Waterstons
we're with you

+44 345 094 0945
www.waterstons.com

Case study

Sector Professional Services
Service Cyber Security

Apr 2021

Gold Standard Security for People's Postcode Lottery

Highly successful People's Postcode Lottery (PPL) run charitable lotteries to raise money for good causes. Since 2005 they have raised in excess of £700 million for good causes. Due to the nature of their business, PPL are required to abide by regulations outlined by the Gambling Commission. These regulations extend to ensuring that appropriate security controls are in place to protect players of the lottery. However, to provide greater reassurance to players and regulatory bodies, PPL decided to 'go for gold' by signing up for ISO 27001:2013 certification.

Results at a glance

- Player confidence that data is held securely
- Regulatory compliance through ISO 27001:2013 certification
- Holistic security controls implemented across areas of people, process & technology
- Programme of continual improvement established

ISO 27001:2013 certification is considered to be the gold standard when it comes to information security best practice, demonstrating commitment to data protection, resilience and control of information security. While the Gambling Commission currently requires operators to implement just a subset of the standard's security controls, PPL set out to implement all 114 controls, meeting all the requirements of the ISO27001 specification. In successfully doing so, PPL have shown their commitment to protecting the data entrusted to them by players and established their position as a champion of security best-practice within their sector.

With those 114 controls to implement, the first question is “where do I start?” Having done our own journey to ISO 27001:2013 certification, we were able to help PPL put a plan and structure in place to ensure they met the necessary requirements on time, and on budget. In addition our plan understood PPL’s business style which allowed us to increase security and reduce risk whilst avoiding unnecessary red tape and bureaucracy.

Implementation

Working closely with PPL, we designed a programme to achieve certification, which had five simple stages; Step 1 – work out where they currently stood.

To get the full picture we completed workshops with every department within PPL to map all of the critical people, processes and technologies which support business operations.

The outcomes of the workshops provided us with a list of critical assets, key systems and vital information across the organisation. We then worked with PPL stakeholders to identify potential risks, and, drawing on our knowledge of security best-practice, opportunities for improvement as part of an official risk assessment. We soon had a “risk treatment plan”, setting out prioritised tasks and projects to further improve security covering the three key streams of people, process and technology.

> **“Waterstons’ partnership approach meant they worked side by side with us like one of our team to make sure our ISO 27001 project was not only a success but delivered real value right across the business.”**
>
> John Young
> IT Security Manager

Armed with the plan, and once again working closely with PPL stakeholders, we set about delivering the tasks in those three key streams in parallel (Steps 2, 3 and 4):

The ‘People’ stream was focussed on training and awareness – bringing improvements to existing staff handbooks and designing a tailored security programme to help teams remember the security fundamentals in day-to-day operations. With the help of the creative heads in PPL no sooner had we said “remember to lock your screen!” than we were awash with custom coasters, postcard guides and colour coded document templates that were used to help deliver clear security messages.

We also set up a security forum in the business, which acted as a hub for teams to provide feedback on changes and raise opportunities for improvement. Finally we put in place regular management reviews to ensure that consistent security briefings were provided, strategic decisions could be made effectively and direction was provided from senior management.

The ‘Process’ stream was centred on documenting security policies and procedures across the business. Using existing documentation, we worked with our PPL partners to establish what the ISO standard calls an ‘Information Security Management System’ where all relevant documentation is gathered in one place, helping to make security part of everyday operations.

To ensure business processes were repeatable and associated risks were understood, we completed a number of workshops with PPL stakeholders. These involved collaborating with multiple departments across PPL and led to us identifying ways to make processes not only more secure, but also more efficient.

The ‘Technology’ stream worked closed with PPL’s IT team and software developers to create a service catalogue of key systems and their owners. In our review of these systems we considered how information was protected, and identified ways to reduce the risk of this data being compromised. Our technology specialists then worked alongside PPL to implement a number of improvements such as protecting logging information offsite, implementing encryption, and identifying ways to ensure data would always be available securely even in the event of a disaster scenario such as loss of power, which would force relocation to an alternative site.

Once we had covered all the areas outlined in the ISO 27001:2013 standards we set about the final stage of the journey; Step 5 – Review and Improve. We trained a team of PPL staff as internal auditors able to review the effectiveness of security processes and systems. Compiled audit reports were reviewed within the security forum and actions taken to further improve the effectiveness of security controls. PPL were committed to living and breathing security best-practice, not just simply seeing ISO 27001:2013 certification as a ‘tick-box exercise’. The review stage was key to maintaining momentum and driving further security improvements across the organisation.

Using the tried and tested ‘Deming cycle’ of ‘Plan-Do-Check-Act’ to structure the security programme we successfully implemented all the required controls outlined by the international standard for data security. From December 2016 to January 2017 PPL invited external auditors to independently assess their new Information Security Management System, and it was confirmed that it met the requirements of the standard; with PPL successfully accredited to the much sought-after ISO 27001:2013 certification.

The Benefits

PPL are now able to provide assurance to their players and regulatory bodies that security is, has always been, and remains a priority for their organisation. Players of the People’s Postcode Lottery can be assured that potential risks to their data are continuously under review, with steps taken to protect it using the latest technologies and best-practice security controls.

An added, and unexpected bonus is that PPL colleagues have highlighted that collaboration between departments is much improved. The security programme has helped to agree standard processes for change management within the organisation, for example, which is now followed consistently. In addition, the regular security forums provide a focal point for improvements to cross-department processes, improving efficiency as well as increasing security.

We’ve also worked closely with PPL colleagues to transfer knowledge and skills which allow them to effectively run their Information Security Management System without external support. Undoubtedly, as the business continues to grow, new challenges will arise; however PPL now have a framework in place to manage and mitigate new risks and are well equipped to ensure that the information they handle is protected from an ever-evolving landscape of threats. They can provide confidence in their security controls and resilience, to both players and regulators, as they continue in their quest to raise even more money for good causes.

"Following our ISO 27001 certification we can now send a clear message to both players and regulatory bodies alike that security is of paramount importance to our organisation"

John Young
IT Service Manager

Finally, this engagement has also shown that ISO 27001:2013 is not an impossible task even for a large and complex organisation like PPL; but that it can be used to drive improvement across a business, and deliver real value. We were able to work in partnership with PPL to ensure that operational effectiveness, and the cultural values which make them who they are, were never compromised by introducing red tape or bureaucracy. As in all our work, we took a pragmatic approach, tailoring the standard to meet the needs of their business and which allowed them to achieve the Gold Standard in data security, giving confidence to players, and regulatory bodies alike, that data security is top priority.