

## CAS Certified to ISMS Class

### About the Company

Founded in 1969, CAS (Computer Application Services Ltd) has an enviable record of delivering excellent value ICT solutions and services on time and within budget. Employee owned, CAS is a model of financial stability and delivery-focused management. CAS's speciality is supplying business critical software, systems and consultancy to both public and private sector organisations. CAS has worked to develop and apply customised software solutions to unique business needs and provides a full range of IT solutions including consultancy, application development and support services.



CAS's consultants have extensive experience gained across a variety of organisations in both the public and private sectors. The organisations Complaints Management System is used throughout the UK by Ombudsman services, CAS has built up considerable knowledge of best practices in the complaint and enquiry handling area. Other CAS customers include UK Armed Forces, United States Air Force, Local Authorities, Scottish Government, Universities and others.

As a List-X registered company all its staff are security cleared. CAS experience in the military sector demonstrates its ability to work to strict quality guidelines, PRINCE2 project management processes and to deal with sensitive and secure information. In addition the organisation is a Microsoft Registered Partner and a Borland Connections Partner.

### Business Drivers Behind The Project

CAS realised that protecting its corporate and customer's information has become the greatest challenge facing today's information technology (IT) professional. With nearly 40 years experience providing IT services to both Government and industry, CAS is able to help its clients avoid the pitfalls and business risks that arise as new threats and technologies evolve. Information Security is therefore key to CAS's business and operating an ISO27001 certified Information Security Management System (ISMS) was a priority.

"The ISO27001 certification project was driven by our customer's requirements," comments David Wells, Managing Director of CAS. "CAS works predominantly within the public sector and it has become a requirement for working with many public sector bodies to demonstrate compliance with ISO27001 as a sign of good practice."

CAS was already certified to ISO9001 and the whole organisation adhered to strict Quality guidelines. As CAS was a certified body the staff there understood the challenges for achieving ISO27001, but more importantly that certification to the standard would provide an excellent framework for proactively protecting organisational information.

### Choosing the Right Partner

CAS had initially carried out a gap analysis several years ago, the purpose of which was to gauge the work required to ensure the organisation became ISO27001 compliant and achieve certification to the standard. Due to limited resource to allocate to the project, it had stalled but as CAS's clients became more security focussed, the management team realised that certification to ISO27001 was a must.

"We knew that we needed to achieve certification to ISO27001 to maintain competitive in our market place," said David. "We wanted a quick turnaround and aimed to achieve compliance in 12 months, but at the same time we knew that we did not have enough experience in house to move this forward."



CAS met with a number of consultancy firms with the aim of finding a partner to guide them through the 12 month certification project. One of the organisations to tender for the project was leading IT security consultancy, Sapphire.

Sapphire's consultant, Andrew Parry, provided the CAS management team with a thorough scoping document which outlined tight deadlines and clear milestones for the organisation to achieve in order to meet the 12 month target for certification.



## SAPPHIRE

David Wells said "Sapphire itself was certified to ISO27001, this gave us a lot of confidence in its consultant's experience. The individuals we spoke to within Sapphire had a great in depth knowledge of the standard and felt passionately about Information Security. In addition to this, CAS was aware that Sapphire also played a major part in the promotion of information assurance and I have attended its annual conference, the National Information Security Conference in the past. In my opinion, this gave the organisation a high level of credibility."

### The Project

CAS engaged Sapphire and tasked the consultancy firm with achieving certification in a strict timescale. The requirement was to implement a fully operational ISMS which was fully integrated with its existing certified ISO9001 quality management system. The project took 12 months to complete. An information security forum was established and an Information Security Manager appointed who worked alongside Andrew Parry (Sapphire's appointed Security Consultant) to develop the framework management system and implement security improvements throughout the organisation in line with ISO27002 the best practice information security standard.

Pete Murray, Information Security Manager at CAS was responsible for driving the certification project internally. "Although CAS was largely compliant, we needed to tie down the documentation and formalise the process for feedback and incident reporting" comments Peter. "For several years we had been trying to develop a concept of ownership and an information security culture. In the past we had taken a 'shotgun' approach, but working with Sapphire, we developed a structured approach to awareness and the change of culture worked well for us.

We now have a process for incident reporting and security is discussed at every staff meeting, not only at board level."



ISO27001 was integrated with ISO9001, this process was relatively straight forward as the existing quality standard provided a framework in place that could be utilised to operate key functions of the new ISMS including the existing incident reporting function, internal audit function and management review meeting which could be used as a vehicle for the ISMS review.

Pete went on to say, "Working with Sapphire enabled us to streamline our current security procedures. Their guidance allowed us to look at our existing procedures and focus on the important aspects of the ISMS, for example proper risk analysis and to quantify and qualify the security of every asset."



#### The Result

CAS was certified to ISO 27001:2005 in November 2008 by its ISO9001 certification body BM Trada.

By operating a certified ISMS CAS now ensures:

- Future security objectives are established
- Employee roles and responsibilities for information security are clearly established
- Highlights top level management commitment to Information Security
- Shows organisational wide commitment to information security
- States an acceptable level of organisational risk
- Establish criteria for accepting the risk
- Ensures compliance to policy through conducting internal audits
- Instils confidence for existing and potential customers

#### The Benefits

Pete Murray, Security Manager sees the practicality of achieving certification to ISO27001. "Working towards ISO27001 has enabled us to concentrate our efforts on the important areas of our business. Before working with Sapphire, we knew what needed to be done but found it difficult to prioritise the issues into critical and non critical areas. After the project, we had a clear idea of what security measures are to be maintained and improved on."

David Wells, Managing Director at CAS see's the benefits from a business perspective saying "the process of ISO27001 certification has been beneficial, we take a more structured approach to information security, therefore making the security process more efficient and productive. At the same time, we have the benefit of being able to tell our prospective and existing customers that not only do we comply with the standard, but we have achieved certification proving that we take security seriously."

#### In Conclusion

CAS intends to maintain its certification to ISO27001 and to use the skills acquired during the project to expand its current portfolio and provide ISO27001 consultancy services to its clients.

When asked to comment on the project and the service from Sapphire, David Wells said "Sapphire's consultants were flexible and friendly. Andrew Parry was our main point of contact throughout the project and had exceptional project management skills. He worked closely with our internal team to ensure that deadlines were achieved and that we hit every milestone when expected – achieving certification in 12 months as originally scoped."

