Automating Legal Compliance Documentation for IoT Devices on the Network

Tania Quill
Dept. of Computing
Letterkenny Institute of Technology
Letterkenny, Ireland
L00111952@student.lyit.ie

Ruth Lennon
Dept. of Computing
Letterkenny Institute Institute of Technology
Letterkenny, Ireland
Ruth.Lennon@lyit.ie

***Abstract*— Auditing of compliance with laws and regulations takes up much of security administrator's time. With the increasing number of IoT devices in a company network verification may go unchecked. This paper describes stage one of a research project to automate the generation of compliance documentation for Irish Laws in a large industry. Initial findings from the implementation and configuration of the tool indicate that the process is still significantly labor intensive.**

Keywords—RegTech, Automation, IoT, Compliance

I. Introduction

RegTech consists of many aspects including automation of background checks, risk assessment and regulatory mapping. In this paper the automation of regulatory compliance documentation with particular reference to the risk IoT devices carry is discussed. Automation of tasks including security and regulatory compliance are increasingly considered integral steps of the software development lifecycle. DevOps enhances the development process through open communication and automation of tasks. There are a small number of commercial tools available but the focus of this paper is on the adaptation of an open source tool to suit the automation of compliance documentation for European laws and regulation.

II. Risk and IOT

Whilst in the past companies focused on documenting the security controls of standard network controls and end user devices such as desk top pc's and laptops, now consideration must be given to IoT devices. Many companies hold devices such as tablets, ip phones and cameras, smart plugs, smart heating and so on. Each of these devices not only can be considered part of the IoT range but should be considered an entry point into the data center. A recent talk by Philip Close [1] provided an insight into how many of the vulnerabilities he found during pen testing came from edge or IoT devices. In some cases private or confidential data may be held on IoT devices. In other cases they simply provide an access point into the network. Either way IoT devices should now be considered a core part of the network when evaluating risk and documenting compliance with the relevant laws and regulations.

Interestingly new standards on Drones and related technologies including: P1937.1 [15] and P1939.1 fail to indicate the importance of security of payloads and operational features from the outset.

Often forgotten is the Industrial Internet of Things (IIoT). In a white paper by F5 [2] the security risks and disruptive nature of IIoT is expounded. Consideration should be given to the documentation of compliance with regulations when considering machine to machine communications. It may be a case of a medical fridge notifying the data center that a blood produce was removed, or a tablet blister packing device notifying a manager through intermediary devices that a batch of tablets of a specific type have failed the automated quality checks. Information of this nature may be restricted with regard to visibility thus the documentation of processes and automation of security checks can prove beneficial.

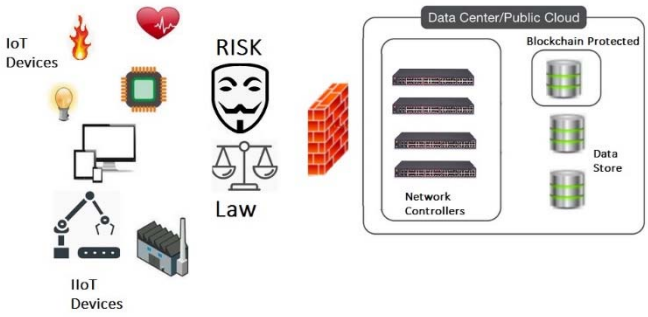

Fig. 1. IoT & IIoT Risk & Restrictions

This wall of risks and of legal restrictions stands between the IoT devices and the data stores. Refer to Fig. 1. Some data stores may be secured using blockchain to aid data security and provenance. Regardless, the documentation of these controls are still required in many cases for legal purposes.

III. Open Control

The Open Control Architecture (OCA) "is an architecture for system control and connection management of media networks." [3]. OpenControl was initially created was to ensure that security controls were documented although it's importance in establishing compliance with legal requirements can arguably be more important. A complete System SecurityPlan can be created using OpenControl content schemas and tools. The three main security processes which should be adhered to are [4]:

978-1-5386-4980-0/19/$31.00 ©2019 IEEE

- System Security Plans (SSPs) .
- Requirement Traceability Matrixes (RTMs) where a bill of materials can be created.
- Security Assessment Plans (SAPs) where system elements configuration are validated against compliance requirements.

In the authors views the use of OpenControl is crucial due to the fast pace of the DevOps pipeline, the increasing use of IoT devices with in company networks and the continuous change to laws and regulations. In order to apply automated compliance documentation for this research, the Compliance Masonry tool was selected.

A. Tool Selection

When considering which tool to use it was necessary to first investigate the available tools. Many of the tools listed as RegTech tools focused on narrow list of reporting capabilities targeted directly at traditional devices. However there are a number of tools which focus on evaluating compliance with laws or regulations or indeed with the generation of documentation to document compliance. This work focuses initially on the generation of documentation based on the European regulations. Blueprint, ADAudit and Qualio software were certainly interesting but they are commercial based and do not allow for the adaptation we required.

B. Compliance Masonry

Compliance Masonry is an open source software which we could adapt to the needs of this project. The nature of the tools under the umbrella name of Compliance masonry enable the "restructure the process of writing, updating, and reviewing compliance documentation." [3]. A document of structured data can be worked on by the team and then it can be formatted in different ways using the automated system. This flexibility of adaptation can enable documentation to be restructured to suit reporting for the purposes of not only legal requirements but standardisation groups. Again, considering the inclusion of IoT devices into the network may require the generation of documentation to document the compliance with best practices such as COBIT. Creating a System Security Plan is often repetitive and much of the required information can be inherited from the system [3].

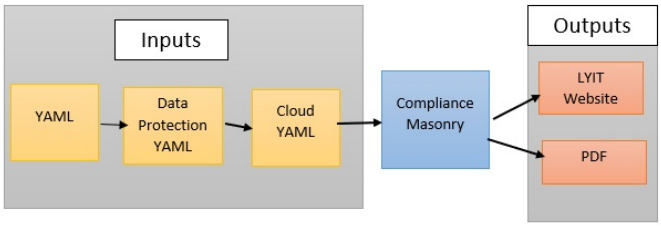

Fig. 2. Data Protection Compliance Documentation Process (Stage 1).

The process of generating documentation can be simplified as Ccompliance masonry includes multiple YAML files as input and produces output as a HTML website and a PDF document as required. The author feels that compliance masonry is very useful and is a very relevant tool set as it can take away repetitive and it will also add consistence. The additional benefits of knowledge management should not be discounted. Understanding the risk and the processes to mitigate against the risk form a large part of security systems. Thus having automated websites to update such information enhances the overall security of a company. Below in the image is an Inputs section and a Outputs sections with a compliance Masonry in the middle.

Identify applicable funding agency here. If none, delete this text box.

IV. Need for Open Compliance

In order for a company to use legal compliance documentation tools it is important that the legal framework is understood by the company. The company should have a list of best practices and current company policies. If a process is new it may be necessary to get legal guidance on the nature of the applicability of the law or regulation. The company risks lawsuits and bad public relations if they do not follow the licensing and other laws.

There was a survey carried out in 2015 called Future of Open Source survey. In this survey the percentage of companies which say that they use open source software was 60%. From the same survey it was also established that the majority of companies do not have anything in place to ensure that the correct licensing and also regulations are being met. Free and Open Source Software (FOSS) compliance should be considered as part of the Risk Plan. A FOSS compliance program may have a "Open Source Review Board" (OSRB) [5] which can be part of the legal compliance considerations for the automated system.

In the authors option compliance with legal documentation comes in from many risk areas and is a greater risk when open source is being used without careful consideration.

V. Need for Open Compliance

DevOps ensures that software is able to be designed, built, tested and also realized faster to produce more secure and reliable software. Through DevOps collaboration, mindset and integration are much better. In order for the work to be more efficient and faster, agile, continuous delivery and automation are all combined [6]. This compounded with the proliferation of IoT devices which often remain untracked can pose security risks. Thus we propose that the automated evaluation and creation of the legal compliance documentation should be considered integral to any system pipeline.

Whilst it is difficult to define 100% compliance with any standard from this research it is recommended that Best Practices for IoT Security [11] be applied. In addition to best practices we recommend Self-Certification using the IoT Security Compliance Framework [12].

Through the development of this project compliance to laws and security regulations is provided through the automated creation of a PDF and website. This research project was built on an Ubuntu machine. The system was modified to take into consideration the Irish Data Protection Act.

VI. AUTOMATION

IT automation and orchestration are terms which are often used together however, they are different. There is no need for human intervention with automation as it will counties to complete the task repetitively. Whereas Orchestration will need a user in order to synchronize the automated tasks. Thus, software tools are relied on intensely [7]. Automating the process of generating compliance documentation provides the advantages of:

- Enabling the security team to focus on the task of security review and system hardening
- It will reduce errors and variations in security documentation
- It will improve governance.

The second part of the research is to carry out the monitoring of IT process automation and service provisioning and to ensure that systems conform to the compliance documentation. IT process automation (ITPA). ITPA is also known as (RBA) run book automation. There is also automated provisioning and it is known as self-service provisioning and this is when a pre-defined procedure is used for an information technology. It is a policy-based management. Rights is given either on permissions-based or role-based [8]. With the provisioning of IoT devices to staff and the deployment of IoT intelligent devices the monitoring of the devices it may be difficult to ensure that configuration of all devices appropriately matches the legal requirements. Automating the system would aid in this process.

In the authors opinion automation will remove the element of inconsistencies between the level of work employed and the final product. Regardless, the authors believe that it is important to ensure that there is a person allocated time to carryout oversight of the automated work to ensure that all processes are quality checked on a regular basis.

When this research is complete the monitoring, management and conformance checks will be able to be applied automatically to ensure that the correct security compliance procedures are met. In this paper the automatic creation of documentation is discussed.

VII. REGTECH

A company should be regulatory compliant and this means that they are meeting the correct laws, regulations, guidelines and specifications in relation to their business. If a business does not meet the above listed, they may end up facing legal punishment. There are a number of different regulations and laws of particular interest, they include:

- Dodd-Frank Act
- Payment card industry data security standard
- Health Insurance Portability and Accountability Act
- Federal Information Security Management Act
- Sarbanes-Oxley Act
- GDPR

Whilst each of these are important the Data Protection Act is discussed separately as it was the initial act chosen to be implemented.

The short-term benefits of RegTech tools are as follows:

- Cost can be reduced due to automated mapping of tasks to risks and on to compliance requirements.
- RegTech solutions which are sustainable and scalable.
- Regulatory information can be easily analyzed and this then enables a company to discover risk patterns.

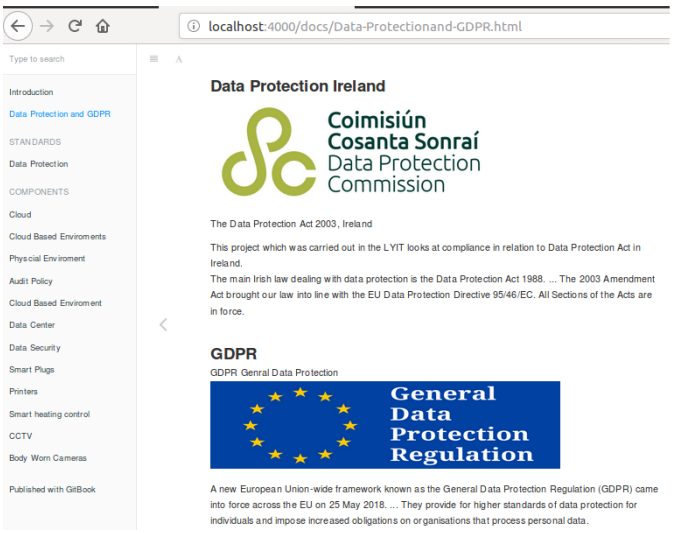

Fig. 3. Data Protection Compliance Documentation (Stage 1).

The practices of RegTech aid with Fraud prevention, Regulatory compliance automation and Compliance and conduct analytics these are just a few of the practices.

In the authors views RegTech is helps ensure that all branches of the organization are running of the same standards and all reaching the correct laws and regulations in order to protect both the company and staff. The onboarding of new staff is also enhanced as they become aware of the guidelines and standards to follow.

VIII. DATA PROTECTION IN IRELAND

The Irish Data Protection Act as amended in 2003 provides an enactment of the ePrivacy Data Protection Directive. This act concerns the governance of data. However, technology evolves more quickly than laws can keep up. The use of IoT devices is now prolific and includes wearable cameras for staff, smart plugs and tablet devices. Each of these IoT devices may include data that needs to be secured. It may be necessary to for devices and data to be secured even when they do not constitute Personally Identifiable Information (PII).

In October 2018 California State implemented their Cybersecurity bill requires that makers of internet connected

smart devices apply reasonable security. The law will not come into effect until 2020. There is no equivalent law in Ireland.

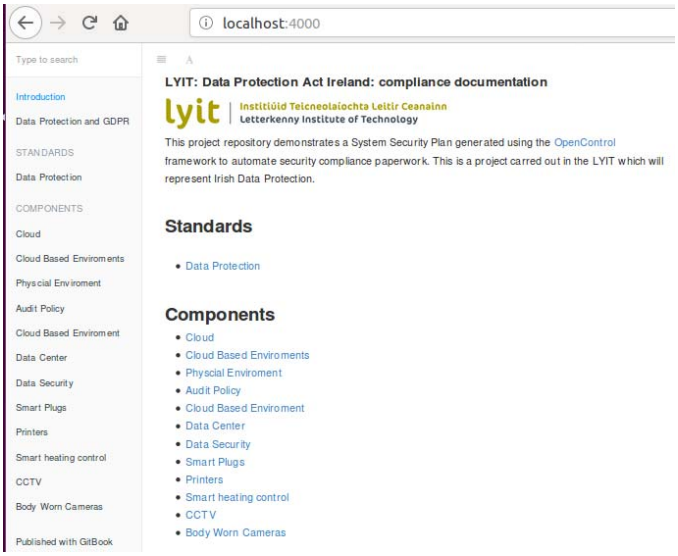

Fig. 4. Compliance Documentation Components (Stage 1).

A survey [9] taken by Global Privacy Enforcement Network (GPEN) in 2017 showed that many companies failed to refer to the security of data collected and held on their website. The creation of websites such as that shown below clearly identifies the various IoT components and how they comply with the regulations. The survey fails to mention the risk of data on IoT or IIoT devices. On the other extreme Hypponen [10] has stated that "whenever an appliance is described as being "smart", it's vulnerable". The authors here would argue the contrary. The devices can be made as secure and compliant with law as any larger device. It is down to the administrators to carry out the appropriate analysis, configuration and continuous security review as they would with any other networked device.

The cost to business can be staggering, in [13] it has been indicated that the cost of Cyber Attacks can be as much as $2.35mill per incident with the additional cost of fines of up to 4% of revenue. A recent report in the RTE News [14] noted that there was a 70% increase in the number of data breaches reported to the Data Protection Commission in the previous year. As a note of the importance of data breaches funding for the DPC has risen almost 7 fold from €1.7mill in 2013 to €11.6mill in 2018. It is clear that further research is required in order to establish the true cost of data breaches within Ireland. Further it is also clear that there is a dearth in research into the cost of breach as a result of IoT. This could be further extended to a review of the application of security measures and their effectiveness on IoT devices. It is anticipated that in a later stage of this research such investigations will be carried out.

For each of the components on the website or pdf separate documents are listed. For example in the AU_policy.md the properties of the auditing system are listed in relation to the relevant standard. The smartplug for example connects to the network to enable a failsafe of shutting down devices from a remote location. This can be useful if the attacker of the server has locked out the administrator. The administrator can then use the IoT devices for the remote shutdown.

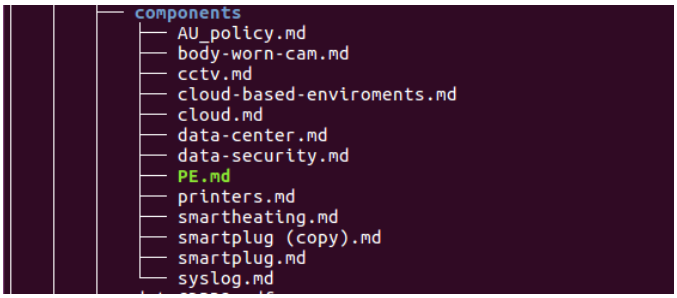

Fig. 5. IoT Components Documents (Stage 1).

Considering the device from the administrator's perspective it is also necessary to ensure that all software patches are installed and that the plug is considered in the overall network. This should not become a simple point of entry into the network. As such it is necessary to list the device into the security documentation and to add the relevant information.

The research defined here is at an early stage and the documentation is initially being manually populated as per the required format which is a tedious process. The problem lies in part with the fact that there is no open source tool available that enables adherence with EU and Irish regulations.

```
schema_version: "1.0.0"
name: diss-tania-dataprotection
metadata:
description: LYIT : Data Protection project for Ireland a compliance document
maintainers:
- tania.quill@yahoo.ie
- ruth.lennon@lyit.ie
components:
- ./Data Protection Act
- ./Cloud
- ./Cloud-based-enviroments
- ./Physcial Enviroment
- ./Audit Policy
- ./Cloud Based Enviroment
- ./Data Center
- ./Data Security
- ./CCTV
- ./Body Worn Cameras
- ./Data Center
- ./Data Security
- ./Smart Plugs

standards:
-url: https://www.dataprotection.ie/docs/Law-On-Data-Protection/m/795.htm
revision: master
certifications:
-url: https://www.dataprotection.ie/docs/03-07-12-Cloud-Computing/1221.htm
-url: https://dataprotection.ie/viewdoc.asp?DocID=1689&ad=1
revision: master
```

Fig. 6. Opencontrol.YAML (Stage 1).

The documentation in pdf format and websites is automated but the content of the markup files is manually created. Stage 2 of the project is to used automated monitoring to check for compliance with the documentation as created. Figure 5 shows the initial opencontrol.yaml file which incorporates the folders of manually created md files, standards information from their source websites and other configuration item information.

The documentation in pdf format and websites is automated but the content of the markup files is manually created.

The process of creation of the compliance documentation in line with the relevant regulations will take quite some time but is in progress. Once this stage is complete, any changes to laws or regulations would require changes to the format document in the majority of cases rather than to the individual md files. This

is a significant advantage of this tool. Stage 2 of the project involves using automated monitoring to verify and validate compliance with the documentation as created. This phase of the research is currently under development.

IX. Conclusions

The advent of GDPR has caused many companies to examine how they show compliance with legal and regulatory restrictions. The prolific use of IoT devices for a range of purposes has resulted in poorly documented devices which do not always conform to the aforementioned legal requirements. Significant hours are spent by security staff in generating compliance confirmation documentation on a regular basis for different auditing groups. Much of this work is repetitive. In the opinion of the author's whilst the current commercial tools are good they are not adaptable for European or Irish laws. To have a more dynamic tool an open source solution was found to be most appropriate.

The configuration of the tool initially was easy, however, it was discovered that there is a significant portion of work required to manually configure the basic information into each of the files which is then read by the tool to enable auto generation of the website or pdf demonstrating compliance with specific laws.

From the very few examples of the tool that can be found online most simply refer to the work in theoretical terms rather than discussing the practical implementation. It is the author's opinion that that time it takes to carry out the initial implementation is a significant fact here. Further, we suggest that many groups fail to complete the process for this reason. We have yet to find any papers which refer to the use of tools to document regulatory compliance of IoT or IIoT devices.

There are a significant number of dependencies required in order to install and run the tool. This also detracts from the installation process and may increase the attack footprint of the machine with the software installed. The installation of the product on a Linux operating system showed no errors but installation on a Windows operating system did show errors on the dependencies.

It is has been found that little research into automatic validation of compliance with legal and regulatory requirements has been carried out to date. This is an area that needs investigation considering the increasing number of devices that fall into the category of IoT.

This research is still in the early stages but it is already clear that a better solution is required in order for companies to take regulatory compliance seriously.

Acknowledgment

The authors would like to thank Letterkenny Institute of Technology for their funding of this research work.

References

[1] P. Close, When Application Security Fails: Tails from the Trenches, OWASP Letterkenny Meetup, Letterkenny, December 2018.

[2] F5, The Industrial Internet of Things and Network Security, F5, July 21, 2017, https://www.f5.com/services/resources/white-papers/the-industrial-internet-of-things-and-network-security

[3] A.Feildman, Compliance Masonry for the Compliance Literate, October 2016, https://github.com/opencontrol/compliance-masonry/blob/master/docs/masonry-for-the-compliance-literate.md

[4] S. Wells, Tackling Compliance with OpenControl, May 2017, https://shawnwells.io/2017/05/13/tackling-compliance-with-opencontrol/

[5] I. Haddad, Using Open Source Code, The Linux Foundation, 2015, https://www.linuxfoundation.org/resources/open-source-guides/using-open-source-code/

[6] J. Humble, D. Farley, Continuous Deliver: Reliable Software Releases through Build, Test and Deployment Automation, Adobe, Pearson Education, 2010.

[7] M. Rouse, IT Automation, Whatis.com, October 2017, https://searchitoperations.techtarget.com/definition/IT-automation

[8] A. Guzman, A. Gupta, IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices, Packt Publishers, 2017

[9] Anon, Global Privacy Enforcement Network (GPEN) Survey Press Release, Data Protection Commission, 24 October 2017, https://www.dataprotection.ie/docs/EN/24-10-2017-International-data-protection-authorities-enforcement-operation-finds-website-privacy-notices-are-too-vague-and-generally-inadequate/i/1674.htm

[10] M. Hypponen and L. Nyman, The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation, Technology Innovation Mangaement Review, 7, 4, April 2017.

[11] D. Hamilton, Best Practices for IoT Security, Network World, 27 March 2018, https://www.networkworld.com/article/3266375/best-practices-for-iot-security.html

[12] IoT Security Foundation, Bes Practice User Mark FAQ and Terms of Use, Accessed on 1 March 2019, https://www.iotsecurityfoundation.org/best-practice-user-mark/

[13] Business Matters, The risks of not being GDPR compliant, 24 July 2017, https://www.bmmagazine.co.uk/in-business/advice/risks-not-gdpr-compliant/

[14] W. Goodbody, Surge in number of data breaches reported to Commission in 2018, 28 Febuary 2019, https://www.rte.ie/news/ireland/2019/0228/10033343-data/

[15] IEEE, P1937.1 Standard Interface Requirements and Performance Characteristics for Payload Devices in Drones, 2019, https://sagroups.ieee.org/1937-1/