Audit and Assurance Specifics in Cloud-Based Industry 4.0 Environment

Frantisek Simeting
University of Economics in Prague, Prague, Czech Republic
simetinger@outlook.com

DOI: 10.20470/jsi.v9i3.349

Abstract: This paper focuses on the actual situation in Industry 4.0 environments which are based or with the involvement of cloud-based components. The paper summarizes the perception and understanding of these cloud-based manufacturing solution proposals and discusses their new specifics from auditing and assurance perspective. The identified components of these solutions are placed in the context of norms and requirements.

The aim of the paper is the identification of new tasks and operations in auditing and assurance procedures which should be covered and performed in such environment. Results of the research indicate the growing intensity of security controls and controls on the infrastructure level.

Key words: IT Governance, Industry 4.0, Compliance, Audit, Assurance, ISO, cloud-based manufacturing

1. Introduction

This article summarizes initial results of research in the area of IT Governance specifics in the context of Industry 4.0. Definition of these specifics is one of the support goals of dissertation thesis focused on development and exploration of new economic and valuation methods for IT services. The supervisor of this dissertation thesis is prof. Ing. Josef Basl, CSc. This article was prepared in the course SA_903 - Information Systems Quality Management under the supervision of doc. Ing. Vlasta Svatá, CSc.

1.1 Research Question

What is the impact of Industry 4.0 environments which are based or with the involvement of the cloud-based components on IT/IS assurance and audit?

1.2 Research Method

The current phase is still focused on research on professional literature, actual and recent articles and official publications. Summarized discoveries are base for the definition of more comprehensive starting points.

Regarding this article, the following steps were used:

- Analysis of textbooks related to the field of study and the subject of this research
- Analysis of professional literature and official publications related to the subject of this research
- Targeted searching of relevant published articles and summarization of the recent conclusions in the relevant areas
- Evaluation of cloud providers and their solution of the compliance of the subject of this research
- Definition of high-level approaches to realization in the relevant areas
- Comparison of identified best practices and procedures with needs of realization in the relevant areas
- Summarization of specifics and definition of suggestions on the subject of research

---

1 It is meant audit and assurance
2 It is meant cloud-based environment and/or Industry 4.0
2. Current Status

The area of cloud and applications offered via this model is very broad. The research is focused on cloud-based services usable within Industry 4.0.

2.1 Cloud-based Solutions

The most comprehensive vision of the cloud-based manufacturing is described in the publication (Kubler et al., 2016). It introduces the taxonomy of cloud-based manufacturing with the description of the involved components. This taxonomy is shown in the Fig. 1.

![Cloud-Based Manufacturing Taxonomy](image)

**Fig. 1 – Cloud-Based Manufacturing Taxonomy** (Kubler et al., 2016)

Taxonomy introduces different components which are closely described in the following text. The terms, involved components and technologies were the basis for the additional literature search. Regarding Industry 4.0, there are already defined terms “cloud manufacturing” (Kubler et al., 2016; Tao et al., 2017; Thames and Schaefer, 2016), “cloud-based manufacturing” (Pisching et al., 2015), “cloud-based design and manufacturing” (Wu et al., 2017), and “service-oriented manufacturing” (Tao et al., 2017). The idea and awareness of using the cloud technologies in Industry 4.0 context already exist.

The articles discuss the possibility of the cloud-based components within the Industry 4.0 implementation and their impact on the architecture. The perception of Industry 4.0 in the manufacturing and its key components is summarized in Tab. 1.

**Tab. 1. Discussed terms as part of cloud-involved Industry 4.0** (author)

<table>
<thead>
<tr>
<th>Article</th>
<th>SOA</th>
<th>CPS</th>
<th>Cloud Applications</th>
<th>IoT</th>
<th>IoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Thames and Schaefer, 2016)</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>(Tao et al., 2017)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>(Kubler et al., 2016)</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>(Pisching et al., 2015)</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>(Wu et al., 2017)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

According to the research, any type of pure cloud application is possible from the perspective of all cited articles. There are often mentioned cloud storage applications (Pisching et al., 2015; Tao et al., 2017; Wu et al., 2017), CAD applications (Kubler et al., 2016; Thames and Schaefer, 2016; Wu et al., 2017), analytical applications (Tao et al., 2017; Wu et al., 2017) or ERP applications (Wu et al., 2017). Also, the paradigms CPS (cyber-physical system) and IoT (internet of things) are used. SOA is directly referenced only in three articles, but with the concept of service-orientation is worked also in the rest of articles. On the other hand, the term IoS (internet of services), is used only in one article.

As the important topic is also mentioned the security. Except (Tao et al., 2017), which did not mention this area in the article, all authors perceive the security as a critical issue which must be solved and considered on the architecture level.
2.2 Audit and Assurance

As a starting point for audit and assurance can be referenced (Svatá, 2016). This publication provides an actual overview of principles and best practices in the audit and assurance area. In this publication is also explicitly defined the relations between governance and the audit: “IS audit is closely related to the conception of IT management called Governance of Enterprise IT” (Svatá, 2016). The following levels of the governance are defined:

- Corporate Governance
- Enterprise Governance
- IT Governance

From this perspective, the IS audit is part of the general audit procedures of an organization (Svatá, 2016). As the most important families of norms for IT quality management are listed by (Svatá, 2016):

- ISO 20000 – IT Services Management
- ISO 25000 – IT Quality Management
- ISO 27000 – IT Security

The relevance of these norms for IT Governance and IT Management is confirmed by (Vorisek et al., 2015). In (Svatá, 2016) is also discussed the continuity to other IT management frameworks like ITIL and COBIT. This is elaborated in the diploma thesis (Simetinger, 2012), where the connection between ISO standard families and frameworks ITIL, COBIT, and TOGAF are described. The conclusions are corresponding with (Svatá, 2016). In diploma thesis (Simetinger, 2012) is also provided the conclusion that following of complete reference implementation of these frameworks lead to the compliance with the ISO standards. The analysis of overlaps between standards and frameworks (Vorisek et al., 2015) shows that the COBIT 5 is prepared better for the handling of IT-related risks.

In (Svatá, 2016) the main components of audit and assurance, which should be covered, are defined:

- Main parties (assurance professionals, responsible and accountable parties, and stakeholders)
- Assurance object (policies, information, processes,...)
- Suitable criteria (objectivity, measurability, understandability, completeness, relevance)
- Execution (how the audit is performed)
- Conclusion (scenarios with proposals, suitable solution, necessary steps to be done)

Considering cloud providers which are audited by external auditors, the SOC1, SOC2, and SOC3 reports are important (Svatá, 2016). These reports are defined by International Standard on Assurance Engagements (Svatá, 2016). Leading cloud providers are publishing their compliance using these reports besides the other certifications. As an example are listed the following cloud providers and their levels of compliance:

- Google (“Committed to protecting your organization’s data | G Suite Security,” n.d.)
- Microsoft (“Microsoft Trust Center | Perform a risk assessment and assess the compliance of Microsoft cloud services,” n.d.)
- SAP (“Cloud Certifications and Compliance | SAP Cloud Trust Center,” n.d.)

According to the number of customers of these cloud providers, it is not possible to perform external audits by every customer. In general, the customer must rely on audits done by external auditing companies which guarantee the compliance of the audited provider. There are usually defined the exceptions in the compliance statements and terms of use of the cloud services, when the customers may perform audits by themselves. There are defined cases as the serious security incidents and the costs of such audits are fully paid by auditing customer.

From the perspective of auditee cloud solutions, especially assurance of their security, there is a list of proposals (Mangiuc, 2014):

- Security and protection of cloud-based and cloud-hosted solutions must be far more intensive
More controls must be done by auditors, including completely new procedures suitable for a cloud environment. Auditors must perform physical level security controls, virtualization technology controls, identity and event logs controls. Auditors must perform additional compliance controls according to a region and industry-specific regulations. Audit must be adapted to the organizational cloud environment and corporate network scope.

There are also proposed the adequate norms and frameworks for performing audits in the cloud environment with a focus on IT risks (Mangiuc, 2014):

- ENISA Cloud Risk Assessment – introduced by European Network and Information Security Agency
- FedRAMP – introduced by federal agencies in the US
- COBIT – introduced by ISACA
- Security Guidance for Critical Areas of Focus in Cloud Computing – introduced by Cloud Security Alliance
- The Automated Audit, Assertion, Assessment and Assurance API – introduced by CloudAudit/A6

For comparison, in the article (Svata, 2014), example frameworks designed for use in the cloud are mentioned:

- Cloud Control Matrix (CCM) – introduced by Cloud Security Alliance
- Self-Assessment Scheme (SAS) – introduced by Jericho Forum
- ISACA Cloud Computing Management Audit/Assurance Program
- An Introduction to Securing a Cloud Environment – introduced by SANS Institute

The publication (Svata, 2014), also mentions three approaches to the execution of the assurance:

- Risk-based assurance
- Regulation-based assurance
- Balanced Scorecard (BSC)-based assurance

There are mentioned the frameworks COSO, ISO 27001, ITIL, Risk IT, and COBIT as focused on Risk-based assurance scenario (Svata, 2014). The compliance with ISO 27001, SOX, COSO and other requirements is highlighted in COBIT by (Mangiuc, 2014; Svata, 2014).

Discussion about importance and need of new elements in SLA (service level agreement) is in (Rizvi et al., 2017). The publication summarizes the recent research about the development of SLA and also introduces new methods for measuring the QoS (quality of service). At the same time, the publication highlights the need for auditing the real availability of service on both sides – on customer’s as well on provider’s side. The same author in different publications (Razaque and Rizvi, 2017, 2016) elaborates new approaches of stakeholders authentication and incorporation of these new methods into the SLA. Publications (Razaque and Rizvi, 2017, 2016; Svata, 2014) define three types of stakeholders:

- CU (Cloud User)
- CSP (Cloud Service Provider)
- TPA (Third-Party Auditor)

This method is called “Triangular data privacy-preserving model” (Razaque and Rizvi, 2016) and it ensures proper storing of sensitive data and its transparent auditing. The main responsibilities of TPA are auditing of violations of CPS policies, and auditing of CSP services (Razaque and Rizvi, 2017).

From the cloud perspective, the CSP stakeholder can be diversified into two different assurance relevant sub-stakeholders (Svatá, 2016):

- The user of assurance outputs = the person who manages the business processes
- Responsible party = the person who delegates own responsibility for compliance to another person who really ensures the compliance on assurance object level
The Identity Management topic is also elaborated in (Mangiuc, 2014) where are described possible issues and risks related to the migration to cloud and following integration with Identity Management system (like Active Directory or LDAP).

Literature research conducted in this part indicates the preference of COBIT as the main reference framework for audit and assurance. COBIT is mentioned in the majority of referenced articles, conference papers, and literature. It is possible to accept risk-based approaches preference in the cloud-environments because measures against new and existing risks are at the center of interest of the referenced works. According to this conclusion, COBIT is used as the reference framework for the analysis of cloud-manufacturing specifics for audit and assurance in the following text.

3. High-Level Implementation

According to the research in the area of cloud-based solutions, cloud-based manufacturing, the reference architecture for these solutions can be identified. As it was mentioned in the previous part, the publication (Kubler et al., 2016) introduces the taxonomy of cloud-based manufacturing with major building blocks.

3.1 Cloud-Based Manufacturing Taxonomy

The taxonomy described in (Kubler et al., 2016) consists of the following main components:

- **Cloud Computing** – this component brings reliability, elasticity, scalability, and disaster recovery in the flexible and cost-effective way; it is highlighted the importance of using the open standards for communication and tendency to use IoT messaging standards for achieving the Systems-of-Systems integration
- **IoT** – this component represents communication endpoints based on REST and Open API; it is highlighted that a large number of IoT devices generates a huge amount of data, and only some decisions can be done locally, the involvement of cloud is then an alternative how to handle operational decisions effectively and efficiently
- **Product Centric Control** – this component processes, assembles, and handles materials and products; it is the central point of the whole cloud-based manufacturing solutions, it is able to recognize every product and it adaptive according to provided data, it allows to develop new DDM solutions
- **DDM (Direct Digital Manufacturing) with 3D Modeling and 3D Printing** – this component produces parts according to the provided digital model; this flexible tool for production decreases time-to-market with maintaining low costs and high efficiency because 3D printers are managed via cloud and it is decided during modeling and production which location will be used for printing

3.2 Service Oriented Architecture

As it is described in previous part, it is expected that IoT component will communicate using REST and Open API (Kubler et al., 2016). As it is mentioned above, using of SOA is accepted by more authors (Pisching et al., 2015; Razaque and Rizvi, 2016; Tao et al., 2017).

SOA is recognized as an answer to needing communication between different platforms, systems, appliances, etc. On the other hand, the SOA requires complex administration and it is resources demanding. Also, SOA is sensitive to the quality of SOA Governance. SOA Governance exceeds into the IT Governance and it is critical to the success of the whole solution (Simetinger, 2012). At the same time, it provides the required flexibility and representation of IoT appliances is “natural” for SOA services and according to standards, SOA services should be designed natively with defined SLA (Simetinger, 2012).

As is described in cloud-based manufacturing taxonomy, it is supposed that IoT appliances communicate inside the organization (with product centric control), but also outside with cloud services. It requires additional security measures because endpoints which represent IoT appliances must be protected as any other endpoint available from outside of the organization.

Last, but not least, considering the proposal described in (Kubler et al., 2016), communication should be based on messaging. It will create new requirements for cloud-services providers for securing of their messaging systems.
3.3 Cloud Applications and Services

As it is described above, it is possible to consider various cloud-based applications and services involved in the cloud-based manufacturing solution. According to citation analysis, there are derived three possible basic scenarios with different levels of risks:

- Cloud storages and applications (CAD, Office, and similar) – this scenario supports collaboration and sharing of the information; as is described in (Wu et al., 2017), in the case of CAD, the main goal is to provide universal access to designs and eventually size an opportunity to use the HPC computing infrastructure.

- Analytics – this scenario sends data from IoT appliances for future processing and reporting; because analytical applications are sensitive to data quality, it is needed to provide continuous access of IoT appliances and other critical components to such application like BI engines, data warehouses, data marts, etc.

- ERP type application – this scenario uses cloud-based services for deeper coordination, handling, and management of the whole solution; it is required highly reliable communication line with the cloud application because without this access, the whole solution is not able to operate or it can operate only in some limited regime.

The defined scenarios represent the levels of integration and following dependency of the cloud-based solution on cloud services and applications with different requirements to the agreed quality of service and security.

4. Audit and Assurance Perspective

As it was mentioned in the text above, according to results of the relevant literature research and review, it is possible to accept COBIT 5 as a basic framework which can be extended in terms of cloud-based manufacturing (Industry 4.0) specific needs. COBIT 5 is mentioned in a majority of cited articles related to the audit and assurance, and it is covered by respected independent international organization ISACA. As dimensions for extensions can be used the components proposed by (Svatá, 2016) because they represent the agreed domains of interests.

Based on the partial conclusions from the previous parts, the proposed components may be extended in the way described in the following text.

4.1 Main Parties

Cloud User party is affected especially by the information security direction. According to the actual trend of new norms (for instance in European Union Data Protection Directive (DPD) (Svata, 2014) or General Data Protection Regulation (GDPR)), it must be ensured that users are informed about the new requirements and they are able to provide all necessary approvals and changes as it is defined in these new norms. In other words, the cloud services, if it is needed, must be designed in the way that the users are able to perform all tasks with their personal and sensitive data as defined by the legal norm. Of course, it is needed the possibility to prove that all users are in compliance with all regulations (for instance via application logs analysis (Svatá, 2016)).

Cloud Service Provider party is affected by new risks and growing importance of SLA. As it is mentioned in the previous text, identity management, infrastructure and application/endpoint security, and quality of service monitoring are crucial. The cloud environment is risk-based, so new scenarios must be prepared. These new scenarios should reflect the following traits:

- Number of users – as the number of users is higher, the security risks and requirements for the automation of compliance monitoring are higher.

- Quality of service – the guaranteed availability of service must be demonstrable; as it is mentioned in the text above, the guaranteed availability is audited on the side of provider and on the side of the consumer as well.

- Security – according to the industry, it can be required particular tier of data centers or their location and disaster and recovery policies, networking security standards, and application security; completely specific group is security monitoring of endpoints because in a hybrid cloud environment the endpoints are contact points between consumers and providers of services.
All these traits are defined in SLA and cloud service provider must accept the appropriate measures how to sustain them. SLA may define specific norms and then these norms will be required in a report from the corresponding audit.

Third-Party Auditor party is affected by the Cloud Service Provider relevant legal and industry required norms, specific scenarios, and other agreed norms. In fact, in the case of hybrid cloud environment (and specially Cloud-Based Manufacturing and/or Industry 4.0 environment) it may extend the scope of audit and assurance projects significantly. On the technical level, the checking of norms which are related to the production lines may even require the involvement of specialist and professionals who are able to check the compliance of specialized devices, appliances, equipment, and software which operates these components. It is also possible that involvement of specialists from cloud service provider on the consumer’s side will be needed. On the organizational and process level, SOA Governance processes and tasks (if they are applied and used) should be also under the scope of the audit because they directly affect the overall quality of information system. From this perspective, the security of the endpoints is important and related processes and tasks are the objects of the interest.

4.2 Assurance Object

Assurance object depends on the side where the audit is performed. If the audit is conducted on the side of Cloud Service Provider, it means that the goals are to evaluate the compliance with the norms presented in their level of compliance. Usually, it means SOC1, SOC2, and SOC3 reports, ISO norms from families 9000, 20000, and 27000, and other norms which can be required by agreement in SLA or in another contract.

4.2.1. Assurance Objects on the side of Cloud Service Provider

From assurance object perspective, the audits on the side of Cloud Service Provider involve all common objects like general controls, application controls, software development controls, and infrastructure security controls. In the context of cloud and Industry 4.0, three assurance objects have the increased importance – general controls, application controls, and infrastructure security controls.

As it is described in (Svatá, 2016), general controls are focused on the adequacy of tasks like change management, backup and recovery strategies, planning, and organization of IT. In this case, the general controls scope should be extended by relevant SOA Governance processes and tasks affecting the lifecycle of services and their operations. It is described in (Simetinger, 2012), these processes ensure the continual availability of services and continual improvement via monitoring and assessment. These processes and activities then represent the main extension of general controls as assurance object on the side of Cloud Service Provider.

Application controls are focused on the condition of the applications as security, data management, and data quality management (Svatá, 2016). This assurance object is mainly affected by agreed SLA. The extension depends on agreed additional parameters as it is described in the text above. For instance, if the cloud user requires (agreed with provider) some very specific norm important for running their production line, during the audit it must be ensured that the application which communicates with the production line (manages it, monitors it, analyzes it, etc.) is able to be in compliance with agreed norm. This assurance object is also affected in the case of special security measures within the cloud-based manufacturing, if the cloud-based service handles the automated designs of products for the production lines, it can be expected higher requirements for security from the side of cloud user. And additional possible extensions can be derived to every possible element in Industry 4.0 like IoT or IoS which are bringing completely new norms with themselves.

Infrastructure security controls are partially related to the previously described assurance objects. These controls are focused on the infrastructure elements like firewalls, networks, applications, and others (Svatá, 2016). As it is described in the previous text, cloud-based manufacturing and Industry 4.0 may require a connection on the application level via endpoints. It creates new requirements on the security of the infrastructure where multiple zones for different use cases should be available. It is important to balance the performance and security measures like encryption, data validation, etc. Activities and checks of these specifics are the extensions of this assurance object. During the audit, these areas must be involved in the defined scenarios or there must be defined new scenarios with risks related to the described specifics.

4.2.2. Assurance Objects on the side of Cloud User

Assurance objects are affected differently on the side of Cloud User. There are important the same assurance objects, but there are a convergence and overlapping of objects. In the case of the
involvement of cloud services in the infrastructure of Industry 4.0 applications or even cloud-based manufacturing, high reliability is required. So, from the audit perspective, the services and operated applications on the side of cloud user area audited in the manner of more assurance objects at the same time. There is also the presumption, that it is a common audit and not exceptional. It means, that the cloud user relies on official auditing and assurance reports done by the third-party auditor on the side of cloud service provider.

As the main three scenarios were derived (according to literature analysis above), the cumulative tendency of audit scope (and involvement of more assurance objects) can be described. The first scenario describes using cloud storages and applications. This scenario is in the center of general controls assurance object. In this case, the audit should check the ways and operations which are done by users in the subscribed applications. The question of the security is on the processes and policies level (for instance the restrictions as using the USB sticks on the workstations and so on) which are under the responsibility of general controls. The main extension of general controls assurance object is the definition of the scenarios related to data manipulation on workstations and related areas like internal identity management and internal security policies for users.

The second scenario describes continual IoT appliances access to the subscribed analytical applications. In this case, the assurance object infrastructure assurance controls are added to the scope of the audit because there is a risk of exposing the internal endpoints (IoT interfaces) to the attackers. And in other direction, the cloud service provider may have access to the internal systems of the cloud user (though only reading). New scenarios may involve additional security measures like using VPNs (virtual private networks), secured and encrypted tunnels between endpoints, security communication arrangement policies and so on. On the other hand, it also important the monitoring of the subscribed services if they are conforming with the agreed SLAs. The main extensions are then these processes which ensure the security protocols, procedures and standards, and at the same time they are providing the agreed level of the quality because the deviations in the availability may affect the production optimization.

The third scenario describes the transfer of significant part of business logic into the cloud-based complex application like ERP. In this case, software appliances on the side of cloud user are perceived as agents of the main application in the cloud and they are more less dependent. This scenario is the most difficult and the scope must be extended across all rest assurance objects – application controls and even software development controls. In the current situation, the agents developed and implemented on the side of cloud user are still quite specific and if the software is purchased, there is a probability that individual changes are needed. It creates new requirements to audit. It must be ensured compatibility of technologies and protocols, compatibility with security standards, ability to keep production in some controlled state if the connection to main application in the cloud is lost, adequate performance to the performance of the subscribed service in the cloud, and other similar. These requirements derive new scenarios related to the data manipulation, the decision about the chosen technology, deployment scenarios, testing procedures, documentation of the application architecture, and many other scenarios which describe application checks in the hybrid-cloud environment.

4.3 Suitable Criteria

Suitable criteria can be derived from assurance objects described in the previous part. As the starting point can be perceived the SLA with all conditions, quality of service, standards, and other agreed properties and traits of subscribed services. In the case of Cloud-Based Industry 4.0 Environment, SLA represents more than “service level agreement”. Especially in the derived third scenario, the SLA describes what exactly is expected from Cloud Service Provider by Cloud User including detailed implementation technical details and scenarios how the subscribed services are used.

As it was mentioned, the Cloud Service Provider must demonstrate the compliance by the publishing of audit results in the level of compliance of the provided services. So, in the case there are some individual extensions of the SLA, the Cloud Service provider should provide to the Cloud User the results with a description of compliance with these extended parameters.

In the case of Cloud User, the criteria depend on the scenario. In the first scenario, the results of a regular audit from Cloud Service Provider and common audit on the side of Cloud User defines the criteria without any significant deviation from the standards. On the other hand, second and third scenarios bring new areas which must be checked. According to the presumption, SLA can be the starting point because it defines the extended and required parameters. Then the suitable criteria are
corresponding to the assurance objects. It should be required the compliance with security standards, technical standards, data manipulation policies, the performance of agents, communication infrastructure and communications channels, disaster and recovery policies. But the exact number and shape of the suitable criteria depend on the scale of integration of cloud-based services.

4.4 Execution

As it was mentioned above, in the case of Cloud-Based Industry 4.0 Environment, the execution of the audit requires the involvement of other specialists who are able to assess the technical compliance of resources. The impact to the execution on the side of Cloud Service Provider is not such significant as on the side of Cloud User. With the presumption, that the Cloud Service Provider must conduct audits regularly, the extension in the way as it is described in assurance objects parts does not requires huge changes in the process.

On the other hand, the audit of Cloud-Based Industry 4.0 Environment on the side of Cloud User will be more complex and it may require the coordination and cooperation with the Cloud Service provider and may lead to the increased costs of the audit. The recommendations for the audit execution are corresponding to the cumulation of the assurance object as it is described in the previous part. It means the audit should be diversified into the phases according to the applied scenarios with the same cumulative logic – start with the audit common audit corresponding to the first level and then continue with the more specialized audit with different audit team members (for instance mentioned technical specialists who are able to assess the specific technology). The diversification to the phases has another advantage and it is higher flexibility. It is possible to adjust the controls and time schedule to the particular assurance objects involved in the applied scenario. If some very specific norm is required (for instance industry specific), the separated audit focused on such norm is convenient to conduct. Also, in the more extensive implementations, it can be beneficial to arrange a permanent audit team for technical audits (focused on technology and standards compliance) and those audits conduct as internal audit only.

The complexity on the Cloud User side is deeply described in the (Nurhajati, 2016). This publication highlights the task needed during compliance checks. From an organizational point of view, methods for transforming business goals to the policies which are applied across the IT processes are important for assurance execution. It includes the methods of checking the vendors and suppliers of cloud-based services if they are able to be compliant with required norms and policies. From a technical point of view, during the assurance execution, the workflow and service orchestration implemented on the Cloud User side must be checked, if they are in compliance with norms and policies. The conclusions in (Nurhajati, 2016) support the previously mentioned principles and other conclusions of this work like increased effort on the side of Cloud User or the idea of creating the specialized internal team.

4.5 Recommendation

As was mentioned in the previous parts, the specifics are depending on many factors. From the perspective of Cloud Service Provider, not much changes are expected and it is also valid for the audit report. In fact, according to the presumptions, it is expected that the compliance of individual extensions of the SLA, will be reported in the form agreed between Cloud Service Providers and Cloud User.

On the different side, on side of Cloud User, the situation is different. There should be designed appropriate reporting tools and documents which help with the compliance statement. For instance, in the case of the compliance with technology and security standards, the matrix “SLA parameters/operated agents” can be used. In the case of the compliance with disaster and recovery policies, the description of policies and processes must be provided and the compliance confirmed by in the audit report. Development or internal modifications of the agents deployed on the side of Cloud User should be audited in the common way when the documentation and testing protocols are properly stored well maintained across the whole life cycle of the agent.

In general, all extensions are based on some existing type of the audit. It means that there is an appropriate part which describes the level of compliance in the recommended audit report template. It means that individual audit report can be created as combination standardized templates which are corresponding to the checked assurance objects.
5. Conclusion

Industry 4.0 with the involvement of cloud-based components, called cloud-based manufacturing solutions, brings new opportunities for increasing productivity, efficiency, effectiveness, and innovative products. At the same time, it represents new threats corresponding to the nature of such solutions.

According to the performed research, there are described specifics related to cloud-based manufacturing solutions and suggested extensions of main components in COBIT 5 audit and assurance framework. Considering these suggestions and their incorporation in auditing and assurance routines, the identified risks can be mitigated or eliminated.

Main proposals are in the components Main Parties and Assurance Object. These two components are affected in terms of scope, new tasks, and new objects of the interest. The extended Assurance Objects are then SLA forming factors which affect the other components.

As the secondary discovery is the difference between impact to the auditing routines on the side of Cloud Service Provider and Cloud User. Is it possible to state, that Cloud User carries the main increase of the audit difficulty because in the Cloud-Based Industry 4.0 Environment a lot of new checks are required on the side of Cloud User.

References


JEL Classification: L00, M15