Acuity Group

the Specialists in
Governance, Risk & Compliance

Implementation

Integrated Management System

Change History

Version Number	Status	Date of Issue	Reason For Change	Change Control Reference
1.0	Awaiting approval	07/01/2016	Creation date	
1.0	Approved	12/01/2017		1.1

Quality Assurance

Name	Responsibility	Signature	Date
Author:			
Charles Critchley	Director, Acuity Group		11/01/2017
Approved:			
Stephen Hall	Director, Acuity Group		12/01/2017

Content

0.0 Executive Summary

International Standards compliance is increasingly becoming a mandatory contractual requirement for outsource services. However, there is a distinct difference between Certification Compliance and Operational Compliance.

International (ISO) Standards are adopting a common Management System structure, formalising the Plan, Do, Check, Act (PDCA) methodology.

'Plan', 'Check' and 'Act' are the core for the Management System and can be standardised across most standards, whether:

- Information Security Management System (ISMS), i.e. ISO 27001
- Quality Management System (QMS), i.e. ISO 9001
- Business Continuity Management System (BCMS), i.e. ISO 22301

We refer to this as an Integrated Management System (IMS) and is the priority for accelerating the initial phase of an ISO compliance requirement. Acuity has developed and implemented this methodology successfully for many large organisations, achieving huge savings in time, cost and ongoing management efficiency.

The Acuity IMS is guaranteed to achieve Stage 1 Certification.

'Do' relates to the implementation of Operational Controls specific to each Standard. Acuity will provide all core Control documentation and tools to achieve Stage 2 Certification in the shortest time possible. We anticipate participation in ensuring acceptance within the business which is crucial. Stage 2 certification is the area that is most likely to benefit from automation by software tools, or other techniques that support the company's culture, e.g. Intranet or Documentation Control system. This can be carried out as a subsequent phase as it is not critical to achieve the primary goal of Certification.

There is a choice of Standards Certification Bodies. We recommend the British Standards Institution (BSI). BSI certificates incorporate both the UKAS (UK Accreditation Service) and ANAB (ANSI-ASQ National Accreditation Board). The BSI is the only Certification body that can issue a Group Certificate that would meet UK (Europe and International), as well as specific USA business requirements.

1.0 Understanding

Maturing service and technology led markets are recognising Governance Risk and Compliance (GRC) solutions as the catalyst for new growth and consolidation of individual industry best practices into a single programme. The new business challenge is to combine multiple compliance standards management into a common integrated system, thereby simplifying deployment and achieving economies of effort through more efficient use of resources.

Key requirements of GRC solutions must include:

- Costs kept to a minimum, doing all possible to maximise the value of work already completed by internal staff and to reduce reliance on external resources (and cost)
- Clear planning, to facilitate internal resource scheduling to not compromise any existing operational activity and potential GRC data feeds.
- A natural integration into established and new operational programmes. Leveraging all existing capability, investment and operational resource.

Our solution will reduce business risk, improve management oversight, and help realise operational efficiencies by adopting accepted ‘best practice’. Standards Certification also presents a platform for enhanced brand value and marketing advantage.

See http://www.acuitygroup.com

2.0 About Acuity Group

Acuity Group: Un-complicating Governance, Risk Management and Compliance

Acuity Group exists to fulfill one objective, to make governance, risk management and compliance more accessible, more affordable and more profitable for all businesses.

A growing partnership between likeminded professionals and companies, Acuity Group is the only provider capable of a truly end-to-end and objectives-oriented GRC approach. Individually brilliant, the products, services and solutions offered by the Acuity Group partners come together to form a unique, powerful and comprehensive portfolio for corporate GRC.

Experienced in the delivery of **GRC**, **IMS** and **International Standards Compliance** solutions on a global scale, Acuity Group is the ideal partner for any business looking to satisfy such objectives without unduly diverting its attention away from the strategic direction.

We differentiate ourselves by:

- Fully Integrated Management Systems
  - International Standards (ISO) (Acuity Group Documented Methodology)

We attract business by:

Our **ambition, establishment, knowledge and innovations.**

- We have a fabulous track record, with each partner bringing a wealth of relevant and valuable experience. A true GRC solution company.
- We deliver exceptional levels of change and benefit to the organisations involved.
- We start where it matters, by increasing your profitability, reducing revenue loss and improving the value of what you do.
- We apply our framework of interlocking pillars, creating a cycle of integrity, resilience and improvement within your business.
- We innovate best practice and we apply them exceptionally well. We provide economic, automated ways of keeping things that way.

3.0 Integrated Management System

Proposal for Integrated Management System (IMS) Implementation.

General Objectives are to:

- Implement a complete and operational IMS for whichever standards are relevant to the organisation.
- Identify existing complementary business components and to integrate their management effectively into one enterprise wide framework.
- Present a fully aligned, Stage One, compliant Management System to International Standards Organisation (ISO) expectation and industry Best Practices (EICC).
- Present a comprehensive and complete set of 'tools' to capture, document and create all necessary records to drive 'operational compliance', maximising business value from the IMS investment.
- Identify and present 'automation' capability to rapidly mature the IMS, delivering better value and greater informed management information for potential business improvements.

General Scope of an IMS project includes:

- Fulfilling the above implementation objectives
- Production of operational deliverables or capabilities.
- All operational activities carried out across the entire UK enterprise.

Note: IMS Implementation is a necessary rapid precursor to accurately sizing the full extent of work required. For example:

ISO 22301 – Business Continuity
Business Impact Assessment (BIA), dependencies/needs.

ISO 27001 – Information Security
Assessing Confidentiality; Integrity and Availability (CIA) and risk against a Statement of Applicability (SoA) to agree business minimum control requirements.

ISO 14001 – Environmental Management
Applying legal and/or regulatory requirements against appropriate identified environment aspects, associated to the business.

ISO 9001 – Quality Management
Governance/Dashboard view of adherence and performance to process measures over agreed corrective and preventative action.

OHSAS – Health and Safety
Conducting the number of possible risk assessments against the registered number of identified hazards.

Corporate Social Responsibility (CSR)
Evaluating the Human Rights and Business Ethics of the organisations 'Code of Conduct and Ethics' documentation for; Human Rights, Labour and Anti-corruption.

3.0 Integrated Management System

Continued…

General Programme

To ensure a successful implementation of a fully integrated management system and to guarantee maximum skills transfer to the client, enabling self managed operational ownership.

Underpinned by as much consultant and client interaction as possible for the duration of the IMS implementation.

An IMS implementation will deliver:

- Up to 11 modules to establish **management control** over the operational deliverables of the required standards.
- Up to 13 modules to deliver **operational compliance** of the required standards.
- A full set of documentation books, covering the;
    - Planning
      Scope, design and requirements of the complete management system.
    - Delivery
      A bespoke set of operational manuals for each compliant standard/location.
    - Culture
      Centrally managed requirements to maintain the life and accuracy of the IMS.
    - Assessment
      Centrally management requirements to review and improve the operational achievements of the IMS/Business.

- A full set of Microsoft Office technology ‘tools’ to capture, document and create all necessary records to drive ‘operational compliance’.
- A stage one compliant product, ready for a full stage two external 3rd party audit for a single site, 6mths after implementation engagement starts.

Future

Replicate and knowledge transfer the IMS framework across, as appropriate, to a choice of our GRC software products/partners to demonstrate operational efficiency and scalability.

3.0 Integrated Management System

Continued…

General Assumptions that the Business will:

- Provide an authorised readily accessible senior contact for the duration of the project.
- Provide prompt access to any reasonably requested information, facilities or resources.
- Review and sign off each accepted deliverable within 2 weeks of submission by Acuity Group.

General Approach is in five stages:

Based on a FULL IMS implementation of: CSR; ISO 22301; 27001; 14001; 9001 & 45001 for a single site.

Stage	Detail	Effort (md)	Elapsed (wks)
1. Preparation	Initial meeting to set detailed project terms of reference (scope, security, NDA, project contributors etc...)	3	1
2. Discovery	Information gathering and high-level review and understanding of the current business model, known risks; organisation, technology, operations, influencers and enablers etc...	20	8
3. Analysis & Design	a) Scope b) Objectives c) Policies d) Guidelines	15	5
4. Construct & Implement	a) Documentation Sets (Deployment Bundles) b) Record Repository (File and Folder Structures) c) Refining Tool Sets (Adapt, Adopt and Apply as appropriate) d) Consultation and Awareness Sessions (IMS Participants) e) Deployment Schedules f) Audit Checks g) Management Review	35	15
5. Management	Administration and contingency.	7	3
TOTAL		**80**	**32**

4.0 Benefits of ISO Standards

The Acuity Group GRC IMS methodology affords you complete control over your IMS implementation and supports the development of your internal knowledge and capabilities. After obtaining the IMS methodology, you can literally implement your complete system without external support and enjoy the business benefits of achieving ISO and/or other standards.

Business Continuity is the process by which a company makes sure it can still function in the event of total, or partial, loss of its internal or external support systems, people or facilities.

Benefits of ISO 22301 include:

- Protecting the long term health of your customers.
- Developing a 'blue print' to get the business back on its feet.
- Understanding your own dependencies and across those of your suppliers.
- Capturing and retaining the knowledge of how your business operates.
- Reassures stakeholders of the quality of your corporate governance.

Information is critical to the efficient running of any organisation
Regardless of the size of your business, an accredited ISO/IEC 27001 management system independently confirms your organisational risks are properly identified, assessed and managed, while formalising information security processes, procedures and documentation.

Benefits of ISO 27001 include:

- Demonstrates the independent assurance of your internal controls and meets corporate governance and business continuity requirements.
- Provides a competitive edge by meeting contractual requirements and demonstrating to your customers that the security of their information is paramount.
- Proves your senior management's commitment to the security of its information.
- The regular assessment process helps you to continually monitor your performance and improve.

Environmental impact is becoming an increasingly important issue across the globe, with pressure to minimize impact from a number of sources: local and national Governments, regulators, trade associations, customers, employees and shareholders.

Benefits of ISO 14001 include:

- General requirements.
- Environmental policy.
- Planning implementation and operation.
- Checking and corrective action.
- Management review.

Continued

4.0 Benefits of ISO Standards

Continue...

As one of the most established standards with over 20 years of success, ISO 9001 has helped many organisations to become more sophisticated, better informed and able to manage their expectations for growth.

Benefits of ISO 9001 include:

- Policies and objectives set by 'top management'.
- Understanding customer requirements to improve customer satisfaction.
- Improved internal and external communications.
- Greater understanding of the organisation's processes and clear traceability of products and services.
- Understanding how statutory and regulatory requirements impact on the organisation and your customers.
- Clear responsibilities and authorities agreed for all staff.

Many organisations are implementing an Occupational Health and Safety Management System (OHSMS) as part of their risk management strategy to address changing legislation and protect their workforce.

Benefits of ISO 45001 include:

- Planning for hazard identification, risk assessment and risk control.
- OHSAS management programme to drive operational control.
- Structure and responsibility through performance measuring, monitoring and improvement.
- Training, awareness and competence.
- Consultation and communication.
- Emergency preparedness and response.

Corporate Social Responsibility is recognized as a key differentiator in the Global delivery of products and services. Organisations that voluntary commit and publish their position on Human Rights and Business Ethics, attract strategic Global Partners and clients.

Benefits of Corporate Social Responsibility (CSR) include:

- Assurance of safe working conditions and respectful & dignified treatment of workers/associates.
- Management and removal of unethical conduct in the conditions and practices of delivering services, ensuring good corporate citizenship.
- Safety of workers/associates dignity and respect within the ethical conduct of normal business operations.
- Alignment to international standards/best practices such as; SA 8000, UN Global Compact, EICC and Carbon Disclosure Project (CDP).

5.0 Conclusion

Acuity Group offers a range of products and services that are developed explicitly to fulfil GRC objectives. Each is fine tuned to offer the perfect balance of flexibility and out-of-the-box completeness. Our products are affordable, user-friendly, and permit small and large businesses alike to satisfy internal or external demands for established GRC processes.

Our products combine to provide any size business with all the tools that it requires integrating its compliance to standards and management and mitigation of risk with effective business stewardship. Our consulting services are focussed on adapting and implementing them to satisfy your specific needs, moving you quickly towards your complete GRC solution.

Whether your objectives are financial, information or enterprise centric and your organisation domestic or global, Acuity Group has the products and services to support them.

If you have any questions or require more information about Acuity Group or its products and services, please contact us in the usual way and we will be pleased to respond.

For Acuity Group Ltd

Appendix

Appendix A - Case Study (Previous Experience)

Introduction
Sitel is one of the world's leading suppliers of outsourced customer care and complimentary back-office processes. Sitel employs 57,000 people in 25 countries in order to provide high quality and business critical services to a wide range of customers globally.

Challenge
Sitel's services reach to the very heart of clients' organisations by supporting their customer care, sales, technical support, collections and back office processes. This, paired with Sitel's large, globally distributed workforce, means that corporate governance, the management of risk and compliance with relevant regulations are all key topics for the leadership team. In 2011, a major business opportunity demanded that Sitel enhance its GRC systems and achieve ISO 9001 compliance at a number of sites internationally.

Selection
Sitel selected Acuity Group after evaluating its **off-the-shelf IMS methodology**. Sitel recognised that with a complete, robust and tested IMS methodology, Acuity Group would be able to help it achieve its objectives within challenging time and budget constraints. In addition, Acuity Group demonstrated how its methodology satisfied not just the immediate need for **ISO 9001 certification** but also for other standards such **as ISO 27001, ISO 22301, ISO 14001 and PCI DSS.**

Solution
Acuity Group provided Sitel with an end-to-end programme for the implementation of the IMS and the achievement of ISO certifications. The programme included detailed requirements capture and project planning though to implementation, including follow the sun resource planning to ensure global availability. Acuity Group also worked directly with BSI in order to ensure a perfect fit between their certification policies and Sitel's specific requirements.

Acuity Group implemented its IMS methodology, which in turn allowed it to efficiently prepare 20 Sitel locations for successful achievement of ISO 9001 and 27001 certification. **The IMS system is a scalable solution, automated by GRC software** that enables Sitel to continually and effectively manage governance, risk and compliance within the 20 certified sites.

Future
Following the successful completion of the project within 20 sites, Sitel now has plans to expand the roll out to more of its 120+ sites globally.

Testimonial
About working with Acuity Group, Global Vice President Security & Compliance for Sitel, says "The Acuity Group methodology, automated by GRC software have really demonstrated how the achievement of GRC objectives can be fast and efficient, even within large enterprises. The solution put in place supports from identification of a GRC need, though to audit and certification. The systems are installed at 20 of our sites we are already expanding use to additional sites. There is no doubt in my mind that Acuity Group is the ideal partner for us."

Appendix

Appendix B – Data Protection

EU General Data Protection Regulation (GDPR)

OUR APPROACH TO THE PROTECTION OF PERSONAL DATA

1 Introduction

1.1 The spirit of the General Data Protection Regulation (GDPR) is the protection of personal data of a natural person.

1.2 COMPANY XX will be seen as a Data Controller and Processor by the ICO because of the way it handles client/patient data, received or generated directly and/or indirectly. COMPANY XX also obtain, holds and processes high volume of employee data to fulfil its role as an employer.

2 data mapping exercise

2.1 GDPR requires the mapping of personal data types across the business with a view to identifying the relationship it has with it – either as internal controller or processor. This will provide an in-depth understanding of how and why personal data is accepted into the business and the treatment of that personal data throughout the business once it is received

2.2 As part the data mapping, it will defined the personal data held by a number of personal data "types" – we have currently listed 47 and expect as the industry becomes more mature that we will see more definitions – e.g. DNA is now a new personal data "type"

2.3 Our data mapping will identify the logical and physical containers – i.e. where it resides on a PC, application, phone or in paper / physical format within our business. It will also identify where the data moves within the organisation, and whether or not it is shared with others.

3 protection of personal data

3.1 We are proposing to look at GDPR and the risks that arise in 3 pillars:

(a) protection around the personal data that resides in those containers (security)

(b) the ethical behaviour of how we interact with that personal data, and

(c) understanding the collective rights of the data subject

3.2 With regards the first pillar of risk; the protection and security of the personal data, it is intended that this will be partially addressed by the organisation's alignment to ISO27001 good practice guidance. ISO27001 will establish up to 114 controls that will protect the information that resides in the logical and physical containers. That programme may need to be uplifted where specific GDPR requirements exceed that of 27001 controls.

3.3 The other two pillars are initially being approached by a mapping exercise of the GDPR requirements. This will enable you to identify the articles, defined by recitals, and where fines are specifically associated to recitals. This will help you to prioritise which procedures need to be addressed first.

3.4 Procedures will either be for the collective rights of data subjects or the control of the intrusion by the organisation (e.g. through disclosure or misuse of the information). These procedures will ensure the protection of the data and the mitigation of fines under the GDPR.

3.5 Once all procedures for the pillars of risk are written, you will be able to leverage the ISO27001 framework. The ISO27001 framework will have established an Enterprise Risk Management (ERM) manual for use by management and heads of administrative and support services. It defines the controls they will have to adopt for their functional activities. We call this set of controls the Statement of Applicability (SoA).

3.6 Therefore, with an Compliance Manual deployed and SoA defined for each activity, it will set the foundation for the ability to self-audit for compliance with the GDPR and report your GDPR risk profile through the ERM programme to the risk committee.

3.7 It should be your intention to establish and partially complete this programme of work by May 2018 for GDPR alongside the wider GDPR work which will include the drafting of policies and notices, consideration and implementation of internal procedures.

4 NEXT STEPS

4.1 Once the initial data mapping is complete. The next step is to consider and document the legal basis for processing the data held.

4.2 Form a team of contacts from each relevant business area (e.g. HR, IT, Finance, Business Development) who can be called on to provide views and guidance when they are needed to shape our approach and policies.

5 post 25th May 2018

5.1 GDPR will not stop at May 2018, your work will continue onwards after May 2018. We are likely to highlight a resource gap in the level of resources assigned to the project. It would be right to raise the budgeting challenge for the pre-May resource demand but also post-May, as this may require administrative procedures which are not assigned to mitigation of potential fines (e.g. Erasure, the so-called ‘Right to be Forgotten’ and investment in technology such as data leak prevention) which supports your onwards business as usual work to support our compliance with GDPR.

5.2 Key risks in terms of resource relate especially to your supply chain and regional offices. The work involved in reviewing supplier agreements and ensuring the security of your data once it has been shared, will be extensive. With regards to other offices, the data mapping carried out for the Head Office will in part have covered at a regional level for information stored locally. There are also likely to be local practices and local applications that will need identification and assessment in due course.

[END]