Published in Proceedings of 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), 17-20 December 2018, Zürich, Switzerland, which should be cited to refer to this work.
DOI: 10.1109/UCC-Companion.2018.00030

Security Governance as a Service on the Cloud

Ciarán Bryce
Geneva School of Business Administration – HES-SO
University of Applied Sciences and Arts Western Switzerland
Ciaran.Bryce@hesge.ch

***Abstract*—The increasing number of security attacks is placing organizations in difficulty, especially SMEs. Their workload is exacerbated by information handling obligations imposed by insurance companies as part of cyber-insurance contracts, and by regulations like the GDPR. An emerging possibility is for security and compliance to be provided as a cloud service that SMEs can connect their IT infrastructure to. The advantage of the cloud is that competence can be outsourced outside of the company, and that a cloud provider can act as a trusted third party when the company is audited for compliance or following a data breach.**

***Index Terms*—Compliance, security, security as a service, cloud, business process modelling, burden of proofs.**

I. Introduction

Cyber-security is an increasing challenge for large and small organizations as attacks like crypto-mining, phishing, DOS, ransomware, etc. continue to grow. The challenge is particularly important for SMEs since they can lack the expertise and resources to defend themselves correctly. Cyber-insurance contracts have appeared recently in some countries, but these contracts require that companies prove they are taking the necessary precautions to defend themselves. SMEs require help for this in a manner that minimizes the required investment.

Frameworks like the ISO/IEC 27001 series [6] were devised to help companies improve their cyber-defense. These present procedures and processes for prevention, detection and recovery. These frameworks are not intended to offer bullet-proof security, but help by creating a company culture where security risks are managed. However, these are informal frameworks, and automated help is required for security to be implemented effectively and at low cost.

In addition to protection of information, companies are increasingly under legal obligations concerning data management. One example is the European Union's *General Data Protection Regulation* (GDPR), that came into effect on May 25th 2018 [13]. This obliges companies to enforce processes for acting on requests for customer data erasure, requesting consent, reporting data breaches, etc. The GDPR is the most pressing compliance example compared to IPAA in the health domain [1] and Dodd-Frank in the finance domain, since it applies to all sectors of the economy.

We propose a framework for implementing compliance and security processes as a cloud service. A user company defines formal processes for security (prevention, detection, recovery) and compliance. These processes are modeled using BPMN 2.0 (Business Process Model and Notation language). The language is extended with **burdens of proof** elements. At runtime, these elements collect evidence of implementation of security/compliance to high-level management and external parties (auditors, insurance providers, . . .). Figure 1 shows a simple process that applies a software patch and restarts the server. Evidence of applying the patch is collected after installing – this is used to demonstrate *a posteriori* that patches were installed.

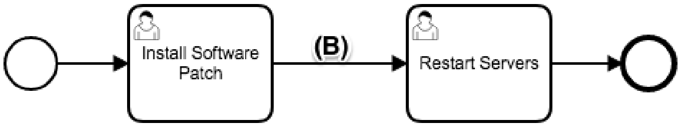


Fig. 1. BPMN Example with Burden of Proof

The advantage of a cloud solution is that the security competence required might not exist within the company, so outsourcing is necessary. Further, the cloud provider can act as a trusted third party concerning the status of the company's processes. This can be important when the company is audited for compliance or following a data breach.

This paper motivates the cloud-based model for governance security, and examines its design and implementation. The remainder of this paper is organized as follows. Section 2 motivates the need for a governance model. The model is presented in Section 3, and its implementation in Section 4. Related work is presented in Section 5, and conclusions and future work are discussed in Section 6.

II. Security and Compliance

Organizations must adopt the mindset that security attacks will happen and that some will succeed in causing damage like data loss. Even the best prevention techniques can be short-circuited by zero-day exploits. This has two implications. First, effort must be equally spent on cyber-attack prevention (e.g., employee screening, patching software, etc.), attack detection (firewall and anti-virus software installation, security awareness cultivation, etc.) and recovery (e.g., managing information backups, business continuity planning, etc.). Second, organizations must dispose of a means to demonstrate that they are taking the necessary protection steps to auditors, clients and management to prevent litigation in the event of a data loss. Thus, an organization must implement a number of *processes* for security.

The design of processes for security and compliance involves IT, management and legal. Management decides on the resources that need to be protected and on the minimum services that need to run before the disaster recovery plan is put into operation. Legal is needed to define and verify controls on data handling. Even a task as seemingly "IT" as using anti-virus software relies on organizational procedures. That is, management must define who can install the anti-virus software, who can deactivate or update it, the choice of anti-virus provider. Management must also ensure that the anti-virus software is being used by employees. Legal must verify that the software provider is furnishing updates to its malware database and releasing fixes for its own bugs. Without these processes, the anti-virus software is not as effective as it could be. In general, the collaborative nature of policy design requires that policies be expressed with clear descriptions of responsibilities and in a manner understandable to all stakeholders (IT, legal, management).

While processes for security, compliance and insurance are designed to help organizations, these need to be implemented effectively since otherwise a new risk is created for organizations.

- From a security standpoint, as well as being a target of an attack, a company can inadvertently be the source of a security attack. For instance, an attacker might place botnets within the IT infrastructure of Company A. Sometime later, these botnets are used to participate in an Internet attack on Company B. In this case, Company A might be considered liable for the attack, if the security measures put in place are deemed insufficient to avoid the original botnet attack.
- Under the GDPR, the penalties for a poorly managed security process that leads to a data loss are very high[1]. Thus, the onus is on the company to ensure the effectiveness of its security process.
- From the cyber-insurance policy standpoint, an insurance company can refuse to pay for damages if the security process is deemed ineffective.

In all of these cases, organizations need assurance that the processes they implement are effective. Assurance is needed for management, or for external entities like governmental auditors verifying compliance to regulation or insurance companies verifying implementation of contractual security procedures. Further, since a company is obliged to demonstrate implementation, the participation of an independent party can help. One way to achieve this is to offer security and governance as a service that runs from the cloud. This paper presents the design and implementation of such a service.

III. The Security and Compliance Model

The architecture of our model is presented in Figure 2. Security and compliance processes run on a process server on the cloud, to which the client IT infrastructure is connected.

There are two layers to the model. First, we use BPMN 2.0 to model all processes that are used for security and compliance. In a second stage, we extend BPMN with *burden of proof* annotations that collect proofs of process implementation for management or auditors.

A. Process Modelling Library

The Business Process Model and Notation (BPMN 2.0) language is maintained by the Object Management Group. The primary purpose of the language is to model business processes and activities [9]. Note that "business" is a generic term that applies to any organizational activity. The language was motivated by the need for a specification language that is accessible to IT and non-IT personnel alike, which is a major departure from earlier specification languages like UML [14]. This argument is particularly relevant to security and compliance since the specification of security policies and their enforcement depend on end-users, IT administrators, management, legal and HR.

A simple BPMN process is modelled in Figure 3. Without going into too much technical details, the boxes represent steps of the process. These include manual tasks (e.g., localization of IT systems), script tasks (e.g., erasure of data) or form tasks (e.g., creation of data deletion request). The horizontal bars are *swim-lanes* that represent who can execute the tasks contained within. In this example, only a company designated *operator* is allowed to list the IT systems where data needs to be removed. The circles represent events – in this example we see the process start and end events. Finally, the diamond shapes represent *gateways* which encode decision logic. In this example, a decision on the validity of the request is made before the erasure can take place.

However, BPMN is not just a modeling language. Many software engines exist for executing BPMN process descriptions, e.g., Camunda[2], Bonita[3], jBPM[4], etc. Many commercial implementations exist also. BPMN engines have had great success in industry for workflow applications like supply-chain management and client on-boarding in financial institutions. Also, the Swiss government has mandated that BPMN 2.0 be used to document public service processes.

The first stage in our framework is to model key security and compliance processes in BPMN, and to store these in a process library. Processes from the library may be reused in different organizational contexts as companies tailor them to their specific needs. Note that even this simple BPMN model is progress compared to the current state of affairs since the BPMN process descriptions are formal and precise descriptions of the tasks that need to be done for security and compliance. More clarity is provided compared to the verbose explanations in IEC/ISO 27000 as BPMN descriptions offer guided implementation steps. Organizations can measure progress of security and compliance implementation by the number of processes in their library and by their execution states.

As illustrated in Figure 2, the process is run in real-time in parallel to the real-life business process. Process task

[1] Up to 4% of worldwide revenues or 20 MEuros.

[2] http://camunda.com

[3] www.bonitasoft.com

[4] www.jbpm.org

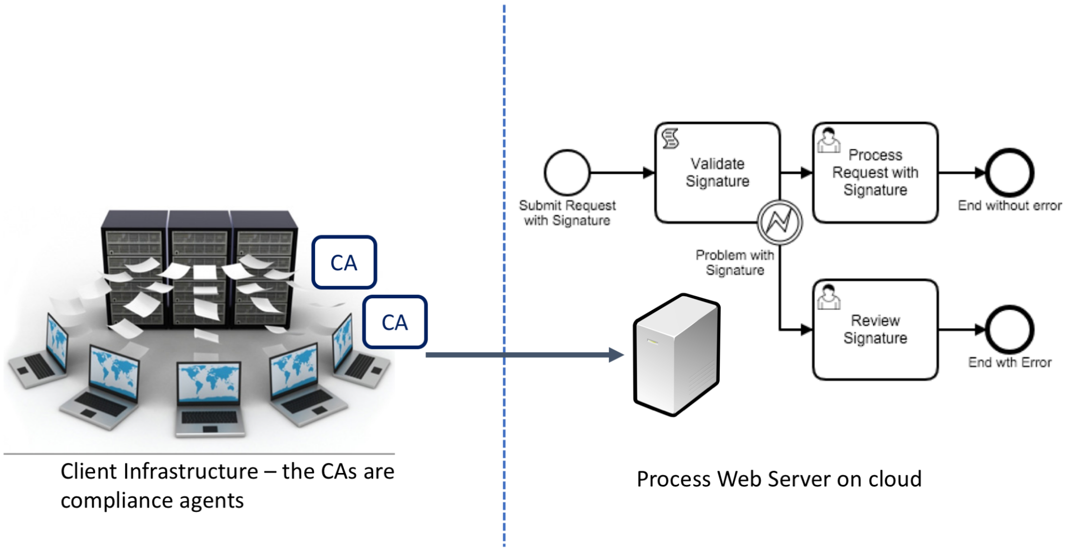

CA
CA
Client Infrastructure – the CAs are compliance agents
Submit Request with Signature
Validate Signature
Process Request with Signature
End without error
Problem with Signature
Review Signature
End wth Error
Process Web Server on cloud

Fig. 2. Processes run on engine in a trusted environment

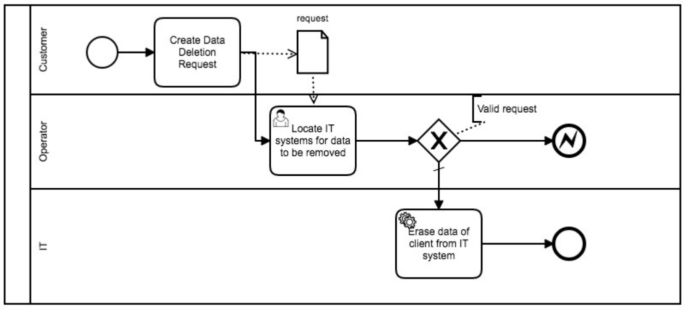

Customer
Operator
IT
Create Data Deletion Request
request
Locate IT systems for data to be removed
Valid request
Erase data of client from IT system

Fig. 3. BPMN Process for Data Deletion

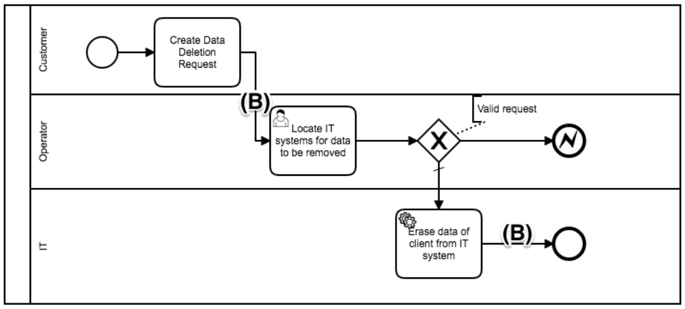

Customer
Operator
IT
Create Data Deletion Request
(B)
Locate IT systems for data to be removed
Valid request
Erase data of client from IT system
(B)

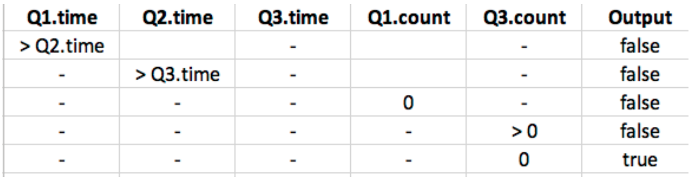
Fig. 4. Data deletion process with BoPs

completion is represented by the responsible user, who is the named participant of the swim-lane, logging into the system and making a request to the process engine. The process engine is run from the cloud, and thus administratively isolated from the organization's IT system. Process instance state (task execution, times, etc.) are securely stored on this server.

B. Burdens of Proof

Recall that the primary goal of our framework is to help demonstrate that processes are being implemented, and consequently security and compliance are being enforced. We extend the BPMN model with annotations called **burdens of proof** (BoP). These are a form of intermediate event within a process. A BoP acts as a synchronous rendezvous point; process execution can only continue once evidence has been provided to a burden of proof and then validated. Figure 4 shows the example process from earlier annotated with two burdens of proof.

The organization's security policy officer associates a **policy** with a BoP that defines the evidence that must be furnished to the BoP for it to allow process execution to continue. This policy is expressed using *Decision Model Notation* (DMN), and an example is shown in Figure 5. DMN is a notation for decision modelling from the Object Management Group. Each decision is represented by a table, with input arguments and corresponding outputs. Decision tables can be placed in a tree structure to represent the outcomes of one decision being used as inputs to the parent decision table in the tree.



Q1.time	Q2.time	Q3.time	Q1.count	Q3.count	Output
> Q2.time		-		-	false
-	> Q3.time	-		-	false
-	-	-	0	-	false
-	-	-	-	> 0	false
-	-	-	-	0	true

Fig. 5. DMN Decision table for data deletion process

The example policy in Figure 5 specifies evidence needed for demonstrating that a data deletion request has been executed. Under the GDPR, a company must be able to respond to such a request. One can verify compliance with this request through three database requests. Query Q1 is issued before the actual deletion, and is a select query on the DB for the specified client data. Q2 is the deletion request, and Q3 is the select query again, which this time should return empty data.

The data input to the policy decision are the times of the three requests and the count (i.e., number of results) from the two SQL select statements. There is a column for each input value and a row for each policy configuration. In this policy, we tell the BoP to allow process execution to continue only if the select count of Q3 is zero (Row 5). We note that if the requests are not ordered correctly (Rows 1 and 2), then the proof validation fails. Similarly, if the first request did not find the client data (Row 3) or the delete request did not remove the client data (Row 4), then the validation fails. The syntax of the cell expressions is defined by the tools we use in our implementation[5].

The evidence document is transferred to the process engine by a **compliance agent** deployed in the organization's IT system. The compliance agent is specifically programmed to collect the data required by the BoP. For the data deletion request, the compliance agent runs the three certified DB requests to extract the data. Compliance agents are represented by the boxes in Figure 2. The execution of a compliance agent is triggered from the process portal page where a user finds the list of tasks he has to execute.

C. Threat Model

The underlying requirement for the model is to help an organization implement security and compliance processes, and to furnish proof that process steps are being taken. For the latter, a process instance validates documents (evidence) sent from a compliance agent. The documents are then stored within the trusted confines of the process engine.

Being on the cloud, the process engine is considered to run in a trustworthy environment since it is outside of the organization's boundary (purview of the organization's IT administrator). Nonetheless, agreement is needed between the company and process engine provider about data exchanged in burden of proof documents. For instance, documents containing personal data falls under the jurisdiction of the GDPR.

The compliance agent must be protected from tampering so that evidence is not fabricated. Currently, we run them as *setuid* enabled programs on our Linux platforms, where the user identity attributed to the programs is that of an administrator of the process platform. The only drawback is this does not handle the threat of a malicious IT administrator. There are two possibilities to addressing this shortcoming:

- The compliance agents run in their own protection domain. The Intel SGX (Software Guard Extensions) mechanism allows user code and data to be placed within a memory *enclaves*. Enclave memory cannot be directly accessed by code running in kernel mode. This means that we can run code that is safe from manipulation by kernel-level code, and thus, safe from manipulation by malicious administrators. An example of its use for secure databases is presented in [7]. We intend to investigate this possibility as future work.
- A more "organizational" solution is to put in place a process where an external auditor oversees the installation of the compliance agents at the company site, and where the contract stipulates that the auditor may conduct regular checks concerning the functioning of the agents. This approach is analogous to that taken by insurance companies in relation to fire safety equipment in buildings. The advantage of this approach is the processes implementing these can be specified within the model – BPMN processes with burdens of proof. An example installation process is shown in Figure 6. Two burdens of proof are added: the first requires evidence of the creation of the compliance agent, the second requires evidence of the compliance agent's installation. Evidence for the first BoP would include the code for the compliance agent containing the HTTP call to the process platform and the signature of the program corresponding to that of the security policy administrator. Evidence for the installation BoP would include the (/usr/bin) directory containing the compliance program.

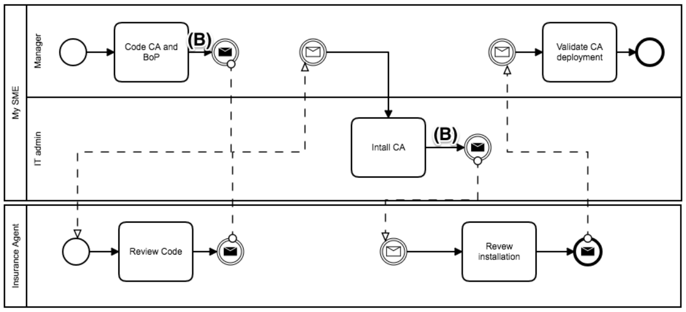


Fig. 6. Installation process for compliance agents

IV. Implementation

We use Camunda's community edition[6] as the process engine of our platform. As shown in Figure 7, Camunda supports BPMN 2.0 and DMN 1.1. Camunda is an open-source platform and is one of the leading BPMN platform providers today. The platform has a REST interface for manipulating process descriptions, process instances, variables and users. Camunda is packaged as a servlet and we run it over an Apache Tomcat Web server container.

For the process platform, the choice was made to use customizable off-the-shelf components. Our process environment runs in parallel to the Camunda/Apache server over a MERN stack (MongoDB, Express, React and Node). This environment manages the process descriptions, with a link to an editor for creating and editing descriptions. It also contains a portal, see Figure 8, with a list of the current process tasks that a user has to execute. The user executes tasks from this portal. He can also activate compliance agents from the portal,

[5] We are using the Camunda platform (www.camunda.com) which supports DMN. This implementation supports JUEL (Java Unified Expression Language) and FEEL (Friendly Enough Expression Language) expressions in cells.

[6] www.camunda.com

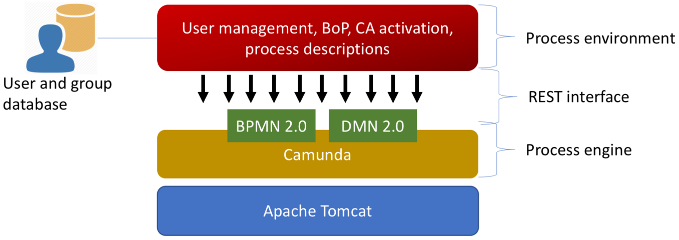


Fig. 7. Process Platform Stack Architecture

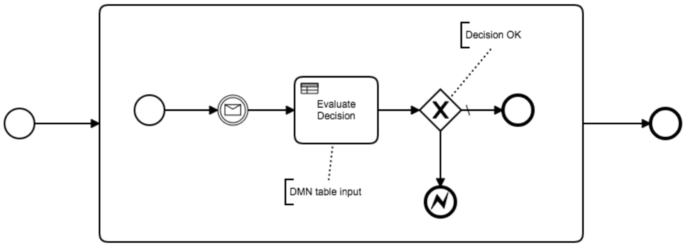
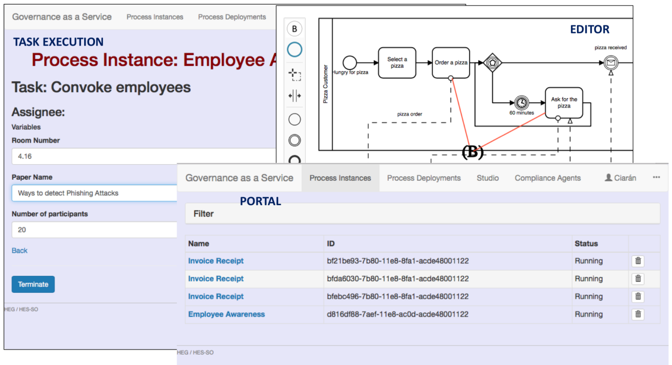


Fig. 9. Implementation of the BoP element

the role of which is to collect and send evidence from the IT platform to the process environment. This uses Camunda's REST interface to control processes.



TASK EXECUTION

Process Instance: Employee A

Task: Convoke employees

Assignee:

Variables

Room Number: 4.16

Paper Name: Ways to detect Phishing Attacks

Number of participants: 20

Name	ID	Status
Invoice Receipt	bf21be93-7b80-11e8-8fa1-acde48001122	Running
Invoice Receipt	bfda6030-7b80-11e8-8fa1-acde48001122	Running
Invoice Receipt	bfebc496-7b80-11e8-8fa1-acde48001122	Running
Employee Awareness	d816df88-7aef-11e8-ac0d-acde48001122	Running

Fig. 8. Screenshots from the Portal

Compliance agents are deployed on the side of the client organization site. These programs can take any form, but they must make an HTTP call to the process engine to transfer evidence to the BoP. In our prototype, we have coded compliance agents as bash scripts that, for protection reasons, are setuid programs so they can be called by any user and run with the privileges of the process platform administrator. At the same time, they remain protected from non-admin users. This user is in the sudoer group so he has access to system files. As mentioned, a compliance agent gets triggered from the process environment portal. This requires that an *Agent daemon* run in the organization's that receives requests for compliance agents and launches them.

A BoP element can be implemented using existing BPMN components. Each BoP is transformed into the sub-process task shown in Figure 9. One of the task types supported by Camunda is a *Business Rule Task*. This task evaluates a DMN decision table. In our framework, the BoP's policy decision table gets linked to the business rule task. The policy outputs true or false, depending on the evidence provided. A negative decision leads to the BoP generating an error event. Finally, the BoP gets triggered by a receive message event. This is triggered by a message sent from the platform, which in turn is triggered by the HTTP request made by the corresponding compliance agent in the client IT system.

In the processes, swim-lanes have users (or groups) assigned to them that represent who has the responsibility of executing tasks in the swim-lane. As suggested in Figure 7, we took the option to have a separate user database to the client IT system to maintain independence from administration of the client IT system. Thus, we create user accounts for all users and maintain these. Most IT infrastructures today use LDAP or Active Directory (AD) to maintain their database, and the Java Authentication and Authorization Service (JAAS), which Tomcat implements, does allow us to use LDAP/AD for authentication if we decide in the future to support a tighter integration model between process environment and client infrastructure.

V. Related Work

Governance in computer security and compliance is still regulated in a manual, procedural manner through frameworks like the ISO/IEC 27000 series [3], [6]. These are information system management frameworks that offer guidelines to companies on strengthening their information security. Some larger companies have acquired ISO/IEC 27000 certification, but this is a long process which can be very expensive. ISO/IEC 27000 certification is not accessible to SMEs for these reasons. Ideally, companies should be able to follow ISO/IEC 27000 guidelines without certification. The conjecture of this paper is that automation of the processes described in Appendix A of the 27001 document is the only way for the security processes to be effectively implemented within companies.

The *Cloud Security Alliance* (CSA) provide a definition of Security as a Service (SecaaS): a cloud infrastructure that provides security services such as identity management, data loss prevention, Web and mail security, Business Continuity and Disaster Recovery, as well as security information and event management. This underlines the trend that outsourcing security to third-party providers is now an acceptable option to companies. Nevertheless, the introduction of a new third-party has an implication on risk, as companies require that the cloud service be secure. In [15], the authors present a security model for securing cloud services. All data objects stored by the cloud server have annotations that can be used to express privacy and access control properties. These permit services to be constructed in a security-by-design approach. Such an approach needs to be adopted for the governance as a service. In [5], a model for formalizing the trust relationship with the cloud service is presented. This is important since local IT infrastructures delegate control and pass sensitive data to the service. We can leverage this model for passing burden of proof documents to the process server.

On modelling of security in relation to business processes [8], the two most notable efforts are SecBPMN [10] and SecureBPMN [4]. SecBPMN extends BPMN with annotations for accountability, auditability, authenticity, availability, confidentiality, integrity, non-repudiation and privacy. The result is a modelling language for secure business processes. In addition, the authors also develop an icon based query language in [10] that is used to verify security properties of a process. The main drawback of this work is that it lacks an implementation perspective where actual business processes are run and secured using an implementation framework for SecBPMN. Also, it lacks measures of security about processes that can be used in real-time for governance so that an IT infrastructure can react to security events. SecureBPMN is an earlier effort, with fewer annotations.

In [12], the authors extend BPMN 2.0 with the notion of *compliance scope*. This groups tasks of a business process where compliance rules apply. The approach is to ensure that a process is compliant at design time. A process template is created in a library that can be adapted to different situations, and once the design is ready, compliance can be verified. Thus compliance is only a design time issue, and no means are presented to help demonstrate implementation of compliance at runtime. Another extension, the *compliance domain*, is presented in [11]. This is a means to restrict the data flow in a business process using so-called data context objects. The data context object is an XML data schema that describes the data that may enter and leave a domain. XPATH is then used to evaluate the flows between domains at design time. We believe that DMN is a far more accessible means to express policy for non-IT stakeholders.

VI. Conclusions

This paper has examined the issue of security and compliance. Increasingly, it is necessary for companies to demonstrate implementation of security processes so that they do not become liable to litigation in the event of an attack leading to a data loss, and so that they can demonstrate compliance with legislation like the GDPR. These requirements led us to a cloud solution where the participation of a trusted independent party is leveraged for its competence in the security domain as well as for proof of process implementation. The latter is useful if ever the company is faced with litigation under GDPR or for demonstrating to cyber-insurers that security measures are taken.

The model is based on the BPMN language. Security and compliance processes are expressed in this language and executed in real-time on a process engine on the cloud. BPMN is extended with annotations for burdens of proof. These represent points in the process where evidence must be furnished and validated for execution to continue. These constitute proof of implementation of the process for management and auditors.

Future work includes investigating implementation techniques for compliance agents that protect their execution in environments where the administrator is hostile. Work around SGX offers an interesting avenue in this regard [7]. Another area of investigation is for companies that outsource their whole IT management to a cloud provider, and where the challenge is to integrate our security model with that cloud provider.

References

[1] David L. Baumer, Julia Brande Earp, and Fay Cobb Payton. Privacy of medical records: IT implications of HIPAA. *SIGCAS Computers and Society*, 30(4):40–47, 2000.

[2] Mostafa Behi, Mohammad GhasemiGol, and Hamed Vahdat-Nejad. A new approach to quantify network security by ranking of security metrics and considering their relationships. *I. J. Network Security*, 20(1):141–148, 2018.

[3] Ghada Gashgari, Robert John Walters, and Gary Wills. A proposed best-practice framework for information security governance. In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, IoTBDS 2017, Porto, Portugal, April 24-26, 2017*, pages 295–301, 2017.

[4] Jan Mendling and Matthias Weidlich, editors. *Business Process Model and Notation - 4th International Workshop, BPMN 2012, Vienna, Austria, September 12-13, 2012. Proceedings*, volume 125 of *Lecture Notes in Business Information Processing*. Springer, 2012.

[5] Marco Casassa Mont, Ilaria Matteucci, Marinella Petrocchi, and Marco Luca Sbodio. Towards safer information sharing in the cloud. *Int. J. Inf. Sec.*, 14(4):319–334, 2015.

[6] Antònia Mas Picahaco, Antoni Lluís Mesquida, Esperança Amengual Alcover, and Bartomeu Fluxà. ISO/IEC 15504 best practices to facilitate ISO/IEC 27000 implementation. In *ENASE 2010 - Proceedings of the Fifth International Conference on Evaluation of Novel Approaches to Software Engineering, Athens, Greece, July 22-24, 2010*, pages 192–198, 2010.

[7] Christian Priebe, Kapil Vaswani, and Manuel Costa. Enclavedb: A secure database using sgx. In *2018 IEEE Symposium on Security and Privacy, SP 2018, San Jose, CA, USA, May 22-26, 2018*, pages 3–18, 2017.

[8] Pille Pullonen, Raimundas Matulevicius, and Dan Bogdanov. PE-BPMN: privacy-enhanced business process model and notation. In *Business Process Management - 15th International Conference, BPM 2017, Barcelona, Spain, September 10-15, 2017, Proceedings*, pages 40–56, 2017.

[9] Daniel Ritter. Using the business process model and notation for modeling enterprise integration patterns. *CoRR*, abs/1403.4053, 2014.

[10] Mattia Salnitri, Fabiano Dalpiaz, and Paolo Giorgini. Designing secure business processes with secbpmn. *Software and System Modeling*, 16(3):737–757, 2017.

[11] Daniel Schleicher, Christoph Fehling, Stefan Grohe, Frank Leymann, Alexander Nowak, Patrick Schneider, and David Schumm. Compliance domains: A means to model data-restrictions in cloud environments. In *Proceedings of the 15th IEEE International Enterprise Distributed Object Computing Conference, EDOC 2011, Helsinki, Finland, August 29 - September 2, 2011*, pages 257–266, 2011.

[12] Daniel Schleicher, Frank Leymann, David Schumm, and Monika Weidmann. Compliance scopes: Extending the BPMN 2.0 meta model to specify compliance requirements. In *IEEE International Conference on Service-Oriented Computing and Applications, SOCA 2010, 13-15 December 2010, Perth, Australia*, pages 1–8, 2010.

[13] Colin Tankard. What the GDPR means for businesses. *Network Security*, 2016(6):5–8, 2016.

[14] Richard Thomas. Introduction to the unified modeling language. In *TOOLS 1997: 25th International Conference on Technology of Object-Oriented Languages and Systems, 24-28 November 1997, Melbourne, Australia*, page 354, 1997.

[15] Yiannis Verginadis, Antonis Michalas, Panagiotis Gouvas, Gunther Schiefer, Gerald Hübsch, and Iraklis Paraskakis. Paasword: A holistic data privacy and security by design framework for cloud services. *J. Grid Comput.*, 15(2):219–234, 2017.