Privasec

ISO 27001 CASE STUDY

HOW CANVA EMBARKED ON ITS CYBER SECURITY MATURITY JOURNEY AND ACHIEVED ISO 27001 CERTIFICATION

SUMMARY

Customer: Canva

Industry: Graphic Design software

Business: Graphic design and publishing platform with pre-built design templates

Employees: 1,375

CHALLENGES

To establish a strong security foundation in an incredibly fast changing and growing company

'Bake-in' security in a startup culture and operations for security to scale with the business

RESULTS

Established a security roadmap with ownership at founders and senior leaders' level

Improved security controls with a company-wide focus on security

Attained ISO 27001 certification

CYBER SECURITY FOR STARTUPS:
HOW TO ACHIEVE COMPLIANCE WITHOUT HINDERING CULTURE OR GROWTH

Canva

CUSTOMER BACKGROUND

Canva Pty Ltd is a leading graphic design giant and publishing platform based in Australia. Started in 2012, Canva is valued at US$6 billion and has more than 1,375 staff, making it one of Australia's fastest growing unicorn startups. Canva provides a graphic designing tool that is easy to use and comes with an abundance of pre-built designs and templates to facilitate the design process. Canva is regularly featured in the news for its values and culture, attracting key talents from across the world and is regularly listed as one of the best tech employers.

CANVA'S OBJECTIVES

"We are really particular about positive security and risk management outcomes because that is what's going to drive the growth in the future." - Geoff Chiang, Canva IT Risk Manager

CANVA WAS LOOKING BEYOND 'JUST' ISO27001 CERTIFICATION, FOR REAL SECURITY AND RISK MANAGEMENT OUTCOMES THAT WOULD HELP THE UNICORN SUSTAINABLY 'BAKE-IN' SECURITY INTO EVERYTHING THEY DO WITHOUT COMPROMISING ITS CULTURE NOR ITS GROWTH

KEY OBJECTIVES

1. Improve Canva's security posture and maturity by establishing a lasting risk management framework;
2. Implement security as a culture so that it is 'baked-in' in its operations and can inherently scale alongside the business;
3. Increase the enterprise market credibility and trust by accelerating the security initiatives already in play;
4. Toughen security ecosystem to reduce the likelihood of future information security breach.

WHY CERTIFICATION?

Canva has over 30 million monthly active users across 190 countries who have collectively created over three billion designs to date. Initially launched as a B2C platform, Canva quickly became the design application of choice for marketing and content creating teams within businesses, and now offers a fully fledged enterprise platform for larger business users.

Housing and protecting its IP as well as its users' data is mission-critical to Canva, which embarked on a significant security uplift journey at the back of a data breach in 2019. As part of this journey, Canva wanted to adopt a risk approach that would 'bake-in' security in its culture and operations.

Given the rapid growth in cyber attacks and the ever increasing footprint of Canva, Canva was also determined to demonstrate its security commitment to its users. Many of the professional users of Canva do require their suppliers and contractors demonstrate a secure environment as a mandatory requirement for doing business.

CANVA'S CHALLENGES

> We had to build a risk management framework from the ground up. Once something's in production, it's in legacy and it takes effort to keep up with security that gets introduced after you've jumped into a technology.
>
> Geoff Chiang, Canva IT Risk Manager

Think silicon valley fast-paced and agile technology company. That's Canva. The challenge was to establish a strong security culture within a fast growing company with a lot of competing priorities. With the constant change in an organisation that is continually building and incorporating technology at a rapid rate, there becomes a crucial need to 'bake-in' security in all operations so that it can grow and keep up with the pace of the business.

Canva also has a critical mission to ensure that the increasingly growing user information being amassed daily is secured and personal information exposure is reduced to a minimum. Lastly, to enable its incredible growth, Canvanauts (the people working at Canva) had historically been given huge autonomy and agility. Canva needed to preserve that culture whilst at the same time introduce better security governance and oversight in its operations.

KEY PARTNER CRITERIA FOR CANVA

Privasec, who had already worked with several tech giants, was no stranger to the Canva way of working and understood well its values, culture and the importance of implementing a solution which preserved them.

Beyond its proven track record of implementing ISMS certified to ISO27001, Canva chose to work with Privasec because of its cultural fit, flexibility, and the shared ideology in achieving security and risk management outcomes without hindering business growth.

> We needed someone who would take into account the state of Canva as it was before we start this project. Not only the state of our security and risk management maturity at the time, but also very importantly, the culture of the organisation. Privasec was very good at this. They had a high level of expertise, are very communicative and we had incredible engagement.

PRIVASEC'S SOLUTION

Privasec's governance approach is centered on the principle that 'no two organisations are the same'. This means no two effective Information Security Management Systems (ISMS) are ever the same. "As an organisation, we are based on very strong values of ownership, flexibility, and have an overall no-nonsense commitment that allows us to easily adapt to the working style at Canva," echoes Vivienne Mutembwa, Privasec's ISMS Consultant.

> What we wanted was someone who understood the journey, what our organisation looks like and how we operate. We did not want a cookie-cutter approach to things.

Privasec worked with Canva to design an ISMS around this constant growth and change that the team at Canva thrives on, ensuring that the methodology was customised to fit the culture and precise needs of Canva and its operations. This was an essential step in the implementation process – "if the risk methodology does not fit with how the business is run, the staff will be unable execute, resulting in a near certain breakdown of the ISMS in the longer term" explains Vivienne Mutembwa, ISMS Consultant at Privasec.

Implementing a system that every Canvanaut will, and can use themselves, was also a key consideration. Privasec typically offers its clients free of charge, a Microsoft SharePoint ISMS portal which Privasec has built and matured over years of practical security operations and auditing. This approach would not work with Canva, which needed something tailored to their existing productivity tools. Privasec was already very familiar with the tools and technologies used by Canva, using many of these daily. In addition to the fact that Canva did not have to purchase any new security governance platform, Canva's stakeholders were also much more willing to adopt the ISMS.

Privasec and Canva conducted over 40+ interviews and workshops, from the new starters to the founders, to identify and formulate security risks at a level that Canva could manage, along with an actionable list of items which would work with the organisation, existing culture, processes and technology choices.

> **THE TEAM AT CANVA HAS TRUELY BEEN INSPIRATIONAL BOTH IN EAGERNESS TO IMPROVE AND IN THEIR DEDICATION TO GET THINGS DONE**
>
> **VIVIENNE MUTEMBWA, ISMS CONSULTANT**

RESULTS

- Canva implemented an ISMS specifically designed to best meet its ways of working and its ever-changing organisation;
- Security was given organisational level priority and is owned directly at the founder level;
- Canva achieved certification to ISO27001. Privasec acted on behalf of Canva through the certification process;
- Canva successfully set up a team of security champions across the different group functions, ensuring all key business stakeholders are involved, and are having conversations about security.

> **"I THINK IT'S FAIR TO SAY THAT CANVA WOULD HAVE A MUCH TOUGHER JOURNEY WITHOUT PRIVASEC."**

Canva found it exceptionally helpful to have a Privasec representative guiding the team through the entire audit itself. "Facing off to the auditor was essential", Geoff remarked, "it was helpful to have someone who knew our organisation, and also what the auditor was looking for."

> In a well designed ISMS, everything flows naturally, driven by business need. You shouldn't have to do anything for the sole purpose of compliance. If you do, not only are you wasting time and money but you are potentially exposing yourself to a hard landing in the future.
>
> Romain Rallu, Privasec CEO

SETTING THE TREND

In the few months since its certification and using a risk approach to manage security, Canva grew its security investments and security resources 5-fold, with no plan to slow down or stop. Some of the brightest security minds in the industry have joined the security group which now has a dedicated response and adversarial simulation capabilities. Security uplifts are now baked in both company-wide and team-level goals and every Canvanauts know and understand why security is core to Canva's business.

"We could not have done it without your guidance. Thank you for helping us through it all!"

Cameron Adams, Co-founder, Canva

WHAT IS ISO 27001?

ISO 27001 is the international standard that sets out the specification for an information security management system ISMS. It contains a set of best practices to allow organisations to implement a world class risk management system to strategise and coordinate their security investments whilst getting marketable recognition for it.

Many organisations, including governments, are now insisting that their suppliers and contractors demonstrate that they manage security in compliance with ISO 27001.

WHAT DOES AN ISMS DO FOR YOU?

- Greater security awareness across all levels of the organisation
- Recognised certification & enhanced customer confidence and perception of the organisation
- Understanding and ownership of security risks by business leaders, and commitment to an actionable security improvement roadmap
- End to end visibility & centralised view of security risks
- Make easier investment decision with better business cases based on risks
- Translates cyber security problems into tangible business impacts

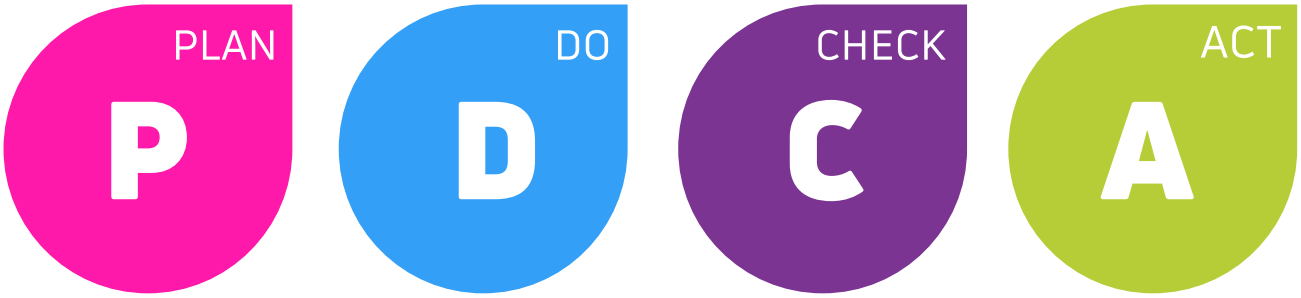
"We used the certification as a framework to prioritise security roadmap and have an external entity that holds Canva accountable for milestones defined.

Paulywn Devasundaram, Canva Engineering Leader"

IMPLEMENTATION

ISO 27001 Clauses 4 to 10 prescribes the minimum requirements of the ISO 27001 standard for the establishment of an Information Security Management System (ISMS). It follows the continuous improvement cycle - Plan-Do-Check-Act (PDCA) - which an organisation must establish in order to be able to go through certification.

1. Plan – Identify Risk to the Confidentiality, Integrity and Availability (CIA) of assets
2. Do – Put relevant controls in place
3. Check – Audit the implementation for efficiency and effectiveness
4. Act – Improve ineffective or inefficient controls



To design the best possible system, Privasec begins by understanding the business environment, business objectives, constraints, values and culture. Privasec then conducts an initial information risk assessment to identify the actions and priorities for managing information security risks. This highlights major gaps and areas for improvement, which allows Privasec to create an associated and tailored risk treatment plan. Lastly, Privasec helps its clients to remediate their gaps and executes an internal audit program to report on security control effectiveness, progress of risk remediation and provides assurance back to the business for review and action.

To ensure that its client are fully prepared for its certification audit, Privasec leverages the internal audit process to help stakeholders get familiarised and comfortable with the process. Privasec also liaises with the chosen Certification Body to guide the entire process and acts on its client's behalf during the certification audits.

ABOUT PRIVASEC

Privasec is one of the fastest growing independent security, governance, risk and compliance consulting firms in South East Asia and Australia. We are driven by business outcomes bridging the gap between the technical and business worlds to create meaningful business cases and enhance decision making. To learn more about us and our services, please visit our website: https://www.privasec.com/