Cloud Compliance Risks

Bob Duncan[*],Yuan Zhao[†]
Business School
University of Aberdeen, UK
Emails: [*]robert.duncan@abdn.ac.uk,[†]y.zhao@abdn.ac.uk

***Abstract*—In the current business climate, there is an ever growing need for companies to comply with a range of legislation, regulation and standards. There is also a need for companies to be transparent in demonstrating that they are in compliance and due to the nature of certain cloud weaknesses, this can prove to be problematic. Given the potential magnitude of fines for non-compliance, there is a strong incentive for companies to be able to clearly demonstrate full compliance. In this paper, we investigate what these challenges are, and suggest a means to resolve these issues so that cloud users stand a better chance of achieving compliance and reducing the risk of exposure to huge fines.**

Keywords–Risk management; Cloud vulnerabilities; GDPR compliance.

I. Introduction

It is very much the case today that all computing systems are continuously under attack. Due to the multi-tenancy nature of cloud computing, this presents additional challenges with respect to achieving a good level of security and privacy for all cloud users. Of course this is not the only challenge they face. Over and above the need to achieve and maintain a high level of security and privacy for good business reasons, there is an additional requirement that most are subject to. That requirement stems from the need to be transparent to a range of legislative, regulatory and standards bodies, depending on the industry in which they operate. This requirement is usually satisfied by achieving compliance with the legislation and regulatory rules they must comply with in order to provide assurance to the relevant regulators.

We have seen some change in these areas over recent years. For example, with the ISO Security Standards in the ISO 27000 series, they have quietly been effecting a shift away from the old "Plan, Do, Check, Act" approach to a new risk based approach. This seeks to better understand the risks faced by users wishing to adopt the standards in order to ensure they adopt the right mitigatory approaches, or at least understand better the risks they face and are prepared to accept. The Cloud Security Alliance (CSA) has long being identifying and recording all cloud vulnerabilities and has been recommending technical solutions, but now also provide an identification of both the risk faced, as well as the potential impact that a breach might have on the company.

Regulatory authorities have been evolving in the range and scope of regulations being implemented across the globe, and the new EU General Data Protection Regulation (GDPR), which became live on 26 May 2018, now has some serious teeth to ensure compliance by all companies who fall under its scope.

There are already a huge range of legislative Acts, which have been passed across the globe in different jurisdictions to try to safeguard shareholders and other stakeholders from the effects of losses arising from poor security. While many of these are outdated when considering their effectiveness against cloud issues, there is no doubt that many are going through an updating process, and there are many more new pieces of legislation in the pipeline. Many governments are reactive, rather than proactive, so are often running behind the evolution of technology.

In Section II, we consider a number of legislative, regulatory and standards compliance requirements to provide a flavour of the scale of the problem faced by cloud users, while in Section III, we consider what kind of challenges are faced by cloud users when seeking to achieve compliance with these requirements. In Section IV, we consider how to address these challenges, and how best to attempt to mitigate the substantial risks cloud users face. In Section V, we discuss our findings, and in Section VI, presents our conclusions.

II. Compliance Requirements (Legislation, Regulation, Standards)

Legislation, Regulation and Standards — are they not all the same? The answer to that is no, they are not. We will use the UK to illustrate the differences. Legislation comes from Acts of Parliament, which are passed by Government to ensure behaviour across society as a whole is controlled on pain of penalty, to ensure the country is run properly and that all citizens and companies behave in an appropriate manner.

Legislation can include criminal proceedings for the worst cases, which can include large fines and even jail sentences. This can cover the behaviour of citizens, companies, indeed even other countries who might have belligerent intent. There will also be legislation to organise how government will perform certain duties, such as the Taxes Acts, which are regularly updated to reflect the changing resource needs of the country as a whole. Compliance is mandatory under force of law.

Regulation has long been used for the control of regulated industries, such as accounting and audit, advertising, agriculture, charities, competition and markets authority, direct marketing authority, education, engineering council, environment agencies, equality and human rights commission, film classification, financial industries, including banks, insurance, investments and so on, food production, forensic science, fundraising, gambling commission, gaming board, gangmasters licensing authority, health, information commissioners office, legal system, other professional organisations, planning inspectorate, press regulation, Scottish housing regulator, security industry authority, social care, transport, such as air, rail, road and sea transportation and, utilities, such as power generation, petroleum, oil and gas, water and sewage industries.

For each of these industries, regulators were appointed under statute to oversee the industry, and were granted certain powers to ensure each industry behaved in an appropriate way. Some had very little power, relying instead on companies “doing the right thing” rather than using enforcement. Of course in many cases it became necessary to have additional powers to ensure proper compliance with the regulations in place. Sometimes the regulator can only suggest a course of action, sometimes they have the right to levy sanctions and fines, and in worst cases, can withdraw the license for the company to operate within that regulated industry. Compliance is mandatory under the terms of the regulations, which are implemented under the guidance of the regulator.

Standard setting has been around a very long time. It is intended to provide a blueprint for, in this case, companies to carry out processes and activities to a common standard agreed by all to adhere to. Compliance is nowadays a voluntary process. The incentive for companies to adhere to common standards is that where large companies are compliant, there is a knock on impact to the supply chain, which encourages them to be compliant in order to gain business contracts from the larger companies. The gain for the larger companies is that they can trade easily with their peers, and where smaller companies in the supply chain are also compliant, the large compliant company gains better comfort in doing business with the smaller companies, leading to a win win situation for all who become compliant. This is usually also good news for the customer, since such compliant companies usually always perform to a much higher standard than those who are not compliant.

There is also the possibility of compliance being required with industry best practice. Some industries have set up their own body to conduct research into providing ‘best practice’ guidelines for all industry members. In this way, the industry can be seen to be transparent in its approach to ensuring all industry body members adhere to high standards of behaviour.

For some companies, this means they will face a raft of compliance requirements across a broad range of legislation, regulation, standards and best practice requirements. This means they will require to implement a means of tracking their compliance with each measure. This will be an ongoing requirement.

Of course, all these compliance challenges will not only be restricted to business issues relating to the industry within which they operate. Nowadays, there is a huge increase of compliance requirements arising from business use of computer systems, and in particular the storing of sensitive information, or data.

If we consider the security and privacy of data, then compliance in the UK would be required with the Data Protection Act, the EU GDPR, and possibly the ISO/IEC 27000 series of standards, and perhaps even industry standards, such as the PCI/DSS industry standard for online payment systems.

Compliance with each will be mandatory. Penalties for noncompliance can be significant. In a recent breach of privacy, the Information Commissioners Office (ICO) — the regulatory body for the UK, fined Newham Council in London £145,000 for a privacy breach of a small amount of data on 203 individuals whose un-redacted data records, collected by the Metropolitan Police legally in their fight against crime, was distributed by the council to 44 groups in contravention of the Data Protection Act . The French GDPR regulator recently fined Google $57 million for lack of transparency on giving clear instructions to new users on what they are signing up for.

The impact of a compliance breach of the ISO/IEC 27000 series will be more subtle. If compliance cannot be maintained, then the company may not use the ISO/IEC 27000 compliance logo on all their stationary and websites. The impact from this will be that other ISO/IEC 27000 compliant companies, will be less inclined to trade with such a company, which could result in the loss of significant revenues over time. A breach of say the PCI/DSS industry standard could in a worst case result in that company having the ability to accept payment cards to collect cash from customers withdrawn, resulting in a potential adverse impact on cash flow.

III. Cloud Compliance Challenges

Computer systems are continuously under attack, and cloud systems are no exception. No computer system is immune to attack, and that is certainly the case for cloud systems. During the past decade, a great many research papers, such as [1]–[14], have made many suggestions, which have improved the level of security and privacy offered in cloud systems. Despite these efforts, no complete solutions have yet been found to resolve the cloud forensic problem.

After an attacker breaches a cloud system, gaining even a small foothold, and becoming an intruder, their next task is usually to try to escalate privileges until they can access and modify, or delete, the forensic log trail to hide all trace of their incursion into the system. This gives them the means to dig deep in order to retain a long term foothold within the system, which allows them to help themselves to whatever data they wish over time. Their primary goal is to achieve this as quickly as they possibly can. They are often able to achieve this task within a very short time frame. This presents a major compliance challenge.

These attackers and intruders are often aided by the lack of scrutiny of server logs evident in many corporate systems. Often, companies neither retain records of which database records have been accessed, nor by whom. This means that once breached, the company will no longer have the ability to understand which records have been accessed, copied, modified, deleted or ex-filtrated from the system, meaning they will be unable to report this incursion to the necessary people or authorities. This will result in an immediate state of noncompliance with the GDPR, resulting in a potential exposure to sanctions or fines. In order to achieve compliance with the GDPR, companies must be able to report a breach within 72 hours of discovery.

Globally, the average time for all companies between breach and discovery in 2012 was an average of 6 months [15] [16]. This had improved to some 4 weeks by 2016 [17] — still far short of what is needed to understand what has been going on with the intruders while they were undiscovered. However, because the EU changed the requirement to report from within 72 hours of breach arising, to within 72 hours of discovery of the breach, companies stopped trying so hard, resulting in time between breach and discovery in 2017 returning to almost as high as 2012 levels, at just under 6 months [18]. This relaxation misses the point that the longer an intruder remains in a system undetected, the more damage or harm they can

ISBN: 978-1-61208-703-0

cause. Considering the fact that encryption is not a requirement of the GDPR, then in a case where a company chooses not to encrypt, the damage caused by undetected mass leakage will very much mean there will be little leeway to claim mitigation when it comes to the eventual inevitable fine by the regulator.

When a company uses cloud, and particularly, where any Internet of Things (IoT) use is included, this raises the question as to just how feasible compliance might really be. Compliance within such a tight time schedule could be all but impossible. Where a company using cloud is breached, and particularly where no special arrangements to ensure the safety of forensic and audit trail data has been made, the 72 hour deadline is moot. With no means of knowing that the company has been breached, there will be nothing to report, exposing the company to huge potential fines. Naturally, ignorance of the fact that a breach has arisen will not be accepted as a mitigatory factor. Once discovery eventually does occur, usually through third party sources, there will be no prospect of ever finding out precisely which records have been compromised, as once they are gone, the forensic and audit trails are gone forever.

In the case where a company uses IoT devices, this can present additional security issues. Most IoT devices are cheaply made, with minimal resources, and frequently with insufficient or no security. The biggest issue is not really the loss of the IoT device data, rather it is the fact that a skilled intruder can easily leverage these compromised devices to gain access to other more sensitive systems. Bear in mind that the Mirai virus started as a simple attack on individual IoT devices, which progressed to seeking out and leveraging other higher powered devices at scale to perpetrate massive Distributed Denial of Service (DDoS) attacks, and from there, once Mirai had been ported to be able to attack Windows machines, to then penetrate sensitive PC networks. Thus, any company utilising IoT devices will have a range of additional compliance risks to face. We do not specifically address the IoT issues here, but recognise that any company using any IoT devices must take special measures to ensure GDPR compliance can be achieved.

Of course, there are additional vulnerabilities to consider. The business architecture of a company comprises a combination of people, process and technology [15], not technology alone. It will be no surprise to learn that attackers have developed approaches to attack each of these three elements of the business architecture. People attacks are generally undertaken through social engineering attacks, which while often relatively simple to perpetrate, are frequently very successful. Attacks on business processes have become more of a problem, and this has been recognised by the Open Web Application Security Project (OWASP) [19]. They regularly identify weaknesses in web based systems, mobile systems, cloud systems and IoT systems. They recommend techniques to mitigate these weaknesses. Naturally, there are a great many attacks perpetrated on the technology of businesses, and the Cloud Security Alliance (CSA) [20] also maintain a full list of these attacks, what to do to mitigate them, what the likely impact might be and thus, how serious the effect on the company.

Every company that does not take special measures to safeguard their forensic and audit trail data will be at much greater risk of becoming non-compliant, thus exposing them to the inevitable breach occurring, leading to the possibility of huge fines. Their ability to discover that a breach has occurred, will be very slim indeed. In the event that they do discover the breach, they would struggle to understand what they need to report. This is very likely to be a factor in raising the level of the fine to which they would be liable.

There is no doubt that the longer an intruder remains hidden inside a company system, the more damage they are likely to be able to carry out. Where the company is unable to discover the breach within 72 hours of occurrence, it is highly unlikely that they will ever be in a position to discover the breach, let alone understand which records have been compromised. With no forensic or audit trails to follow, it will be completely impossible to determine what to report. However, as will inevitably happen, the breach becomes public knowledge, at which point, the regulator will become involved. If it can be shown that the company was negligent in its approach to safeguarding this Personally Identifiable Information (PII) of data subjects, the penalties will doubtless be significant. There is no requirement specified in the GDPR to encrypt data. However, there is certainly a very strong recommendation that this should happen, and within a reasonable time. The regulation also suggests that encryption and decryption keys should not be stored on the cloud instance. Failure to implement encryption properly will certainly lead to stiffer fines in the event of a breach.

Thus, we need to consider addressing the following risk areas:

- Credit Risk
- Liquidity Risk
- Market Risk
- Operational Risk
    - Cloud Operational Risk
    - Cloud Forensic Problem Risk
    - IoT Operational Risk
    - Monitoring Failure Risk
    - No Encryption Risk
    - Business Architecture Risk
        - People Risk
        - Process Risk
        - Technology Risk

Thus, in the next section, we shall take a look at how cloud users should address these risks, and will consider whether this will be adequate for cloud compliance with the GDPR.

IV. How to Address and Mitigate Cloud Compliance Risks

Taking a risk based approach is an excellent way to identify potential exposure to risks. This requires the proper identification of the risks faced by the business, the probability of the risk materialising, the cost of mitigation against the financial impact should the risk materialise. Identifying and recognising all the relevant areas of potential exposure is the first step in the process. Companies do not necessarily have to mitigate every risk, as they might choose to accept any risk if they believe the have the appetite to do so. We can see that there will now be a considerable number of categories of risk to address. We will consider each in turn, with our suggestions on what should be done to ensure compliance.

1 Credit Risk Credit risk is more frequently an issue in financial institutions where banks, for example, lend money to companies and individuals. Credit risk is the risk that the borrower will default on their payment. However, all companies provide lending to their customers in the form of trade accounts, which offer credit terms, with many using cloud based accounting systems, and this can add an additional element of risk to the equation. In addition, where the customer is an EU resident, the company is required to achieve GDPR compliance. Also, many companies provide loans to other companies when they have a huge cash surplus, as they can often obtain far greater rates of return than currently on offer from their banks.

2 Liquidity Risk Liquidity risk is the risk that a company or bank may be unable to meet short term financial demands, otherwise known as 'running out of money.' This can arise due to the difficulty of converting some security or hard asset into cash, from poor management of debtors, or over-extending through poor cash management. There can be many other factors which can cause this risk, but the effects can be catastrophic.

3 Market Risk Market risk is more frequently seen in financial institutions, where banks, for example, experience losses due to failings in the overall performance of the financial markets in which they are involved. Companies may also experience losses due to the way they make both short term and longer term investments of surplus business funds.

4 Operational Risk This area generally addresses all remaining risks and it is clear that the risks in this area are growing significantly.

4.1 Cloud Operational Risk

- **4.1.1 CSP Risk** The use of market leading, experienced cloud service providers familiar with legal and regulatory requirements for safeguarding customer data and other sensitive data;
- **4.1.2 Backup and Recovery Risk** Backup, redundancy, and recovery are at the core of the decision to use an outsourcing vendor with highly redundant and resilient data centres designed for mission-critical applications;
- **4.1.3 Internal Control Risk** Internal controls and security processes must ensure customer information is appropriately segregated and protected by industry-standard compliance policies;
- **4.1.4 CSP Hardware Environment Risk** Leading cloud providers continuously improve their hardware environments to ensure the latest versions of operating systems are installed and use agile software development to deploy feature/function releases on an accelerated basis;
- **4.1.5 Tailored Cloud Deployment Risk** The use of tailored cloud deployment options to meet your specific needs including private clouds solely deployed on your behalf, or a hybrid cloud consisting of shared hardware but segregated data storage would be a prudent move;
- **4.1.6 IT Outsourcing Risk** Outsourcing portions of your information technology infrastructure can free up internal IT resources to focus on strategic initiatives and new product development;
- **4.1.7 Financial Services Risk** Providers with financial services domain expertise reduce complexity and risk for Financial Institutions with their extensive knowledge of global standards, communications protocols and file formats;
- **4.1.6 CSP Global Support Center Risk** Cloud providers with global support centres can provide 24 x 7 support in multiple languages, ensuring your international clients and regional offices have access to the support resources required as problems arise.

- **4.2 Cloud Forensic Problem Risk** This is a huge potential problem unless special arrangements are in place, e.g., a secure forensic and audit trail is maintained using a high security immutable database [21]–[24], and examination of all system access requests to determine the authority of all users to have authorised access to the system. Use of intrusion detection and authentication technology to automate the monitoring for attack attempts is also necessary [25];
- **4.3 IoT Operational Risk** IoT devices used for any purpose by cloud users present a considerable risk, mainly due to the often cheaply made devices with little or no security, often vulnerable to the Mirai virus, which can allow attackers to gain access to systems and to further compromise the main PC and server network due to the porting of the Mirai virus to be able to attack Windows computers [26][18];
- **4.4 Monitoring Failure Risk** We need to understand the 5 Ws – Who, from Where, When did they access the database, What did they see, modify, delete or exfiltrate from the system [27][28]? This allows us to infer the Why so that we can understand their motivation. Simple monitoring and analysis of system logs will go a long way to mitigate the well known exploits currently in active use by attackers [24]. Some, like [29]–[31] propose the use of data provenance to ensure the integrity of data, with others proposing a new method of cloud forensic audit to assure the provenance of the data [32];
- **4.5 No Encryption Risk** Encryption is a good thing to consider [33], but there are caveats – first, the encryption and de-cryption keys must not be kept on the cloud instance. The encryption should be carried out offline in the cloud users' own systems before being transferred to cloud. Done properly, this can provide serious mitigation to the new EU GDPR fine levels, because if an intruder does get into the cloud system, all they get is meaningless data. With strong levels of encryption, it becomes practically impossible to crack [34] (of course, all this could change with the development and evolution of quantum computing, although there is little doubt that once quantum computing becomes an everyday reality that CSPs will introduce quantum cloud to address this issue).
- **4.6 Business Architecture Risk**
  - **4.6.1 People Risk** People are generally seen as the weakest link in any company, and are particularly prone to social engineering attacks. The company needs to keep abreast of these attacks and ensure all people in the company are regularly trained to understand the risks.

- **4.6.2 Process Risk** Processes are often well documented, but also can be woefully out of date. Attackers know to exploit these areas, sometimes in conjunction with social engineering attacks. OWASP are taking a more informed view of dealing with these kinds of attacks.
- **4.6.3 Technology Risk** This is where companies are exposed to highly technical attacks. The CSA has done some good work on identifying these risks, as well as offering good strategies to mitigate the risks.

Many of these issues have been around for many years. In 2011, NASA [35] were one of the early organisations to recommend using a risk based approach for identifying, recognising and dealing effectively with operational risk, particularly where complex IT systems are in use.

Failure to deal properly with the above risks could lead to very serious compliance breaches, which can trigger punitive levels of the fines imposed by the regulator. However, these risks can generate further risks in regard to business diminution; loss of share value; reputational damage risk; an emerging era of potentially serious regulatory fines, the serious expense of forensic investigations after a breach, and the impact on business continuity.

V. Discussion

As is now becoming clear, GDPR compliance will be far from easy to achieve, and for cloud this will be especially problematic and challenging. For a great many organisations, the GDPR brings a great many risks to bear when considering compliance with the GDPR. They come from a great range of sources, and the biggest risk of all is likely to come in the form of failure to recognise just how important it is to identify and mitigate these risks properly.

There are a great many companies will not be able to recognise these risks, particularly where they do not have the financial clout to provide the right level of expertise. The result is that they will be even more exposed than those who do have the means to recognise and address these risks. There can be no doubt that these risks are significant, and potentially devastating for the company should they fail to achieve compliance with the GDPR. A law firm, Cleary Gottlieb [36], provide a GDPR watch service, where they try to clarify how successful breaches might be dealt with.

We hope this paper might provide them with a starting point to consider what is required to achieve compliance, and what the implications might be for compliance failure. The steps outlined here are straightforward to implement. The most important point being that in order to deal with a risk, the company must first recognise the risk, and in order to do that, must have an understanding of what these risks are and how they might go about mitigating the potential impact of these risks.

Companies will need to carry out some serious testing in order to find a satisfactory equilibrium between security, privacy, performance, reliability, accessibility and the accountability we require for GDPR compliance. We plan to conduct a pilot case study on how the technical aspects might be implemented in order to meet all the required goals to ensure compliance can be achieved. This will run around a miniature cloud system, offering both cloud-based and non-cloud based systems to assess what the optimum configuration might be. This will allow us to ascertain how well the cloud-based solution can match the capability of the non-cloud based system, after taking into account the impact of the cloud forensic problem.

VI. Conclusion

For any company using cloud, it is clear that it will prove impossible to achieve compliance with the GDPR in the event of a security breach where they have not at least dealt properly with the as yet unresolved, cloud forensic problem. Claiming ignorance of this problem following a cyber breach will not be sufficient grounds for mitigation of the fine by the regulator after the fact. It will certainly be too late by then. Thus, cloud users who must be compliant with the GDPR will have to take steps now to be thoroughly prepared ahead of time.

We have looked at traditional cloud operational risks and the new risks relating to coping with these unresolved problems and discussed how to go about resolving them, using wherever possible simple, yet effective, approaches to ensure a robust solution that will be both easy to implement and easy to maintain. By this means, we can eliminate a large amount of the risk. We accept that all risk will not be entirely removed, but there is the possibility to make a significant reduction in risk levels involved. More importantly, it will be possible to demonstrate a high level of compliance with the GDPR to the regulator in the event of breach arising.

Implementing these proposals should ensure that a healthy level of compliance can be achieved, without the need for expensive, complex solutions that could prove highly expensive to implement and maintain.

References

[1] M. Felici, “Cyber Security and Privacy: Trust in the Digital World and Cyber Security and Privacy EU Forum 2013 Brussels, Belgium, April 18-19, 2013 Revised Selected Papers,” in Commun. Comput. Inf. Sci. Springer International Publishing, 2013, vol. 182 CCIS, pp. 77–88.

[2] Y. Y. Haimes, B. M. Horowitz, Z. Guo, E. Andrijcic, and J. Bogdanor, “Assessing systemic risk to cloud-computing technology as complex interconnected systems of systems,” Syst. Eng., vol. 18, no. 3, 2015, pp. 284–299.

[3] C. Millard, I. Walden, and W. K. Hon, “Who is Responsible for ’Personal Data’ in Cloud Computing? The Cloud of Unknowing, Part 2,” Leg. Stud., vol. 27, no. 77, 2012, pp. 1–31.

[4] R. K. L. Ko et al., “TrustCloud: A framework for accountability and trust in cloud computing,” Proc. - 2011 IEEE World Congr. Serv. Serv. 2011, 2011, pp. 584–588.

[5] R. K. L. Ko, B. S. Lee, and S. Pearson, “Towards achieving accountability, auditability and trust in cloud computing,” Commun. Comput. Inf. Sci., vol. 193 CCIS, no. PART 4, 2011, pp. 432–444.

[6] N. Papanikolaou, S. Pearson, and M. C. Mont, “Towards Natural-Language Understanding and Automated Enforcement of Privacy Rules and Regulations in the Cloud: Survey and Bibliography,” Analysis, 2011, pp. 1–9.

[7] S. Pearson, “Taking account of privacy when designing cloud computing services,” Proc. 2009 ICSE Work. Softw. Eng. Challenges Cloud Comput. CLOUD 2009, 2009, pp. 44–52.

[8] S. Pearson, “Towards Accountability in the Cloud,” IEEE Internet Comput., vol. 15, no. 4, jul 2011, pp. 64–69.

[9] D. Pym and M. Sadler, “Information Stewardship in Cloud Computing,” Int. J. Serv. Sci. Manag. Eng. Technol., vol. 1, no. 1, 2010, pp. 50–67.

[10] T. Takahashi, Y. Kadobayashi, and H. Fujiwara, “Ontological Approach toward Cybersecurity in Cloud Computing Categories and Subject Descriptors,” in Sci. Technol., 2010, pp. 100–109.

[11] L. J. Sotto, B. C. Treacy, and M. L. Mclellan, “Privacy and Data Security Risks in Cloud Computing,” World Commun. Regul. Rep., vol. 5, no. 2, 2010, p. 38.

[12] J. Bacon et al., “Information Flow Control for Secure Cloud Computing,” IEEE Trans. Netw. Serv. Manag., vol. 11, no. 1, 2014, pp. 76–89.

[13] N. Papanikolaou, S. Pearson, M. C. Mont, and R. Ko, “A Toolkit for Automating Compliance in Cloud Computing Services,” Int. J. Cloud Comput., vol. x, no. x, 2014, pp. 45–68.

[14] C. Chang and M. Ramachandran, “Towards Achieving Data Security with the Cloud Computing Adoption Framework,” IEEE Trans. Serv. Comput., vol. 9, no. 1, 2016, pp. 138–151.

[15] PWC, “UK Information Security Breaches Survey - Technical Report 2012,” London, Tech. Rep. April, 2012. [Online]. Available: www.pwc.com www.bis.gov.uk [Retrieved:March 2019]

[16] Trustwave, “2012 Global Security Report,” Tech. Rep., 2012. [Online]. Available: https://www.trustwave.com/Resources/Library/Documents/2012-Trustwave-Global-Security-Report/ [Retrieved:March 2019]

[17] Verizon, “2016 Verizon Data Breach Report,” Tech. Rep., 2016.

[18] Verizon, “Verizon Security Breach Report 2017,” Tech. Rep., 2017.

[19] OWASP, “Open Web Application Security Project,” 2019. [Online]. Available: https://www.owasp.org/index.php/OWASP_Cloud_Security_Project [Retrieved:March 2019]

[20] CSA, “Cloud Security Alliance,” 2019. [Online]. Available: https://cloudsecurityalliance.org/ [Retrieved:March 2019]

[21] B. Duncan and M. Whittington, “Cloud cyber-security: Empowering the audit trail,” Int. J. Adv. Secur., vol. 9, no. 3 & 4, 2016, pp. 169–183.

[22] B. Duncan and M. Whittington, “Creating and Configuring an Immutable Database for Secure Cloud Audit Trail and System Logging,” Int. J. Adv. Secur., vol. 10, no. 3&4, 2017, pp. 155–166.

[23] B. Duncan, “Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing?” in Cloud Comput. 2018 Ninth Int. Conf. Cloud Comput. GRIDs, Virtualization, no. February. Barcelona, Spain: IARIA, 2018, pp. 1–6.

[24] B. Duncan, A. Happe, and A. Bratterud, “Using Unikernels to Address the Cloud Forensic Problem and help Achieve EU GDPR Compliance.” in Cloud Comput. 2018 Ninth Int. Conf. Cloud Comput. GRIDs, Virtualization, no. February. Barcelona, Spain: IARIA, 2018, pp. 1–6.

[25] M. Neovius and B. Duncan, “Anomaly Detection for Soft Security in Cloud based Auditing of Accounting Systems,” in Closer 2017 - 7th Int. Conf. Cloud Comput. Serv. Sci., Porto, Portugal, 2017, pp. 1–8.

[26] B. Duncan and M. Whittington, “Cyber Security for Cloud and the Internet of Things: How Can it be Achieved?” Cybersecurity Inst. Eng. Technol., vol. Cybersecur, no. September, 2017, pp. 1–39.

[27] B. Duncan, M. Whittington, M. G. Jaatun, and A. R. R. Zúñiga, “Could the Outsourcing of Incident Response Management Provide a Blueprint for Managing Other Cloud Security Requirements?” in Enterp. Secur. Springer B. 2016, V. Chang, M. Ramachandran, R. Walters, and G. Wills, Eds. Springer, 2016, pp. 1–22.

[28] B. Duncan, A. Bratterud, and A. Happe, “Enhancing Cloud Security and Privacy: Time for a New Approach?” in Intech 2016, Dublin, 2016, pp. 1–6.

[29] T. F. J. Pasquier, J. Singh, J. Bacon, and D. Eyers, “Information Flow Audit for PaaS Clouds,” in 2016 IEEE International Conference on Cloud Engineering (IC2E), 2016, pp. 42–51.

[30] N. Papanikolaou, T. Rübsamen, and C. Reich, “A Simulation Framework to Model Accountability Controls for Cloud Computing,” CLOUD Comput. 2014, Fifth Int. Conf. Cloud Comput. GRIDs, Virtualization, no. c, 2014, pp. 12–19.

[31] T. F. J. M. Pasquier and J. E. Powles, “Expressing and Enforcing Location Requirements in the Cloud using Information Flow Control,” Proc. - 2015 IEEE Int. Conf. Cloud Eng. IC2E 2015, 2015, pp. 410–415.

[32] B. Duncan and M. Whittington, “Can Forensic Audit Help Address the Cloud Forensic Problem in Light of the Requirements of the Forthcoming European Union General Data Protection Regulation?” in Cloud Comput. 2018 Ninth Int. Conf. Cloud Comput. GRIDs, Virtualization, no. February. Barcelona, Spain: IARIA, 2018, pp. 84–89.

[33] V. Chang, M. Ramachandran, Y. Yao, Y. H. Kuo, and C. S. Li, “A resiliency framework for an enterprise cloud,” Int. J. Inf. Manage., vol. 36, no. 1, 2016, pp. 155–166.

[34] T. Pasquier, B. Shand, and J. Bacon, “Information Flow Control for a Medical Records Web Portal,” Cl.Cam.Ac.Uk, 2013, pp. 1–8.

[35] M. Stamatelatos and H. Dezfuli, “Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners,” NASA, Tech. Rep. December, 2002. [Online]. Available: http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf [Retrieved:March 2019]

[36] Cleary, “Cleary Cybersecurity and Cyber Watch,” Cleary Gottlieb, 2019. [Online]. Available: https://www.clearycyberwatch.com/2018/01/notification-data-breaches-gdpr-10-frequently-asked-questions/. [Retrieved:March 2019]