Issues in Information Systems
Volume 24, Issue 3, pp. 174-180, 2023

DOI: https://doi.org/10.48009/3_iis_2023_115

Sentry insurance and california consumer privacy act: a business case on IT governance, data security, and compliance

Riley Mueller, *Sentry Insurance, MuellerRa17@uww.edu*
Roger Yin, *University of Wisconsin-Whitewater, yinl@uww.edu*

Abstract

This case paper discusses how Sentry Insurance, a provider of commercial and personal insurance, can effectively implement the California Consumer Privacy Act (CCPA) using ITIL service management and COBIT governance framework. The CCPA regulates the handling of consumer data, and compliance is crucial for businesses operating in California. The article highlights key aspects of ITIL, such as service strategy, service operation, and continuous improvement, that can help Sentry Insurance protect customer data and comply with CCPA requirements. It emphasizes the importance of event management, access management, and problem management in ITIL service operation to ensure data security and address any issues promptly. The article also explores how COBIT can assist in meeting stakeholder needs, creating a dynamic governance system, ensuring a holistic approach to decision-making, distinguishing governance from management, and tailoring the framework to enterprise requirements. By utilizing these frameworks, Sentry Insurance can successfully implement CCPA regulations and safeguard customer data.

Keywords: insurance company, CCPA, IT, governance, data privacy, cybersecurity, risk, compliance

Introduction

Sentry Insurance is an insurance provider of both commercial and personal insurance ranging from manufacturing, real estate, golf courses, long-haul trucking, horticultural, business life insurance, motorcycle, and nonstandard auto insurance (Sentry Insurance, 2023). In the financial services industry, regulatory compliance is quite common, and the introduction of the California Consumer Privacy Act of 2018 is no exception to another law Sentry must account for especially considering they have customers all throughout the United States, including in California.

The California Consumer Privacy Act of 2018 (CCPA) is an act that specifically deals with how companies handle and manage consumer data. The CCPA was signed into law in September 2018, but various updates have been made since then, including amendments in 2019, additional bills in 2020, and a ballot initiative in November 2020 (Shatz & Lysobey, 2021). These various amendments all have different specifics that enhance or clarify the CCPA in one way or another and implementing all these items can be confusing if not fully understood. Making sure consumers have privacy rights is still at the core of all these enhancements. Therefore, diving into these regulations and how they affect the financial services industry, especially Sentry Insurance, is critically important to their continued business operation and expansion in the future.

Sentry Insurance has already implemented significant aspects of ITIL service management, including service operation, and has also embraced distinct governance from leadership through the COBIT

framework. However, to ensure consumer data protection and comply with the CCPA, Sentry Insurance needs to emphasize further other crucial elements of ITIL service management and the COBIT governance framework. This expansion will enable the organization to enhance its practices and successfully meet the requirements of the CCPA.

ITIL Service Strategy

Amid the digital transformation era, being able to continue completing the business objectives but making sure to comply with all regulatory items is a struggle that Sentry Insurance continues to have in an ever-changing technology world. Being able to implement appropriate ITIL Service Strategy items is a significant first step into making sure consumer data stay secure and complies with the essential aspects of the CCPA. (Gillingham, 2023)

Sentry Insurance needs to make sure all aspects of the CCPA are implemented and maintained accurately. Customer data are highly sensitive and personal, and the reason California has gone with the approach of requiring companies to implement protection for their customer data. As already seen from the original writing in 2018, there have been amendments and ballot propositions that have changed the requirements of the CCPA. This may not be the last change we will see to this act, or another act may be implemented to tighten regulations. Having a plan for this implementation of the CCPA is beneficial in the long run as the skeleton of the plan can also be used in the future. (Gillingham, 2023)

A strategy for implementing aspects of the CCPA could look like fully understanding all the regulatory items of the CCPA (or changes as we have already seen), defining what services or internal changes are needed to make sure customer data is protected, and what strategies will be needed to make sure the data is protected going forward. These are all significant steps toward having a service strategy. Things will always need improvement, but a few strategies in place to start is better than nothing and something that can be built on and improved going forward. (Gillingham, 2023)

ITIL Service Operation

Incorporating the event management aspect of ITIL service operation would greatly benefit Sentry Insurance as it allows them to keep up to date on any changes in customer data and make necessary to the retention or security of that data. Event logging is a key part of event management as it allows for a detailed record of any changes. This can include access by internal associates and changes they make, such as a name or address change. No matter what is changed, keep in mind to secure the customer's data is always the number one priority and a necessary part of the CCPA. (Corrigan, n.d.)

Access management is another key part of ITIL service operations, as only the people in related job roles with the necessity for work should have access to the data. It means someone from the internal accounting team should not have access to a specific customer's claim information, but the claim representative responsible for that claim should. Not only is protecting customer data essential but making sure appropriate people can see and manage that customer data is an important aspect of protecting the customer's data. (Corrigan, n.d.)

The other aspect of ITIL service operation that relates to CCPA and protecting customer data is problem management. If there are problems with the systems used to manage and track customer data, correctly mitigating those problems is crucial. If the problems are not addressed as they should be, that could leave consumer data in a vulnerable and unprotected state. Getting the issues resolved will be a top priority to

make sure CCPA regulations and guidelines are followed and correctly in place if anything were to not be operational as expected. (Corrigan, n.d.)

ITIL Continual Service Improvement

To keep evolving with the management of consumer data and keeping in line with the CCPA, Sentry Insurance can use the steps of the ITIL continual service improvement. The first and arguably the most important part is identifying your approach for improvement. If you do not know in what direction you need to go for improvement, all the other steps are just shooting blind as you don't have a clear direction you should go in. Defining the measurements is the second step in making sure you have continuous improvement. This can go hand in hand with some of the logging and access management we mentioned earlier. These systems can be part of the measurement of how much data is being accessed and where from. In addition to this, Sentry also must make sure to collect and process the data in a way that is able to be analyzed effectively. This is the data of how consumer data is being accessed and by whom. There are a lot of types of data being thrown around and making sure to clarify what should be measured is key to my approach. (Gillingham, 2022)

After the data has been analyzed, then teams can meet and present the data. This should only be internal to Sentry and only on the Data Governance and executive levels as we want to make sure the consumer data is being seen by as few people as necessary but making sure the information is secure falls on the Data Governance Team, the Chief Information Security officer (CISO), and the Chief Information Officer (CIO). They are the ones who will make the appropriate decisions and be the ones eventually responsible for all customer data handling. Once improvements have been implemented, the process can start over as needed. (Gillingham, 2022)

COBIT Meeting Stakeholder Needs

COBIT is a leading framework when it comes to meeting stakeholder needs, and this is a key component of making sure customer data is secure and in compliance with the CCPA. Stakeholders in this situation are both the customers and the internal Information Governance team at Sentry. (Simplilearn, 2023)

Another great benefit that the COBIT framework provides is making sure everything is consistent, which is a great aspect of meeting stakeholder needs. The underlying reasons for need may not drastically change, but the things that fulfill those needs certainly will as the CCPA and the world around us changes. Having a consistent framework in place will better position Sentry to adapt to those changes and still meet all the needs of stakeholders, both internal to Sentry and their customers. Makings were sure the Sentry associates and its customers are both taken care of is core to who Sentry is. Adapting when needed is part of making sure everyone is taken care of. At some point in time, everything may not be steady in the world, but having a rock-solid framework such as COBIT is a great thing Sentry can implement in coordination with their compliance for CCPA. (Simplilearn, 2023)

COBIT Dynamic Governance System

The dynamic governance system and meeting stakeholder needs do go hand in hand quite a bit, as being able to adapt but also keep the stakeholder needs at the forefront is key in keeping Sentry Insurance's customer data governed and secure.

As mentioned before, the CCPA has already changed several times since its inception only five years ago. So, it is only a matter of time before it changes or gets amended again, and due to this, a dynamic governance system is needed to help adapt to change as it happens.

When the change happens, Sentry Insurance should have the ability to adapt and change as needed. Being able to take advantage of the dynamic governance aspect of COBIT allows Sentry to be well-positioned as things change. Having a dynamic view over the Information Technology Enterprise Governance (EGIT) allows for the ability to make governance changes as needed. With IT being an ever-changing field, the governance of data, and specifically customer data, are part of that as well. (Rafeq, 2019)

COBIT End-to-End Governance System

Decisions made by IT departments in a company almost always impact the business, and Sentry is no exception. Making sure to recognize that IT governance decisions extend further than just IT and all throughout the business. Not only do the governance decisions extend outside of the IT part of the business, but business decisions may have impacts on IT governance as well. (ALC, n.d.)

With both ends of the spectrum, the decision makers must think about the other parts of the business when making a decision, such as an example of moving into new territory. This isn't Sentry's current case but an easy one to relate to in this scenario. That new territory could be California by the business unit, but it brings in IT Governance heavily as well due to the CCPA regulations. This is just one example of many that apply to both sides of the aisle when it comes to these decisions.

The entire business impact is not something always thought of for business decisions but something that is very important to keep in mind from the IT Governance space as you are asking the business to sink costs into regulatory items that don't directly make money. Being secure and being in line with regulatory items will keep you in business both because of the laws you have to follow and the overall perception of your business. The business will not be in a good spot if you don't have a good reputation for keeping customer data secure. You soon won't have new customers or keep your current ones.

COBIT Ensuring a Holistic Approach to Business Decision Making

Previously we discussed making sure to think of other parts of the business when making decisions, and that plays directly to another COBIT framework of making sure there is a holistic approach to any business decisions. (Simplilearn, 2023)

A holistic approach to business was tapped into already by keeping the other parts of the business in mind when decisions are made, but we can tap into that a little further with this specific COBIT framework aspect. Managing risks is a complicated endeavor and something that can affect an entire organization, so making sure to account for other parts is a key part of successful governance. This also comes into play in making other business units aware of any governance items you are implementing, as they will only be able to stay in line with your governance policies or recommendations if they know about them. So, making sure to keep them in mind and updating the other business units as changes will make really plays into the holistic approach to decision-making as well.

COBIT Distinct Governance from Management

Arguably something that can get confusing is governance and overall management and how they are separate. An important part of COBIT that Sentry will benefit from is making sure there is a clear distinction between governance and overall management. (ALC, n.d.)

IT governance and management require two separate organizational structures, and that is the main reason why these two need separate approaches. Sentry has a lot of internal IT and various organizational business units. These all require their own processes and therefore require the governance and management to be separate. The same policies used to manage a finance team or even an IT team are separate from what is needed for IT governance. (ALC, n.d.)

Implementing the CCPA will fall into the IT governance space but may also need some management overview to help with compliance and implementation on the business side of things. The best way to approach this for Sentry would be to make sure all leaders of teams are well aware of the requirements of the CCPA. These leaders are then responsible for managing how their team stays up to date on issues and staying in compliance. One may think compliance and management would meld together during this, but they need to be separate in order to be successful.

COBIT Tailored to Enterprise Needs

The final COBIT aspect that Sentry Insurance will benefit from in relation to the compliance of CCPA is making sure everything is tailored to the enterprise's needs. Sentry Insurance is an enterprise that is similar to others in its field but not exactly the same as any other company. Making sure to adapt the framework adapts to Sentry is key to making it work. (Rafeq, 2019)

Making COBIT work for Sentry allows them to position themselves for success. All the other parts of COBIT allow Sentry to make it work for them. To be compliant with all the parts of the CCPA, Sentry needs to make everything work for how they operate at a base level and how they best serve their customers. This also includes protecting their data not only to comply with regulatory items but to protect the individuals as a best practice for the interest of their customers. If they don't protect their customers and their data, they may not have customers in the future. Insurance is about protecting your customers when the worst things imaginable happen to them or their companies. Protecting their data so it cannot be used against them or be hacked and exploited is another way to take care of your customers.

Conclusion

After examining the various ITIL and COBIT framework items that Sentry Insurance can use to help implement the CCPA in an effective manner for the organization to succeed. The various ITIL policies are able to help us streamline a service strategy, service operation, and continuous improvement implementation of ITIL for Sentry Insurance and their application to CCPA. Also, the various COBIT framework items we can streamline were meeting stakeholder needs, dynamic governance system, end-to-end governance system, ensuring a holistic approach to business decision-making, distinct governance from management, and tailoring COBIT to enterprise needs. Utilizing all these different framework items, Sentry should be well-poised to implement all requirements of the CCPA.

Recommended Questions

1. *Why should governance and management be separate for Sentry to stay compliant with the CCPA?*

2. *Why does Sentry need to make the COBIT framework work for their enterprise?*

3. *What does ITIL's service strategy allow Sentry to do in their CCPA implementation?*

4. *Why should Sentry consider a holistic business approach when implementing the CCPA?*

Suggested Answers

1. Governance and management need to be separate as the underlying organizational structure is different for both of those and therefore, each requires their own approach when it comes to Sentry's implementation of the CCPA.

2. Sentry is a unique organization and is not the same exact as any other organization; therefore, requires a unique approach to projects, and the CCPA implementation is no different. Sentry should do whatever they need to do to make sure the COBIT framework works for them in this instance.

3. Sentry Insurance can utilize service strategy to fully understand the regulatory items of the CCPA (or changes as we have already seen), define the internal changes that are needed to make sure customer data is protected, and what risk management strategies can ensure the data is protected going forward.

4. All decisions made by the IT department, or the business unit areas affect all other aspects of the business. By using a holistic approach, Sentry can make sure all other aspects of the business are accounted for when implementing changes and especially the CCPA requirements in this instance.

References

ALC. (n.d.). *The 5 key principles of COBIT 5 | ALC Training News*. Retrieved March 12, 2023, from ALC: https://www.alctraining.com.au/blog/the-5-key-principles-of-cobit-5/

Corrigan, L. (n.d.). *Understanding the 5 ITIL service operations processes*. Retrieved March 12, 2023, from Lucid Chart: https://www.lucidchart.com/blog/itil-service-operations

Gillingham, J. (2022, October 25). *ITIL Continual Service Improvement And 7-Step Improvement Process*. Retrieved March 12, 2023, from Invensis Global Learning Services: https://www.invensislearning.com/blog/itil-continual-service-improvement/

Gillingham, J. (2023, January 25). *ITIL Service Strategy: Process, Objective, Scope, Focus & Value*. Retrieved March 11, 2023, from Invensis Global Learning Services: https://www.invensislearning.com/blog/itil-service-strategy /

Rafeq, A. (2019, February 4). *COBIT Design Factors: A Dynamic Approach to Tailoring Governance in the Era of Digital Disruption*. Retrieved March 12, 2023, from ISACA: https://www.isaca.org/resources/news-and-trends/industry-news/2019/cobit-design-factors

Sentry Insurance. (2023). *About us*. Retrieved March 11, 2023, from Sentry: https://www.sentry.com/about-us

Shatz, S. P., & Lysobey, P. J. (2021). The California Consumer Privacy Act of 2018 Updated: More Protection in the Quest to Access and Protect Personal Information. *Buisness Lawyer, 76*(2). Retrieved from https://go-gale-com.libproxy.uww.edu:9443/ps/i.do?p=AONE&u=h2o&v=2.1&it=r&id=GALE%7CA660456176&inPS=true&linkSource=interlink&sid=bookmark-AONE

Shatz, S. P., & Lysobey, P. J. (2022). Update on the California Consumer Privacy Act and Other States' Actions. *Business Lawyer, 77*(2). Retrieved from https://link-gale-com.libproxy.uww.edu:9443/apps/doc/A705927116/AONE?u=h2o&sid=bookmark-AONE&xid=9801b4db

Simplilearn. (2023, February 21). *What is COBIT? Understanding the COBIT Framework [Updated]*. Retrieved March 12, 2023, from SimpliLearn: https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article

Smallwood, R. F. (2020). *Information Governance.* Hoboken: John Wiley & Sons, Ltd. Retrieved from https://doi-org.libproxy.uww.edu:9443/10.1002/9781119491422