Bud's Journey to ISO27001 Certification

An article by Ryan Howells, Information Security Manager, Bud Systems

"A pass with no non-conformities". That is the phrase every security manager wishes to hear at the end of their ISO 27001 implementation journey. Thankfully at Bud Systems, that was the exact phrase that came out of the auditor's mouth when delivering his concluding statement.

Our ISO 27001 journey wasn't as plain sailing as it sounds, however.

It started way back at the start of 2019. It was only the previous year we had addressed GDPR compliance in time for the new legislation in May 2018, and we had already achieved Cyber Essentials Plus the year before. But ISO 27001 is a completely different beast to tame.

We were optimistic, naive, and had been led astray by some outside help that we had instructed to guide us on our way to achieving the certification.

Ironically, that outside help in itself could have been deemed a risk at the time, and had we already had a fully functioning ISMS in place, then our journey would have taken a very different path to start.

Although this obstacle in our journey set us back a bit, it actually turned out to be our saving grace. We decided to bring the mammoth task of implementing an ISMS in house.

While the prospect of this – with no previous experience of implementing ISO 27001 – was daunting, it proved to be the best decision we made. After all, who knows our own systems, and vulnerabilities better than us?

So, it was time to get familiar with this beast called ISO 27001. The ISO 27001 standard is comprised of mandatory management system clauses and 114 suggested risk-reducing controls.

The clauses act as a basis for any security management systems and ensure you have buy-in from top management, have adequate risk management, and ensure that security is ingrained into the base of company.

The suggested controls, however, may or may not apply to the business processes of the business, so can be excluded if you deem it to not be applicable.

For example, if you don't have a network because everything is in the cloud then you may choose to exclude control A13.1.1 Network Controls.

Once you take the time to read through the standard then it soon becomes apparent, that all the clauses are interconnected on a path to guide you through your journey of a logical implementation.

Why are we doing this?

If you don't know why you are implementing an ISMS to achieve ISO 27001 certification then you will fail at the first hurdle. This is where you meet the first of the mandatory clauses.

Luckily at Bud, our senior management team proactively engages with the rest of the company on a daily basis, and it is clear that we all share a common goal.

A SWOT analysis was a good way to help top management understand the benefits of what we were looking to achieve, and also helped guide our journey by identifying opportunities for improvement, strengthen our weaknesses, and address the threats we were hoping to remove.

Why ISO 27001 is important to Bud

- Embeds a culture of security first throughout the organisation
- Has ensured staff have information security understanding at all levels from when they very first start working at Bud
- Ensures all Bud employees proactively address security throughout all business operations
- Cements our expertise in the state-of-the-art technologies and supported services used throughout Bud
- Sets Bud as an industry leader in the market
- Attracts top talent across all departments

Information Assets

After obtaining buy in from senior management through a business case, the first real activity was to identify all the information assets at Bud Systems.

The main principle behind any security standard is protecting the confidentiality, integrity and availability or your information assets. Workshops were held throughout the business to identify all the information assets we had.

Each information asset was assigned a value based on the importance of their confidentiality, integrity and availability and then we discussed potential threats and vulnerabilities against these assets.

Not only did this allow us to identify risks, but it also ensured that the heads of functions, or more so the information asset owners became more aware of the importance of protecting their information, thus engraving the culture of security.

Free pizza

As well as having the mandatory documents required by the standard, the most important part of ISO 27001 is that the ISMS is actually alive. In other words, the plans, policies, and procedures are really put into practice and that all employees understand and comply with them.

Without any of it really working in day-to-day practice, then you could have perfect documentation but still fail the certification. At Bud, we decided to introduce mandatory security lunches on a weekly basis leading up to the audits.

As interesting as that sounds to anyone in security, it may not prick the ears of others quite as much. If you add free pizza to the meeting, then it suddenly becomes more appealing to those who don't get excited by a notification of a breach.

> The free pizza … I mean the highly interesting security awareness sessions were a success, and every employee could recite where to find anything security related when asked like it was a verse from their favourite song.

And they were asked, being randomly chosen by the auditor and pleasing him with their knowledge – even knowing the definitions for C, I, A.

Don't Be Afraid to Ask for Help

One of the requirements for the ISO 27001 stage 2 audit is to have completed an internal audit.

The internal auditor can't be someone who has implemented any of the controls and given the tight timeframe we had set ourselves, this meant that we didn't have time to train someone to perform an internal audit.

Something which helped greatly with our audit was engaging with an external consultant who had previous experience of conducting ISO 27001 audits for the very certification body we had chosen.

This meant our internal audit process was not only efficient but proved to be valuable as we were given a direction of how to approach a security control from someone with a lot of experience.

The Certification Body

Something that was reiterated throughout our audit, and something which is now imbedded into our supplier due diligence process, is choosing a reputable certification body.

What we gained from the audit was much more than just the certificate, we gained excellent insights into the best solutions for ISO 27001 from an auditor with lots of experience.

When the Stage One audit was conducted, although the auditor gave us some non-conformities, it was also part of a lesson, and some valuable tips on how to resolve the issues were also given.

The Audit

Our six-day Stage Two audit consisted of 5 days on site and one day off site for the auditor's report writing. Each day felt like a massive win as we completed the day with no non-conformities found.

An audit plan had already been provided in advance of the audit, so we knew what to expect on which day.

This, coupled with a Statement of Applicability that mapped to the documentation or process (thanks to the Stage One tip), meant we were armed to answer any questions around any of the security controls we had, or hadn't put in place.

The audit worked like clockwork and rather than feeling like a week-long integration, it eased into casual conversations and discussions between security lovers and techies alike.

Lessons Learnt

> If I was to give any advice for anyone else going through the ISO 27001 journey, then it is to give yourself enough time.

With time comes experience, and from each security incident, security meeting, security lunch we learnt something, and learnt how to make it better for the next time.

The whole ISO 27001 certification process is not only about showing how you've identified issues, but also how you've improved for the next time.

Giving yourself enough time allows you to evidence how your ISMS is an ever-evolving machine striving for improvement, and this is what will impress your auditor most.