LockChain Technology as One Source of Truth for Cyber, Information Security and Privacy

Yuri Bobbert[1,2(✉)] and Nese Ozkanli[3]

[1] Antwerp Management School, Antwerp, Belgium
yuri.bobbert@uantwerpen.be
[2] ON2IT B.V., Waardenburg, The Netherlands
[3] Open University, Heerlen, The Netherlands
nese.ozkanli@gmail.com

Abstract. Implementing and maintaining Information Security (IS) in a digitized ecosystem is cumbersome. Multiple complex frameworks and models are used to implement IS, but these are perceived as hard to implement and maintain in digitized dynamic value chains and platforms. Most companies still use spreadsheets to design, direct and monitor their information security function and demonstrate their compliance. Regulators too use spreadsheets for supervision. This paper reflects on longitudinal Design Science Research (DSR) on IS and describes the design and engineering of an artefact architecture, coined as LockChain, which can emancipate boards from silo-based spreadsheet management and improve their visibility, control and assurance via integrated dash-boarding and a reporting tool. LockChain is not a traditional Information Security Management System (ISMS) but is used for the design and specification of information security requirements and measures and privacy requirements. We elaborate "Why" we used Design Science Research into valorisation of the concept of LockChain, we explain "What" we have established in terms of the technology of LockChain and "How" it is applied and the added value LockChain brings for companies on cost savings, Security and Privacy by Design engineering culture and Digital Assurance.

Keywords: Information security controls · Security requirements · Security measures · Security by design · Privacy by design · Digital assurance

1 Introduction

When starting this research journey in 2008, security was mainly IT-oriented and the main focus was on using IT controls to mitigate or detect security vulnerabilities. Research has shown that the number of security incidents has increased [1] over the years, as has the financial impact per data breach [1]. Mastering emerging technologies such as big data, Internet of Things [2], social media and combating cybercrime [3], while protecting critical business data, requires a team instead of a single IT person [4]. To protect this data, security professionals need to know about the value of information and the impact if it is threatened [4]. IT risk management requires different capabilities, knowledge and expertise from the skills of IT security professionals [5]. Hubbard [5] refers to the failure

K. Arai et al. (Eds.): SAI 2020, AISC 1230, pp. 336–347, 2020.
https://doi.org/10.1007/978-3-030-52243-8_24

of 'expert knowledge' in impact estimations and to the importance of experience beyond risk and IT security, such as collaboration and reflection [6].

1.1 Problem Statement

In the past [7] IT security controls were implemented based on best practices prescribed by vendors, without a direct link to risks or business objectives [7]. These controls depended on technology and the audits and assessments (in spreadsheets) were used to prove their effectiveness [8]. The problem with this approach lay in the limitations of mainly IT-focused security and security experts working in silos with limited, subjective views of the world [9]. This is important, as information security is subject to many different interpretations, meanings and viewpoints [10]. In the case of IS, this refers to interactions and reflection between actors e.g. the business, data owners and industry peers on the appropriate level of risk appetite and security maturity [9]. Thus objectivity relates to reality, "truth reliability", testability and reproducibility, while subjectivity refers to the quality of personal opinions. Intersubjectivity involves the agreements between social entities and the sharing of subjective states by two or more individuals [11].

The state of security in 2010 shifted towards "information security". ISO specifies information security as "*protecting information assets from a wide range of threats in order to ensure business continuity, minimise business risk and maximise return on investment and business opportunities*" [12]. Its core principles are Confidentiality, Integrity and Availability (CIA) [12]. Later non-repudiation and auditability were added to comply with audit and compliance regulations. Thus Information Security should ensure a certain level of system quality and assurance [13]. In 2010 many organisations used spreadsheets to practice risk and security management and also proof their assurance via spreadsheets [14, 15].

The scope of Information Security was then expanded to other disciplines in the enterprise since digital became more and more common in our way of doing business [16]. In their book "Information Security Governance", Von Solms and Von Solms describe the growing number of disciplines involved in IS [17]. By 2011 IT managers and IT security managers were increasingly urged to engage with business to determine risk appetite and the desired state of security. In 2005 ITGI proposed to co-develop IS together with the business [4]. Since 2011, the role of culture [10], awareness [18], compliance [19] and knowledge sharing [9] has also been included in security strategy frameworks [20]. Due to research on IT governance at the Antwerp Management School (AMS) [21], relational mechanisms such as culture, behaviour and knowledge were incorporated in the COBIT 5 Information Security Framework [22] in 2012.

IT staff still find it difficult translating security controls into concrete actions in the initial phase of a design and build of software [23]. Because of this complex processes, employees focus on continuous maintenance of documentation to please internal and external regulators, instead of value creation for customers. Khan states in his paper "*Due to constantly shifting regulations, businesses today are having to audit their IT compliance requirements on average four and a half times per year. Now more than ever, the act of adhering to regulatory requirements requires an ongoing commitment* [24]". Without an automated process security & privacy by design and continuous delivery

will not be possible [25]. Compliance processes are complex and time consuming, often manual and the evidence has to be found numerous times for different audits, reviews and different regulators [24].

Up to 2016, the subjective silo approach to IS was designed, maintained and reported via spreadsheets [8]. Experts mapped multiple control frameworks [26] from ISO, ISF, COBIT 5 in spreadsheets and these are still used by regulators such as the Dutch Central Bank [27]. Powell et al. [28] discovered in 483 error instances in 50 spreadsheets. The Powell research is one of the largest examinations into spreadsheet errors. They have identified; Mechanical errors arising from typing or pointing errors, logic errors arising from choosing the wrong function or creating the wrong formula and omission errors arising from misinterpretation of the situation to be modelled. Volchkov stated that collecting evidence of effectiveness of the controls via spreadsheets has limitations [29] and pose a risk on its own. So Governance Risk and Compliance (GRC) tools moved towards information risk, due to the Sarbanes-Oxley Act, and were designed for large enterprises. GRC implementations are complex and their maintenance requires dedicated staff [30]. Integration of GRC tools with operational data via Security Information and Event Management (SIEM) functionality is reserved for companies with extensive budgets and sufficient staff [30].

Filling in spreadsheets with answers to questionnaires is subject to manipulation [28] because it is not a closed-locked-down cycle. Spreadsheets are stored –sometimes double versions- on decentral systems, sometimes not well protected which makes evidencing unreliable. Spreadsheet data is limited to subjective opinions and there is little room for reflection. Spreadsheet data cannot always be gathered from the original sources, which reduces authenticity and integrity [31]. Intersubjective aspects were missing from past timeframes, unless companies used third parties to interpret the data. Objective aspects are not covered, since the various objects (operational processes and data) are not interconnected. Javid Khan quotes "*The use of smarter and more intuitive tools and technologies, along with* automating *processes, will enable organisations to gain the benefits they are seeking, such as real-time alerts, better reporting and bringing all data sources together. Going forward, there will be increased demand for this type of technology that can optimise the compliance process, both from a management and maintenance point of view* [24]".

This brings us to the following problem statement:

"*Maintaining a realtime security administration (e.g. insight and oversight) on the end to end digital assurance is cumbersome. Specifically in a large Agile oriented enterprise with multiple DevOps teams that is subject to multiple regulations.*"

1.2 Design Science Research to Design and Engineer the LockChain Artefact

As mentioned above traditionally, security and risk processes are being implemented by IT or security people only. Most of the time via spreadsheets and Microsoft Word files residing all over the organization with a lack of proper central administration [6]. Khan states *"Given that compliance is such a complex and time-intensive task, automating some of the processes can make realizing compliance on a continuous basis easier to achieve. It can also reduce the potential for human error and make the entire process more accurate and more efficient* [24]*."* Over the period 2016-2019 we have established

an artefact which addresses all of these future digital assurance problems via Design Science Research (DSR). According to Hevner, DSR is based on three major domains: the "Knowledge base" domain, the "Environment" domain and the "Design Science" domain [32]. The first is concerned with knowledge items produced and maintained with academic rigor. Theories, frameworks, models and techniques are produced in science and contribute to such rigor. These are then applied via the design science cycle to the practical environment, which includes organizations, systems and people with real-life problems. At the heart of the DSR framework is the design science cycle, which is concerned with receiving input from the knowledge base, applying this in environments and receiving feedback, in order to master problems and establish artefacts. The three cycles at the center of the framework represent the continuous feed-forward and feedback cycles which strengthen the design and development of the artefact. The main function of this design cycle is to establish and maintain the artefact and the main purpose of the artefact is to solve problems. The process of assessing and refining the artefact requirements is necessary to continuously test the artefact for its relevance to the practical environment (mainly to solve problems) and its contribution to the academic rigor (knowledge base). Creating business value due to the application of DSR artefacts is described as "valorization" and demonstrated in our earlier work [33].

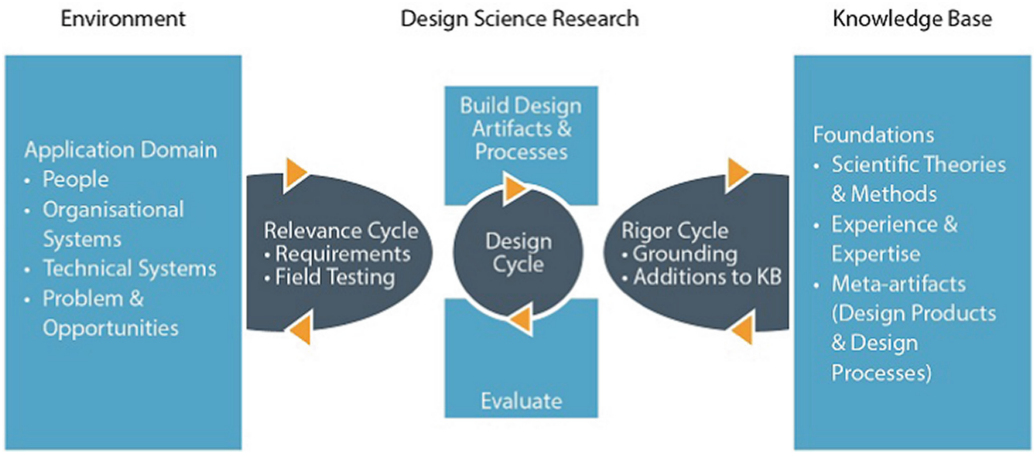

Fig. 1. Hevner's design science research framework for the design and engineering of security artefacts [32].

Hevner et al. [32] produced a broad framework which is used worldwide to perform and publish DSR work. This framework is visualized in Fig. 1 contrasts two research paradigms in information system research: *behavior sciences* and *design sciences*. Both domains are relevant for Business Information Security (BIS) because the first is concerned with soft aspects such as the knowledge, attitudes and capabilities required to study and solve problems. The second is concerned with establishing and validating artefacts. To put it more precisely, Johannesson and Perjons distinguish between the design, development, presentation and evaluation of an artefact [34]. Wieringa distinguished many methods for examining numerous types of problems, e.g. design problems and knowledge problems [35]. In this project we used Hevner's work as a frame of reference to establish, build, test and valorize the artefact coined "LockChain".

2 Lock the Chain of Evidence

LockChain is based on addressing three major problems in BIS [6] being a) silo based thinking and working, b) lack of central administration and oversight on information security requirements on paper versus implementation "one single source of truth" in a scaled agile environment, c) distributed decision making on risk and security without having a clear chain of evidence "end-to-end trust". Departing from these problems we started establishing the first functionalities according to the architecture framework visualized below in Fig. 2. LockChain departs from the principle that security, risk and privacy requirements are being maintained and registered in a central administrative repository. This repository is an integrated database of requirements definition as well as implementation. The result is a more reliable data and therefor better verifiable and auditable. The repository is being accessed and written into by authorization of multiple stakeholders, with clear role based access. Nowadays, with autonomous DevOps teams, it is required to do this in a more distributed and automated manner. This is facilitated for DevOps teams via LockChain since the process of design, requirement setting is done in LockChain and develop, build, deploy, testing and logging changes in version controls is completely automated in the Continuous Delivery Pipeline (CDP) [36] and not in LockChain. The architecture including the functionalities is displayed in Fig. 2. The principle of LockChain is that the central repository is being fed by control objectives originated by regulating bodies, community bodies, security frameworks and/or auditors referred to as "the Body of Knowledge". Normally the design of these controls in IT systems is something the IT department does but since IT is an integrated part of our day to day business more and more people are involved in designing and building new business models and associated systems, regardless if they are in the "Cloud" are on premise. To enable DevOps teams designing and building new applications the LockChain technology guides the autonomous team to design the IT chain end to end from cloud providers to external suppliers. By explicating the "End to End" assets and their owners this enables the asset owner and privacy officer to identify what kind of data is being processed. The level of Confidentiality, Integrity and Availability of the data being processed and the location of the application determines the level of security controls. The LockChain technology presents the required security controls per asset and requires the associated officers to authorize before going live. Traditionally the 1st line security officer, 2nd risk officer and data privacy officers or compliance officer all need to review, endorse and/or approve the going live of the application into production, depending on the internal effectuation of the Three Line of Defense model [37]. This chain of approvals as evidence, into the technology basically locks down (time and name stamping) the required assurance you need in order to demonstrate compliance, this refers to the terminology "Lock the Chain". Since LockChain also enables 3rd parties to access the system you are also able to involve Cloud providers or third parties that need to adopt and comply to your company security standards. LockChain technology enables on the one hand one source of truth for Cyber, Information Security and Privacy, and facilitates on the other hand privacy and security by design. The real time administration of the technology ensures near real-time end to end trust, oversight and enables efficient assurance.

3 LockChain in Practice

In practice, more and more business models are changed and disrupted due to Information Technology (IT) [38]. Business owners, business developers and assets owners sometimes seek their own way in acquiring new technologies when they feel the IT department does not enable them but blocks innovations and new business models, Silic et al. refer to "Shadow IT as IT behind the curtain" [39]. Therefore the need for early involvement of IT and Security staff in designing these new business models and their associated technologies is needed. Normally the assessment of information security risks begins with a Business Impact Assessment (BIA) on the digital asset, making it a business driven activity. The terminology Business Information Security (BIS) [40] also means you involve business and IT and security departments end-to-end across company silos. The DevOps team members such as developers, product owners, engineers are responsible for the development of their solution, supported by the business and asset owners and the craftsmanship the need to develop and maintain for this [41]. LockChain enables this end to end BIA process as well as determining the security requirements. In the section below we describe how it works and how it contributes and demonstrates its value:

As outcomes from the LockChain technology and the rigorous process team members need to follow, the team will establish the CIA rating (Confidentiality, Integrity and Availability) which determines the level of security controls is required. As a result to the BIA process and CIA rating a complete data register, based on current privacy regulations (including the General Data Protection Regulation (GDPR)), a list of security requirements and associated measures is presented. In such a way it is fully aligned with the company's policies. The LockChain technology also presents you the residual security risks that remain "open" after application of the security controls. This residual risk is determined based upon the Threat and Vulnerability Analysis (TVA). In case it is required, an additional Data Protection Impact Assessment (DPIA) can be performed, involving the Data Protection Officers (DPO) who can sign of on it.

Although common in mature organizations, the LockChain technology allows to reduce the burden and cost of information security risk management. A case study at a large financial institute indicated that the overall time spent on traditional security and risk processes is reduced by 50%, all roles and responsibilities that need to approve and sign off included. It also reduces cost of maintenance by 60%. As an example, a Business Impact Assessment (BIA) without existing documentation is considered to take an average of 44 h from initial steps to complete review. With LockChain, this time is reduced to an average of 22 h. As another example, the establishment of security requirements and the inherent Threat and Vulnerability Analysis (TVA) consumes an average of 69 h without pre-existing documentation. LockChain narrows this down to an average of 31 h. With existing documentation, assessment process takes an average of 31 h, time is reduced to 12 h, including the complete review process. In terms of expenses, LockChain reduces the cost of a complete process on a single application/solution from 10K euros to 4.8K Euros for a new asset, without any existing documentation. For an existing asset, cost goes down from 4.3K euros to 1.8K euro's in average. Considering a large enterprise with 5000 application, in theory can realize a reduction of the total risk, security and compliance expenses of 56%.

4 Future Developments

The development of the LockChain technology will continue in an Agile manner. Allowing the users and stakeholders (environment) provide feedback to the design and development team to further enrich and scrutinize the Body of Knowledge, as proposed by Hevner et al. [32] and extended in other work of the authors on building LockChain alike artefacts [6, 42]. Extensive additional literature research has been conducted in 2019 as part of a Master in Science project at Open University to gain new insights into future requirements. Future research and development efforts will primarily focus on expanding the automation of control testing evidence. This Information Security Management System (ISMS) functionality connects with the Configuration Management Database (CMDB), allowing to automatically export the security configuration set up to the assessment and cross-examine the information already residing in the documentation. This will increase the reliability of the evidence, lower the level of manual labor, lower the error-rate caused by spreadsheet usage, and lower the frustration currently being experienced when collecting multiple spreadsheets and Word versions. It will also decrease the subjective discussions on the quality of evidence. The Service Application feature of the LockChain technology is expected to reduce redundancy in the documentation and ease communication between the DevOps Teams. Future research and development will also be focused on how LockChain can orchestrate and further automate operational security processes. An example is the design of security control User Access Management "user verification", this will be designed in the LockChain technology and automatically kicks of periodical process of verifying users based on predefined criteria. Collecting evidence back from these processes back in the LockChain technology can be facilitated via an Application Programmable Interfaces (API). On the privacy management part it is planned to automate the detection of personal data flows between solutions. In combination with relevant metrics, and role base access, the intent is to facilitate the audit by third-parties and even regulator bodies. Therefor enabling "API based supervision" by the regulator instead of sending spreadsheets and documents. Additional privacy requirements and measures will be added, facilitating an application to the new extension of ISO/IEC 27001 and ISO/IEC 27002, the ISO 27701:2019 for privacy information management.

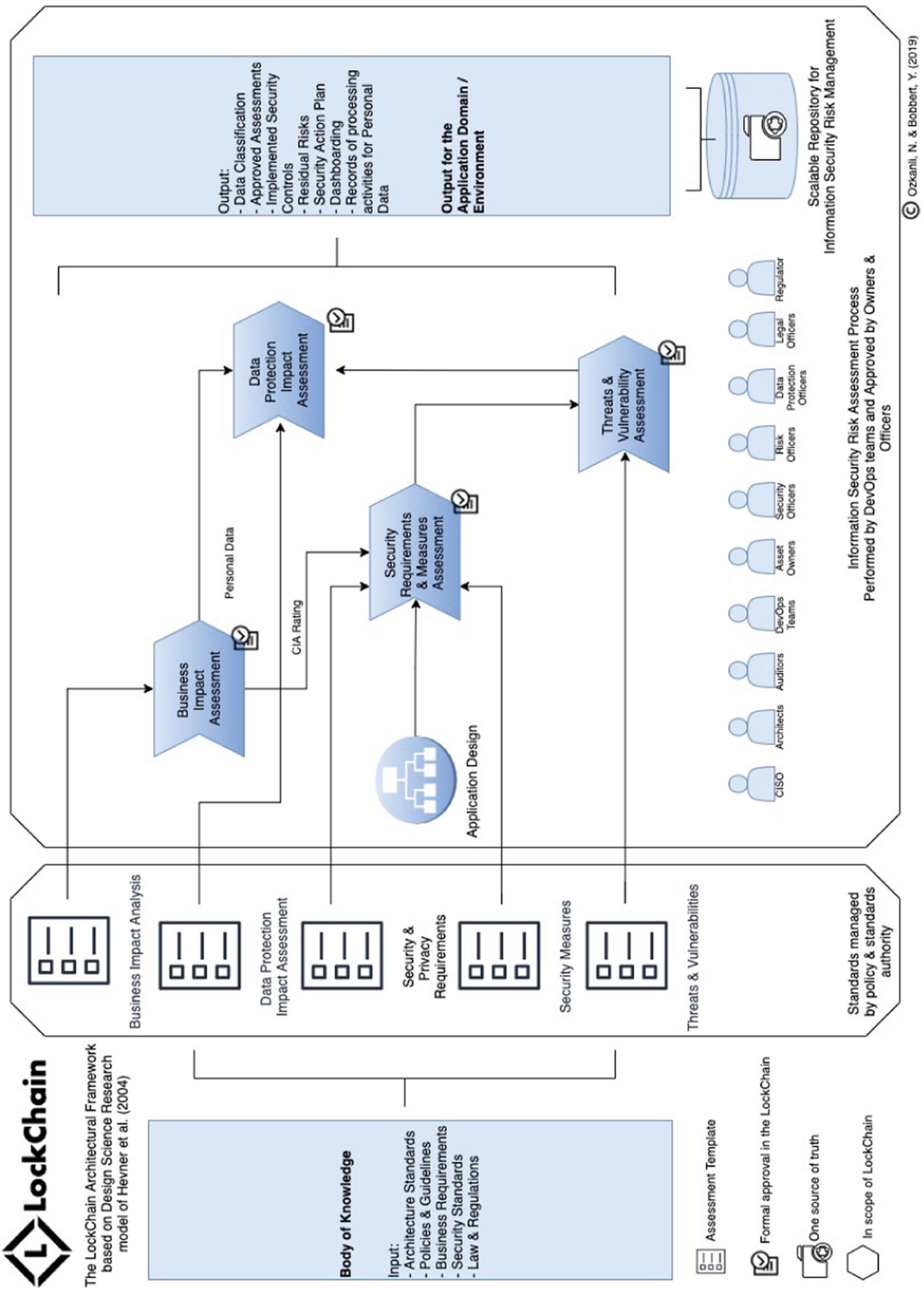

Fig. 2. The LockChain architecture framework based on Hevner et al.

5 Conclusion

The case study used for this paper allows to reduce the cost of security and risk processes by 60%. The case study company onboarded more than 1200 applications in less than a year and facilitates more than 1100 users, and includes the daily connection of 100 unique users, designing, maintaining and approving the security of critical assets. The development was based on a scrum organization of the work in a state of the art Continuous Delivery Pipeline (CDP) according to the CDP autonomy prescribed by Humble and Farley [41], with releases of updates every two weeks and a presentation of the new update by the developers themselves (End of Sprints). This method allows both the users and the development team to receive feedback on the use and needs of the product and its requirements. With rituals like these End Of Sprints (EoS) it establishes a close alignment with the business.

With Security first being practiced only in IT it is now transformed to Business Information Security, where business takes ownership over their critical assets and collectively with security teams designs, orchestrates and applies the requirements. This collectively designing and orchestration of automation is referred to as SOAR According to Gartner's SOAR market guide, "by year-end 2022, 30% of organizations with a security team larger than five people will leverage SOAR tools in their security operations, up from less than 5% today".

While collectively designing and developing the controls on assets, it also encourages ownership and stimulates craftsmanship throughout the company; ownership because each valuable and knowledgeable party is consulted and tracked in its analysis; craftsmanship because the DevOps teams are "by design" guided to the security of their application.

A positive side effect of LockChain is the development of a "Security by Design" culture in the DevOps teams of an enterprise. The simplification of security administration, led to an increase of comments and concerns, awareness on security at the very early stages. The same is observed regarding privacy topics when processing personal data. After a time of usage of LockChain, the challenge of security and privacy measures tends to "shift to the left", gradually reducing the time to review and administer. Ultimately resulting in improved oversight, visibility and control into Security, Risk and Compliance (SRC reporting), via dashboards for the Chief Information Security Officer (CISO), Chief Risk Officer (CRO) and Data Protection Officer (DPO). Figure 3 and 4 display two dashboard examples present in the LockChain artefact.

Fig. 3. Screenshot of the artefact dashboard function, general dashboard available to all users

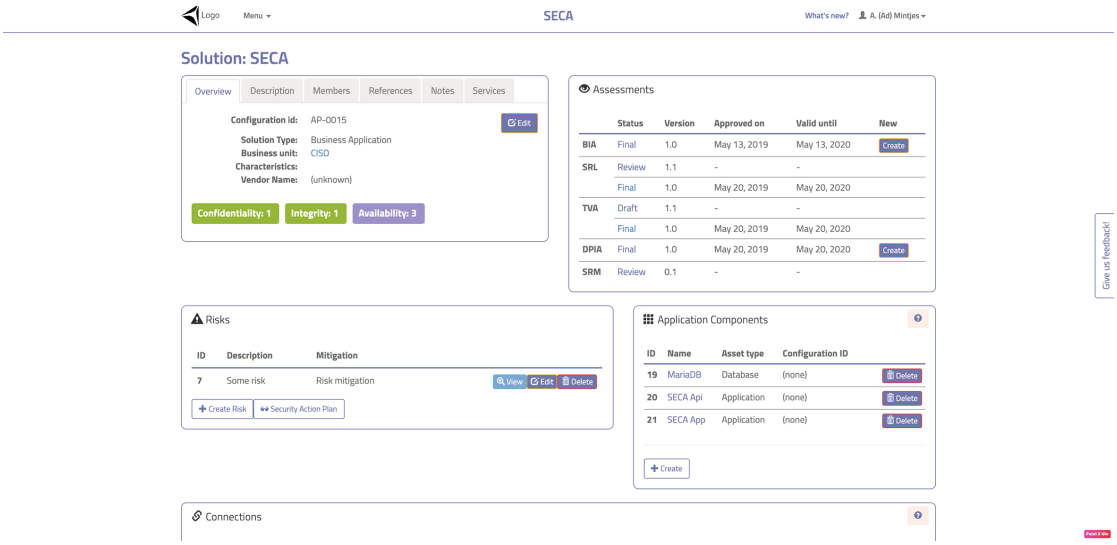

Fig. 4. Screenshot of the artefact dashboard: all information about a specific asset/solution compiled in one place.

References

1. Ponemon: Cost of Data Breach Study: Global Analysis. Ponemon Institute LLC, United States (2016)
2. Conti, M., Dehghantanha, A., Franke, K., Watson, S.: Internet of Things security and forensics: challenges and opportunities. Future Gener. Comput. Syst. Int. J. eSci. **78**, 544–546 (2018)
3. Cashell, B., Jackson, W., Jickling, M., Webel, B.: The Economic Impact of Cyber-Attacks. Congressional Research Service, The Library of Congress, United States (2004)
4. ITGI: Information Risks; Who's Business are they? IT Governance Institute, United States (2005)

5. Hubbard, D.: The Failure of Risk Management. Wiley, Hoboken (2009)
6. Bobbert, Y.: Improving the Maturity of Business Information Security: On the Design and Engineering of a Business Information Security Administrative Tool. Radboud University, Nijmegen (2018)
7. Yaokumah, W., Brown, S.: An empirical examination of the relationship between information security/business strategic alignment and information security governance. J. Bus. Syst. Gov. Ethics **2**(9), 50–65 (2014)
8. Zitting, D.: Are You Still Auditing in Excel? Sarbanes Oxley Compliance J. (2015). http://www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=4156
9. Flores, W., Antonsen, E., Ekstedt, M.: Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture. Comput. Secur. **2014–43**, 90–110 (2014)
10. Van Niekerk, J., Von Solms, R.: Information security culture: a management perspective. Comput. Secur. **29**(4), 476–486 (2010)
11. Seale, C.: Researching Society and Culture, 2nd edn. Sage Publications, Thousand Oaks (2004). ISBN 978-0-7619-4197-2
12. ISO/IEC27001:2013: ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. ISO/IEC, Geneva (2013)
13. Cherdantseva, Y., Hilton, J.: A reference model of information assurance & security. In: IEEE Proceedings of ARES, vol. SecOnt Workshop, Regensburg, Germany (2013)
14. GOV.UK: The Security Policy Framework (SPF). Statement of Assurance questionnaire in Excel - Gov.uk
15. Halkyn: ISO27001 Self Assessment Checklist hits record downloads, 19 February 2015
16. ISF: Corporate Governance Requirements for Information Risk Management. Information Security Forum, UK
17. von Solms, S., von Solms, R.: Information Security Governance. Springer, New York (2009). ISBN 978 0 387 79983 4
18. Al-Omari, A., El-Gayar, O., Deokar, A.: Information security policy compliance: the role of information security awareness. In: Proceedings of the American Conference on Information Systems, US (2012)
19. Al-Omari, A., El-Gayar, O., Deokar, A.: Security policy compliance: user acceptance perspective. In: Proceedings of the 45th Hawaii International Conference on System Sciences, Maui (2012)
20. Stackpole, B., Oksendahl, E.: Security Strategy. Auerbach Publications, Boca Raton (2011)
21. Van Grembergen, W., De Haes, S., Guldentops, E.: Structures, processes and relational mechanisms for IT governance. In: Strategies for Information Technology Governance, pp. 1–36. Idea Group Publishing, Hershey (2004)
22. ISACA: COBIT5 for Information Security, United States: Information Systems Audit and Control Association, ISACA (2012)
23. Visser, J.: Building Maintainable Software. O'Reilly Media Inc., Sebastopol (2016)
24. Khan, J.: The need for continuous compliance, pp. 14–15, June 2018
25. Forsgren, N., Humble, J.K.G.: Accelerate: The Science of Lean Software and DevOps: Building and Scaling High Performing Technology Organizations. Lean IT Strategies LLC, Portland, Oregon (2018)
26. ITGI: COBIT Mapping: Mapping of CMMI for Development V1.2 With COBIT. IT Governance Institute, ISBN 1-933284-80-3, United States of America (2007)
27. Koning, E.: Assessment Framework for DNB Information Security Examination. De Nederlandsche Bank, Amsterdam (2014)
28. Powell, S., Baker, K., Lawson, B.: Errors in operational spreadsheets. J. Organ. End User Comput. **21**(3), 24–36 (2009)

29. Volchkov, A.: How to measure security from a governance perspective. ISACA J. **5**, 44–51 (2013)
30. Papazafeiropoulou, A.: Understanding governance, risk and compliance information systems the experts view. Inf. Syst. Front. **18**(6), 1251–1263 (2016)
31. Deloitte: Spreadsheet Management, Not what you figured (2009)
32. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS Q. **28**(1), 75–105 (2004)
33. Bobbert, Y., Mulder, J.: Enterprise engineering in business information security. A case study & expert validation in security, risk and compliance artefact engineering. A comparative analysis of a security measurement tool. In: EEWC 2018. LNBIP, vol. 334, pp. 1–25. Springer (2019)
34. Johannesson, P., Perjons, E.: An Introduction to Design Science. Springer, Cham (2014). Stockholm University
35. Wieringa, R.: Design science as nested problem solving. In: Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, New York (2009)
36. Bass, L., Holz, R., Rimba, P., Tran, B., Zhu, L.: Securing a deployment pipeline. In: 3rd International Workshop on Release Engineering. IEEE ACM (2018)
37. COSO: Leveraging COSO Across the Three Lines of Defense. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), United States (2015)
38. McKinsey: Disruptive technologies: advances that will transform life, business, and the global economy. The McKinsey Global Institute (2013)
39. Silic, M., Back, A.: Shadow IT – a view from behind the curtain. Comput. Secur. **45**, 274–283 (2014)
40. Bobbert, Y.: Maturing Business Information Security. IBISA, Utrecht (2010)
41. Humble, J., Farley, D.: Continuous Delivery. Pearson Education Inc., New York (2011)
42. Bobbert, Y.: Defining a research method for engineering a Business Information Security artefact. In: Proceedings of the Enterprise Engineering Working Conference (EEWC) Forum, Antwerp (2017)