Management	Protection against emerging threads
Vulnerability Management	Cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities

4 STANDARDS AND BEST PRACTICE GUIDELINES

In this section we provide a summary of the most relevant existing standards, best practice guidelines with the purpose to get a better overview of gaps and overlaps in the current state of the art related to operations security. Existing standards and best practice guidelines that address operational security by providing either methodologies or controls are listed below.

ISO/IEC 270xx series gives an overview and explains the Information Security Management Systems (ISMS), referring to ISMS series of standards with related terms and definitions. The standards ISO/IEC 27000, 27001, 27002 and 27017 are international standards, which have been adopted from different organizations around the world.

ISO/IEC 27000:2016 (Disterer, 2013) gives an overview of information security management systems (ISMS), terms, and definitions used in the ISMS.

ISO/IEC 27001:2013 (Fomin et al., 2013) specifies the requirements for implementing, maintaining, and continually improving the ISMS. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

ISO/IEC 27002:2013 (Calder and Watkins, 2013) gives guidelines for organizational information security and information security management practices including the selection, implementation, and management of controls taking into consideration the organization's information security risk environments. It is designed to be used by organizations that intend to: (i) select controls within the process of implementing ISO 27001, (ii) implement commonly accepted information security controls, and (iii) develop their own information security management guidelines.

ISO/IEC 27005:2011 (ISO/IEC-27005, 2011) is based on ISO/IEC 27001 and provides guidelines for information security risk management and implementation of information security.

ISO/IEC 27017:2015 (ISO/IEC, 2015) provides con-

trols and implementation guidance for both cloud service providers and cloud service consumers. The standard provides guidelines for information security controls applicable to the provision and use of cloud services by providing: (i) additional implementation guidance for relevant controls specified in ISO/IEC 27002, and (ii) additional controls with implementation guidance that specifically relate to cloud services.

The National Institute of Standards and Technology (NIST) 800 series is a set of publications developed as outcome of research for optimizing the security of IT systems and networks.

NIST SP 800-82 (Stouffer et al., 2011) gives an overview of ICS and also what makes it different and unique from traditional IT systems by providing, (i) ICS risk management and assessment, (ii) how to develop and deploy an ICS specific cyber security program, (iii) different ways for architecting the industrial control system for security, and (iv) applying security controls to ICS.

NIST SP 800-184 provides tactical and strategic guidance to support organizations in a technology-neutral way in improving their cyber event recovery plans, processes, and procedures.

The Cloud Security Alliance[7] (CSA) provides best practice efforts by considering 14 domains about critical areas of cloud computing and works on continuous improvement of the published best practice methods concerning security.

CTP - Cloud Trust Protocol, provided by CSA, offers cloud users the opportunity to request and acquire information about transparency with respect to cloud service providers. The primary purpose of the CTP and the elements of transparency is to generate evidence-based confidence that everything that is claimed to be happening in the cloud is indeed happening as described.

Every standard from the ISO 270xx series is designed with a certain focus to build the foundations of information security in an organization, ISO 27001 should be used; to implement controls, ISO 27002 should be used, to carry out risk assessment and risk treatment, ISO 27005 should be used, and to protect the information in the cloud, ISO 27017 should be considered. Standards such as NIST SP 800-82 and NIST SP 800-184, consider the operations security but in most of them is missing a step-by-step guideline how to achieve the intended goals. While most of the standards address the operational security for data exchange or communication protocols, other standards such as ISO/IEC 27017 mainly focus on operations security issues in cloud platforms, which is the reason why we use it for the assessment.

[7]https://cloudsecurityalliance.org/

Table 3: Content of (12) Operations Security.

	Security Control		Security Objectives
(12) Operations Security	12.1 Operational procedures and responsibilities	12.1.1	**Documented Operating Procedures** Operating procedures should be documented and made available to all users who need them.
		12.1.2	**Change Management** Changes that affect information security should be controlled.
		12.1.3	**Capacity Management** The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
		12.1.4	**Separation of Development, Testing and Operational Environments** These environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.
	12.2 Protection from malware	12.2.1	**Controls against Malware** To ensure that information and information processing facilities are protected against malware.
	12.3 Backup	12.3.1	**Backup** Backup copies should be taken and tested regularly in accordance with an agreed backup policy.
	12.4 Logging and Monitoring	12.4.1	**Event Logging** Event logs recording user activities, errors and information security events should be produced, kept and regularly reviewed.
		12.4.2	**Protection of Log Information** Logging facilities and log information should be protected against unauthorized access.
		12.4.3	**Administrator and Operator Logs** System administrator should be logged and the logs protected and regularly reviewed.
		12.4.4	**Clock Synchronization** The clocks of all relevant information processing systems should be synchronized to a single reference time source.
	12.5 Control of operational software	12.5.1	**Installation of Software on Operational Systems** Procedures should be implemented to control the installation of software on operational systems.
	12.6 Technical vulnerability management	12.6.1	**Management of Technical Vulnerabilities** Information about technical vulnerabilities should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the risk.
		12.6.2	**Restrictions on Software Installation** Rules governing the installation of software by users should be established and implemented.
	12.7 Information systems audit considerations	12.7.1	**Information Systems Audit Controls** Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.

5 OPERATIONS SECURITY CONTROLS

As result of the evaluation of existing standards and best practice guidelines which address operations security, we assess clause *(12) Operations security* of ISO 27017 (ISO/IEC, 2015), which provides specific guidelines concerning information security controls for cloud services, to show the applicability in popular commercial and open-source cloud platforms.

Table 3 gives an overview of the related controls and their cloud specific considerations.

Based on this clause, security related metrics are extracted and used to assess the applicability on popular IaaS platforms such as OpenStack and VMware vSphere. OpenStack provides software-defined-datacenter (SDDC) capabilities, while vSphere is a popular commercial Hypervisor providing IaaS. We deliberately choose VMware as it is a de factor industry standard, and OpenStack as we expect more services available via the open source community. As a result the applicability of operations security metrics is compared and discussed.

6 ASSESSMENT OF CLOUD PLATFORMS

Within this analysis the applicability of ISO 27017 Operations Security controls are categorized in four degrees reflecting additional administrative efforts. A lower degree of applicability results in higher administrative efforts. Table 4 provides the degrees of applicability and a description for each degree.

6.1 OpenStack

OpenStack is an open-source software platform for cloud computing mostly providing IaaS. The platform consists of different modules where each module provides a specific service. OpenStack has a modular architecture with code names for its components which are described in Table 5.

The interaction of all services enables a high integration to provide IaaS within a SDDC. A SDDC (Nunes et al., 2014) is a data storage facility where all elements of the infrastructure, networking, storage, CPU and security are virtualized and delivered as a service. Deployment, provisioning, configuration and operation of the entire infrastructure is abstracted from hardware and implemented through software. Each component can be provisioned, operated and managed through an application programming interface (API).

Typically, the core architectural components that comprise a software-defined datacenter include: (i) computer virtualization (compute), (ii) Software-Defined Storage (SDS), (iii) Software-Defined Network (SDN), and (iv) Business Logic Layer (BLC).

This work evaluates the applicability of operations security on a core installation of OpenStack Juno with focus on SDDC capabilities. In Table 5 are listed the core services of OpenStack, the corresponding SDDC component and the functionality of each service.

The applicability of Operations Security controls on an OpenStack IaaS is analyzed using the listed degrees and categories. The following, Table 6 shows the analysis from the providers point of view where are presented the related services, the degree of applicability, and the description of the additional tasks:

12.1.1 - Documented operating procedures is implemented (I) by using the Keystone module. The user roles, participation and the related processes are documented via Keystone.

12.1.2 Change Management is applicable (A). In general the cloud service consumer must be informed manually. OpenStack architecture and processes are documented on the community webpage. Because it does not offer any supporting change management services, the complexity has a high classification.

Table 4: Degree of Applicability for Operations Security Controls.

Degree of Applicability		Description
Not applicable	NA	The control is not applicable
Applicable	A	The control is applicable, a complete manual process is necessary for fulfillment
Implemented	I	The control is implemented as a service, additional, semi-automated administrative tasks are necessary for fulfillment
Natively Implemented	NI	The control is natively implemented as a service.

Table 5: OpenStack module and SDDC component.

Service	Module	SDDC	Functionality
Dashboard	Horizon	BLC	Web-based self-service VM configuration portal
Compute	Nova	compute	VM Life-cycle management
Networking	Neutron	SDN	Multi-tenant network connectivity
Object storage	Swift	SDS	Storage for unstructured data via REST
Block storage	Cinder	SDS	Persistent block storage for VMs
Identity service	Keystone	BLC	Authentication and authorization
Image service	Glance	BLC	Storage for VM images
Telemetry	Ceilometer	BLC	Monitoring and metering
Orchestration	Heat	BLC	Orchestration of cloud infrastructure
Database service	Trove	BLC	Saleable and reliable database storage

Table 6: Applicability of Operations Security Controls in OpenStack.

Security Objectives	Degree of Applicability	Related service	Additional tasks
12.1.1	I	Keystone	customer information via Horizon
12.1.2	A		manual customer information
12.1.3	NI	Ceilometer	
12.1.4	I	Neutron	multiple OpenStack instances and/or SDN
12.2.1	A		anti-virus module missing
12.3.1	A		backup module missing
12.4.1	I	Horizon	log information incomplete
12.4.2	NI	Keystone	
12.4.3	A		Syslog and Keystone Log
12.4.4	NI	Horizon	
12.5.1	A		manual process necessary
12.6.1	A		manual process necessary
12.6.2	I	Neutron	custom images
12.7.1	A		manual process necessary

12.1.3 Capacity Management is completely fulfilled (NI) by OpenStack. Ceilometer provides measurement and metering services for the cloud service provider (future capacity planning) and the cloud service consumer (SLA).
12.1.4 Separation of Development, Testing and Operational Environment is partially implemented (I). Neutron offers SDN capabilities for tenant separation. Storage and compute separation can only be archived by using multiple OpenStack instances.
12.2.1 Controls against Malware and *12.3.1 Backup* are applicable (A). Common Linux anti-virus and backup services are available for manual installation. Consumer information and reporting is not implemented within OpenStack. If snapshots are assumed as a backup, objective 12.3.1 can be considered as partially implemented (A).
12.4.1 Event Logging is partially implemented (I). OpenStack related logs are offered to the cloud service consumer within Horizon. Most events are logged in specific log files and the content is not provided to the cloud consumer.
12.4.2 Protection of Log Information and *12.4.4 Clock Synchronization* are completely fulfilled by OpenStack services (NI).
12.4.3 Administrator and Operator Logs is applicable (A). The requested log files are accessible using the operation system console only.
12.5.1 Installation of Software on Operational Systems is applicable (A). The installation of OpenStack system related components is controlled by the underlying operating system. Additionally, the content of a running machine is not accessible for administrators.
12.6.1 Management of Technical Vulnerabilities is applicable (A). OpenStack offers a vulnerability management process. The installation of hotfixes and patches has to be done by root manually. Horizon does not provide this information.
12.6.2 Restriction of Software Installation is partially fulfilled by OpenStack (I). The OpenStack administrator can publish predefined virtual machine images with no root access. The installation of custom applications is not possible for cloud service consumers.
12.7.1 Information System Audit Controls is applicable (A). OpenStack provides information about external audits, like case studies and white papers. Anyway, external audits are processed manually.

6.2 VMware vSphere

VMware vSphere is a commonly used commercial industrial virtualization platform providing IaaS. vSphere is available in three different editions: (i) Standard, (ii) Enterprise Plus, and (iii) Operations Management Enterprise Plus. The Standard edition offers server consolidation and business continuity features. Enterprise Plus provides resource management and enhanced application availability and performance capabilities. The Operations Management edition offers intelligent operations and consistent management and automation with predictive analytics. Furthermore vCenter Server is a centralized management tool for vSphere within large deployment. Additionally VMware offers a free hypervisor called vSphere Hypervisor (also called ESXi) providing basic virtualization features using a single physical host. This work addresses a limited vSphere Enterprise edition bundled with vCenter server (also called Essential Plus Kit (EPK) and the free version ESXi. A detailed description of all features offered by VMware vSphere 6.0 can be found at (Ser,). In follow, Table 7 shows the analysis from the providers' point of view where is presented the degree of applicability on ESXi and EPK and a description of the additional administrative tasks:

Table 7: Applicability of Operations Security Controls in VMware.

Security Objectives	Degree of Applicability		Additional tasks	
	ESXi	EPK	ESXi	EPK
12.1.1	I	NI	additional tasks necessary	
12.1.2	A	I	manual customer information	additional tasks necessary
12.1.3	I	NI	basic information available	
12.1.4	I	I	multiple vSphere Server and/or SDN	
12.2.1	A	A	anti-virus module missing	
12.3.1	A	A	backup module missing	
12.4.1	I	NI	log information incomplete	
12.4.2	NI	NI		
12.4.3	I	NI	additional tasks necessary	
12.4.4	NI	NI		
12.5.1	A	NI	manual process necessary	
12.6.1	A	NI	manual process necessary	
12.6.2	I	I	custom images	
12.7.1	A	I	manual process necessary	additional tasks necessary

12.1.1 - Documented operating procedures is natively implemented (NI) in EPK by using the vCenter Server. The user roles, the user participation and the related processes are documented. ESXi implements (I) a basic authentication and authorization module for single server management.

12.1.2 Change Management is applicable (A) in ESXi, but it requires a manual information process. EKP uses vCloud Server by implementing change management processes natively (I).

12.1.3 Capacity Management is completely fulfilled by EPK (NI). vCenter provides measurement

and metering services for the cloud service provider (future capacity planning) and the cloud service consumer (SLA). ESXi implement basic tools for measurement the system state (I).

12.1.4 Separation of Development, Testing and Operational Environment is partially implemented (I). In general VMware offers SDN capabilities for network separation. Storage and compute separation can only be achieved by using ESXi instances.

12.2.1 Controls against Malware and *12.3.1 Backup* are applicable (A), but additional software and processes are needed. If snapshots are assumed as a backup, objective 12.3.1 can be considered as partially implemented (A).

12.4.1 Event Logging is partially implemented (I) in ESXi, a basic log viewer is available, log informations regarding system configuration are missing. EPK offers log access in configurable scopes (NI).

12.4.2 Protection of Log Information and *12.4.4 Clock Synchronization* are completely fulfilled by ESXi and EPK (NI).

12.4.3 Administrator and Operator Logs is implemented (I), but ESXi offers only one log file containing all information. vCenter allows the configuration of log access scopes (NI).

12.5.1 Installation of Software on Operational Systems is applicable (A) on ESXi, it is designed as single server hypervisor and does not offer processes of the installation of software on systems. vCenter allows full control on software installation tasks (NI).

12.6.1 Management of Technical Vulnerabilities is applicable (A) in ESXi, but the installation of patches has to be done by root manually. vCenter provides a patch management system natively (NI).

12.6.2 Restriction of Software Installation is partially fulfilled by ESXi and EPK (I). The administrator can publish predefined virtual machine images with no root access. The installation of custom applications is not possible for cloud service consumers.

12.7.1 Information System Audit Controls is applicable for ESXi (A), but implements no additional information. vCenter Server is the central management system and provides specific audit controls (I). Anyway external audits are processed manually.

6.3 OpenStack vs. VMware

Although the direct comparison of OpenStack and vSphere is not addressed in this work the application of Operations Security controls follows similar conditions. Necessary additional manual processes or additional tasks having the same degree of applicability are similar regardless the software. The following, Table 8 shows the comparison of OpenStack and VSphere in a compact view. The comparison of OpenStack and ESXi shows many matches. As a SDDN OpenStack offers comprehensive capacity management functionalities whereas ESXi provides basic performance indicators reflecting the current system state. Because ESXi is a small foot-printed hypervisor the protection of log information is integrated into the software whereas OpenStack uses standard Linux logging features. If vCenter is put on top of a vSphere hypervisor infrastructure the degree of applicability raises because of additional management capabilities.

Table 8: Comparison of the applicability of Operations Security controls on OpenStack and vSphere (the controls with the most manual and semi-automated additional activities necessary across platforms are highlighted).

Security Objectives	Degree of Applicability		
	OpenStack	ESXi	EPK
12.1.1	I	I	NI
12.1.2	A	A	I
12.1.3	NI	I	NI
12.1.4	**I**	**I**	**I**
12.2.1	**A**	**A**	**A**
12.3.1	**A**	**A**	**A**
12.4.1	I	I	NI
12.4.2	NI	NI	NI
12.4.3	A	I	NI
12.4.4	NI	NI	NI
12.5.1	A	A	NI
12.6.1	A	A	NI
12.6.2	**I**	**I**	**I**
12.7.1	A	A	I

7 CONCLUSIONS

This work presents an overview of standards and best practice guidelines with focus on operations security. We have evaluated ISO27017 standard with special focus on clause (12) Operations Security to check if open-source or commercial platforms such as OpenStack and VMware address these objectives. Applying objectives based on ISO 27017 operations security ensure correct and secure operation of virtual machines. Operations security requests the clear definition of operational processes regarding security as well as supporting infrastructure services. Different research projects and scientific works evaluated in our work, analyze and evaluate cloud computing technologies with respect to security risks in sensitive cloud environments but without focusing on ISO 27017 operations security. Considering the outcome of section 6, a practical output of this work is the comparison of OpenStack and VMware based on ISO 27017. Our results show that the security controls 12.3.1 and 12.2.1 are the least sufficiently supported by the investigated platforms. Furthermore, the secu-

rity controls 12.1.4 and 12.6.2 are only implementable with additional effort in the evaluated platforms. To the best of our knowledge relevant research projects, such as those extracted from the CORDIS database, do not explicitly address these findings. Even though some work on anomaly detection can be related to malware prevention, the provided solutions have not been taken up by the development community. Furthermore, we have identified that topics related to the above security controls have not been researched in a context in which private cloud infrastructures are preferred, such as Industry 4.0. This means that the above topics are seen as highly relevant future research and development topics. In our future work, motivated by these findings, we will work towards security and transparency in the cloud.

ACKNOWLEDGEMENTS

The work has been performed in the project Power Semiconductor and Electronics Manufacturing 4.0 (SemI40), under grant agreement No 692466.

REFERENCES

Gartner forecasts worldwide public cloud services revenue to reach $260 billion in 2017. http://www.gartner.com/newsroom/id/3815165.

Server-virtualization-software-vsphere-vmware. https://www.vmware.com/products/vsphere.html.

Anisetti, M., Ardagna, C. A., Damiani, E., Gaudenzi, F., and Veca, R. (2015). Toward security and performance certification of open stack. In *Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on*, pages 564–571. IEEE.

Bicaku, A., Balaban, S., Tauber, M. G., Hudic, A., Mauthe, A., and Hutchison, D. (2016). Harmonized monitoring for high assurance clouds. In *Cloud Engineering Workshop (IC2EW), 2016 IEEE International Conference on*, pages 118–123. IEEE.

Bleikertz, S., Vogel, C., Groß, T., and Mödersheim, S. (2015). Proactive security analysis of changes in virtualized infrastructures. In *Proceedings of the 31st annual computer security applications conference*, pages 51–60. ACM.

Calder, A. and Watkins, S. G. (2013). *Information security risk management for ISO27001/ISO27002*. It Governance Ltd.

Delsing, J. (2017). *IoT Automation: Arrowhead Framework*. CRC Press.

Disterer, G. (2013). Iso/iec 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 4(02):92.

Donevski, A., Ristov, S., and Gusev, M. (2013). Security assessment of virtual machines in open source clouds. In *Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention on*, pages 1094–1099. IEEE.

Fomin, V. V., Vries, H., and Barlette, Y. (2013). Iso/iec 27001 information systems security management standard: Exploring the reasons for low adoption. In *Proceedings of the third European conference on Management of Technology (EuroMOT)*.

Gao, F. and Schneider, S. (2012). Cloud frameworks: an information systems perspective. In *Proceedings of ConLife Academic Conference, Köln, Germany*.

Henning, K. (2013). Recommendations for implementing the strategic initiative industrie 4.0.

Hudic, A., Hecht, T., Tauber, M., Mauthe, A., and Elvira, S. C. (2014). Towards continuous cloud service assurance for critical infrastructure it. In *Future Internet of Things and Cloud (FiCloud), 2014 International Conference on*, pages 175–182. IEEE.

ISO/IEC (2015). Iso27017 - information technology – security techniques – code of practice for information security controls for cloud services. *Information technology-Security techniques*.

ISO/IEC-27005 (2011). Iso/iec 27005 information technology–security techniques–information security risk management.

Madi, T., Majumdar, S., Wang, Y., Jarraya, Y., Pourzandi, M., and Wang, L. (2016). Auditing security compliance of the virtualized infrastructure in the cloud: Application to openstack. In *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, pages 195–206. ACM.

Majumdar, S., Madi, T., Wang, Y., Jarraya, Y., Pourzandi, M., Wang, L., and Debbabi, M. (2015). Security compliance auditing of identity and access management in the cloud: application to openstack. In *Cloud Computing Technology and Science (CloudCom), 2015 IEEE 7th International Conference on*, pages 58–65. IEEE.

Mell, P., Grance, T., et al. (2011). The nist definition of cloud computing.

Montesino, R. and Fenz, S. (2011). Information security automation: how far can we go? In *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*, pages 280–285. IEEE.

Nunes, B. A. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., and Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys & Tutorials*, 16(3):1617–1634.

Ryoo, J., Rizvi, S., Aiken, W., and Kissell, J. (2014). Cloud security auditing: challenges and emerging approaches. *IEEE Security & Privacy*, 12:68–74.

Stewart, J. M., Chapple, M., and Gibson, D. (2012). *CISSP: Certified Information Systems Security Professional Study Guide*. John Wiley & Sons.

Stouffer, K. A., Falco, J. A., and Scarfone, K. A. (2011). Sp 800-82. guide to industrial control systems (ics) security: Supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc).