

» Business Process & IT Outsourcing «

A white paper by Peter Watts,
Siemens Insight Consulting



Very few aspects of the modern corporate world are considered more critical than their IT systems. When it comes to the prospect of outsourcing this key resource, whilst the commercial and operational advantages are significant, the potential risks must not be underestimated. Increasingly, focus is coming to bear on the security and compliance sections of the outsourcing contract as being those that need particular attention and specialist knowledge. A company can outsource its IT environment, but responsibility for the risks to its information still remains with the company. Suitable contractual arrangements with third party providers are key to protecting against those risks.

The potential for compromising what may otherwise be a very strong security and compliance position in a company of any size is probably never higher than at the point that the day-to-day operation of the normal operational processes are handed over to external suppliers. Properly ensuring the service providers understand the requirements of the customer and that they are well qualified and equipped to satisfy those requirements will involve close scrutiny of the supplier's processes and technical and environmental facilities prior to the contract being awarded. Some simple examples of areas where expert opinion will be needed during outsourcing negotiations would include:

- Providing confidence that the suppliers understand your security policy and have the resources and knowledge to enforce it
- Ensuring that any disaster recovery provision proposed in a response is at least as good, if not better, than that already in place

Security

Insight Consulting

www.siemens.co.uk/insight

SIEMENS

Business Process & IT Outsourcing

- Ensuring that the management of system access is carried out securely and does not give rise to the possibility of unauthorised access
- Ensuring transparency in the provision of the service through meaningful monthly reports, service level agreements and key performance indicators
- Proposing a governance structure for the post outsource organisation to enable the fast and efficient management of operational and strategic decisions
- Ensuring future changes to security policy to counter changing and emerging threats are implemented by the providers in the most cost-effective manner.

Having the advice of an impartial, but knowledgeable third party in this situation will protect the interests of the company and help ensure business operational processes and business continuity are not compromised.

Once a contract has been awarded, there should be a continual process of review to ensure that the service provider is maintaining high standards of security, compliance and business continuity. Insight Consulting has previous experience of working with clients who were paying for services or levels of service which they were in fact only receiving either in part or not at all and of rectifying those failings.

A similar situation exists when it comes to the prospect of acquisition. Whilst there may be attractions in purchasing another company for the products and/or services it owns, as soon as the company is absorbed, the combined organisation becomes the 'auditable entity' and this may have a negative effect on compliance and the security situation of the resulting group. It may be the case that contradictions in the security policies of the two organisations need to be addressed and legal and regulatory processes need to be harmonised. Alternatively, the security arrangements of

one of the parties may need uplifting to match those of the stronger one.

Insight consulting has experience of working with clients on both sides of the outsourcing counter. Whether it be drafting contract schedules, RFPs or ITT documents or reviewing PQQ or bid submissions, we can bring practical experience of being able to rectify potential weaknesses in the out going requests or equally any potential issues or anomalies in the responses as they are returned.

To continue to maintain a strong audit and legal position during this critical time in the development of your organisation, ensure you obtain skilled and experienced advice from a trusted source - Insight Consulting.

If you would like further information, or to discuss the topics raised within this white paper, please feel free to contact Peter Watts via insight@insight.co.uk or phone 01932 241000.



Author's biography

Peter Watts is a senior consultant with Siemens Insight Consulting, working within the Managed Services team.

He is a Certified Information Systems Security Professional (CISSP), a BCS accredited Chartered IT Professional and a Founding Associate Member of the Institute of IT Professionals

He has previously held the position of Head of Information Security at an EMEA wide level for one of the largest IT services organisations and a multinational retail organisation.

He has worked in a Vendor and Consumer capacity and has managed large scale environments from a security, risk and compliance perspective.

Coming from a predominately technical background Peter has experience of networking to enterprise level, application development in a variety of languages and environments and a range of technical security issues such as malicious code management and investigations.

Insight Consulting is the specialist Security, Compliance, Continuity and Identity Management unit of Siemens Communications and offers a complete, end-to-end portfolio encompassing:

- Security
- Continuity
- Managed Services
- Compliance
- Identity Management
- Training

Siemens Insight Consulting subscribes to the CERG Listed Advisor Scheme (CLAS) and CHECK services. We're also certified against BS 7799 and are a preferred supplier of services to the UK Government and are an accredited Catalyst supplier.

If you'd like to find out more about how we can help you manage risk in your organisation, visit our web site at www.siemens.co.uk/insight
Siemens Insight Consulting
Tel: +44 (0)1932 241000
Fax: +44 (0)1932 236868

www.siemens.co.uk/insight