Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2006

Outsourcing: the Security Risk Management Challenge

Carl Colwill
British Telecom

Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/64

Outsourcing: the Security Risk Management Challenge

Carl Colwill
BT, United Kingdom
carl.colwill@bt.com

Abstract

The globalisation of business and the growth of the digital networked economy means that virtually any business process can be undertaken by someone else, somewhere in the world. To achieve business transformation within the UK Information and Communication Technology (ICT) sector, BT is taking a strategic approach to outsourcing: this has resulted in a rapid and substantial increase in the outsourcing and offshoring of ICT development, maintenance and support contracts. Each and every outsourcing decision could have major security, legal, regulatory and contractual impacts. It is generally recognised that risks are likely to be compounded when outsourcing to companies based in countries that have different political, economic and cultural environments and, subsequently, that security assessments must be augmented to address this. However, difficulties can occur with the ongoing ownership of responsibilities for outsourced information and its processing, particularly when a number of vendors may be involved with the same product or service. Outsourcing security risks are becoming increasingly dynamic and complex, have major business implications and require both tactical and strategic responses. This presents many challenges for corporate security functions and, to be effective, security assessments must feed into business risk assessments and decisions. This paper describes the approaches taken by BT to ensure that security risk assessments are conducted within a consistent framework and integrated into decision-making processes for outsourcing ICT contracts. Specific tools and techniques have been developed to ensure that engagement with stakeholders is effective and timely, that risks and requirements are identified and understood, and that risk mitigation and management strategies are implemented within appropriate compliance and governance frameworks. The method employed by BT is based on the UK Government's Infosec Standard No. 1: Residual Risk Assessment Method (IS1) and has been tailored to suit a commercial environment. To implement the method, many sources of security profiling data have been consolidated from across the business to create a full picture of information confidentiality, integrity and availability risks; this includes legal and regulatory issues and BT's responsibilities as a fundamental component of the UK Critical National Infrastructure. This has enabled new approaches to categorising systems and applications in terms of data value and impact. To cater for the 'industrial scale' volume of outsourcing requests, automation has been introduced to enable consistent and speedy assessments and to improve the means of communicating the results to stakeholders. The paper also highlights the importance of a taking a hierarchical approach to conducting risk assessments and setting security requirements – within the context of system and contract lifecycles - and the need for effective protective monitoring and audit regimes.

Key Words

Security risk management, security risk assessments, outsourcing, offshoring, Residual Risk Assessment Method (IS1), confidentiality, integrity, availability, security requirements, Critical National Infrastructure, information assurance, compliance, governance, audit.

INTRODUCTION

Outsourcing, offshoring and globalisation are no longer management consulting "buzzwords" but business realities that present many challenges for the security community. Every outsourcing decision can have significant security, legal, regulatory and contractual implications. Risk profiles will change when outsourcing to companies based in countries that have different political, economic and cultural environments. Further challenges are presented by a dramatic increase in the number of business processes earmarked for outsourcing: each of these requires security analysis and many disparate sources of information must be identified and

consolidated to create appropriate inputs to facilitate effective analysis. BT is one of the world's leading providers of communications solutions serving customers in Europe, the Americas and Asia Pacific. Its principal activities include networked IT services, local, national and international telecommunications services, and higher-value broadband and internet products and services. Security risks have become increasingly dynamic and complex and can have major impacts on operational and business decisions, from both a tactical and strategic perspective. BT has therefore reviewed and evolved its approaches to security risk management to ensure that outsourcing assessments are built into the dynamic Information and Communication Technology (ICT) environment and integrated into decision-making processes for outsourcing work. New tools and techniques have been developed to ensure that engagement with stakeholders is effective and timely, that risks and requirements are identified and understood, and that risk mitigation and management strategies are implemented within appropriate compliance and governance frameworks. The new methods are based on the UK Government's Infosec Standard No. 1: Residual Risk Assessment Method (IS1) (GCHQ/CESG, n.d.) .

THE CHANGING FACE OF OUTSOURCING

Globalisation has had a pervasive impact and changed, irreversibly, the way we do business and manage IT infrastructures (Morgan & Bravard, 2006). The growth of the digital networked economy has resulted in high-speed, high capacity and relatively low cost communications, coupled with commoditised processing power. This has opened up new opportunities for *sourcing* work and made geographic location virtually irrelevant for many activities and services. In this dynamic new world, businesses must transform or stagnate and global sourcing is a major weapon to achieve transformation. The British Computer Society (BCS) believes that global sourcing will become a competitive differentiator for businesses (Kobayashi-Hillary, 2006). Effective sourcing requires looking constantly across existing and potential vendors and locations and seeking the right balance between quality, economics, risk, flexibility and innovation.

Offshoring is a specific variant of outsourcing and different business decisions and strategies may be required. Outsourcing involves the contracting out of activities to a third party supplier, which could be onshore in the same country as the customer organisation. Offshoring refers to transferring activities to a third party located in another country, including providing access to onshore data from foreign locations. Traditional drivers for outsourcing, particularly offshoring, are:

- reduce costs;
- staff and skill shortages;
- transfer risks;
- develop strategic partnerships;
- exploit time differences.

In terms of relative importance, cost reduction still a primary factor but the strategic reshaping of business is now far more important. Some believe that we have reached the end of the cost reduction phase and businesses are looking for more sophisticated approaches and innovation to drive more value and revenue from IT (Knights, 2006). Gartner predicts that global offshoring spending on IT services will rise to a total of £28.6bn by 2007 (Underwood, 2006). It is further reported that 81% of UK companies plan to increase offshore outsourcing over the next three years (DTI, 2005). India is currently the preferred choice for offshoring, accounting for 75% of all work, followed by Eastern Europe 28% and China 25% (DTI, 2005). India's current position is underlined by:

- cost base;
- numbers of qualified and skilled people;
- infrastructures (including Government sponsored 'Cyber City' initiatives);
- business language (English);
- track record in Business Process Outsourcing (BPO).

- industry/sector collaboration, for example, the National Association of Software and Service Companies (NASSCOM) (NASSCOM, 2005).

BT'S EXPERIENCE OF OUTSOURCING AND OFFSHORING

BT has redefined outsourcing and offshoring from being a tactical methodology for reducing operational costs, into a strategic tool for business transformation. The business is adopting flexible boundaries and agile working and has taken a decision to offshore the majority of its outsourced work. This strategy has been enshrined in the 2004 "90:10 Rule": that is, at least 90% of all outsourced work must be delivered from offshore; some activities will remain outsourced, but onshore, within the UK. This has resulted in a rapid and substantial increase in the offshoring of the following ICT activities, principally to India:

- data conversion and migration;
- IT development;
- IT maintenance and operational support;
- IT professional services;
- contact centres and help desks (both internal and customer facing).

BT has substantial experience of working with Indian suppliers and partners. A specific Indian joint venture was created in 1987, *Tech Mahindra* (previously *Mahindra BT*), and BT has five strategic partners and many more tactical suppliers on the subcontinent. A common contractual framework has been in place for strategic partners since 2003 and this includes a comprehensive set of baseline security requirements that can be enhanced, depending on the nature of the information assets concerned.

OUTSOURCING SECURITY ISSUES, RISKS AND CHALLENGES

The message that security must be a key part of outsourcing is not new (Thomas, 2004). Equally, the need to set specific criteria for selecting suppliers as part of managing outsourcing security risks has been documented (Leigh, 2004). However, taking into account the short time frames often associated with sourcing decisions, security risk assessments may not always be conducted at an appropriate time and with the necessary granularity. In some cases, changes to risk may not be considered at all, for example, where a very basic "lift and shift" attitude is applied towards outsourcing business activities. Even when security requirements have been agreed, difficulties can still occur with the ongoing ownership of responsibilities and security controls, particularly when a number of vendors may be involved with the delivery of the same product or service.

In simple terms, risk can be defined as a function of the following variables: *vulnerability* (impact) and *threat* (likelihood of exploitation – driven by the variables of *motivation*, *opportunity* and *capability* when assessing malicious attacks). Outsourcing decisions can affect each or all of these variables and should necessitate risk assessments and security reviews. Many data inputs, however, need to be factored into the risk equation and triggers need to be established to conduct timely risk assessments. Granularity in the level of assessment is also important because a "one-size fits all" approach is unlikely to be appropriate and risks, together with cost effective risk mitigation opportunities, may be missed.

Customers and stakeholders have become more concerned about privacy and information confidentiality as a result of an increase in the abuse of personal data through fraud and identity theft. Stakeholders are increasingly aware of their reliance on electronic information and the risks, perceived or otherwise, posed by not just malicious acts but also accidental exposure. Customer requirements are becoming more specific and some may include (sometimes not obviously) a "no offshoring" clause. Many security breaches have been reported from India - mainly from financial services companies - with many £100k allegedly being stolen (Ahmed, 2006; BBC 2006a,b,c,d; Biswas, 2006). It has also been reported that lack of trust in local staff has been the reason for at least one large financial services company closing its Indian call centre (BBC, 2006e) . At the heart of many of these reports is an apparent weakness in recruitment background checks, facilitating the falsification of personal

history and records to gain a job and access to customer information. This is exacerbated within the Indian labour market by the high level of churn of employees between companies. To address this, NASSCOM is working with the Indian Government to train police to tackle IT-related crime, plus set up a national registry of personnel histories (Thibodeau, 2005) . It should be noted, however, that that this type of abuse is not unique to India or the offshoring sector. The author's own experience of auditing Indian companies has confirmed that suitable levels of security can be implemented and maintained (indeed, levels of protection and security awareness - driven by corporate policies - can sometimes be higher than those found in Western European counterparts).

Other changes to threat levels must be considered. BT's prominent position within the UK ICT sector marks it as a target for threat agents seeking to compromise the confidentiality, integrity or availability of its information or its operational capability. A further concern lies with the global extension of corporate (and country) IT infrastructures outside of traditional domains of protection. The selection of a small number of suppliers for business-critical processes can also result in data aggregation that may not have occurred within the company's own IT infrastructure. These changes provide new opportunities for threat agents to identify information assets and vulnerabilities in geographic areas that may be more susceptible to targeting attacks: lines of defences are stretched and new 'hot spots' are created. BT is a fundamental component of the UK Critical National Infrastructure (CNI), a position that brings with it specific security responsibilities and the need to consider a wide range of stakeholders. High-capability threat agents seeking to attack information or other assets belonging to CNI companies may find that they are able to operate more easily in some overseas countries where levels of protection are less stringent. "Insider" threats to information assets are well recognised. However, the use of outsourcing and offshoring services can blur the distinction between a company's employees and third party personnel and great care must be taken to ensure that physical and logical access controls remain effective in a changing and flexible environment. The creation of appropriate levels of 'trust' brings with it a complexity in implementation and a significant cost – *see Figure 1*.

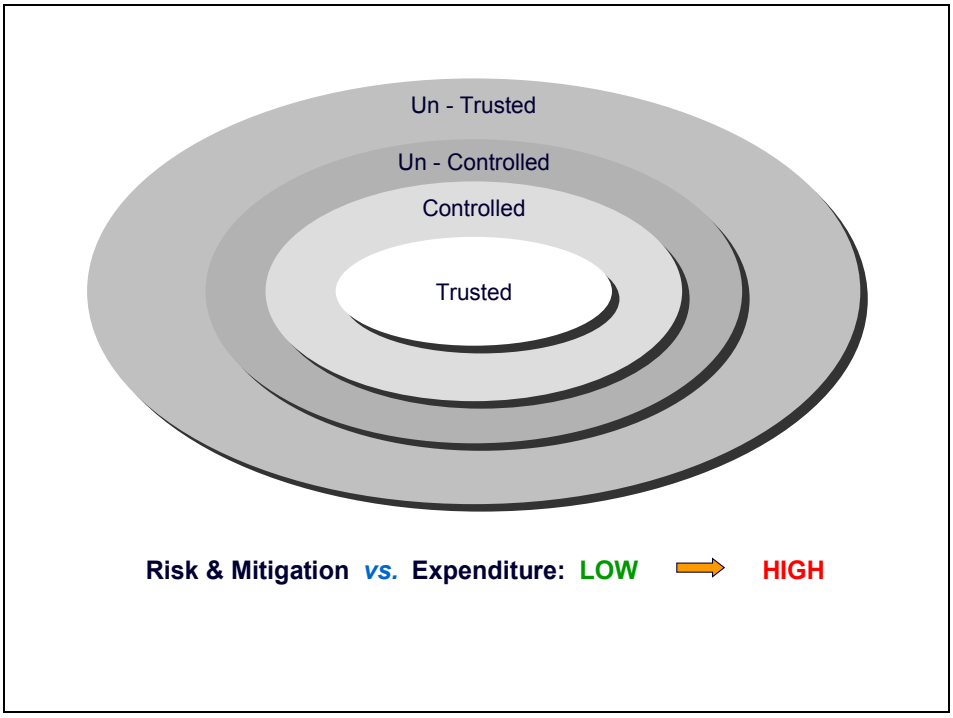


Figure 1: Levels of trust - balancing risk & cost

Legal and regulatory issues are rising up the agenda. The UK Information Commissioner's Office (ICO) has found it necessary to reiterate that outsourcing data processing to foreign suppliers does not absolve companies from protecting the data once it passes to a third party. New guidance issued by the ICO will tighten up rules concerning a company's responsibilities to find an outsourcer who will safeguard the data (Out-law.com, 2006)

. Companies cannot simply put the blame on vendors: those who outsource are still accountable and liable in eyes of customers and regulators. It must also be remembered that the local laws of the country involved will take precedence over contractual requirements.

In all cases, it is advisable to decompose information security requirements into the specific attributes of 'confidentiality', 'integrity' and 'availability' ('CIA') and to consider these from a system lifecycle perspective. *Table 1* presents an example of different levels of information risk over a typical system lifecycle (this will vary depending on the nature of the system and data).

Table 1: Changing information risks

Lifecycle Stage / Info Attribute	Design	Development	Test	Operate
Confidentiality	Low	Medium	Medium	High
Integrity	Medium	Medium	Medium	High
Availability	Low	Low	Medium	High

Such decomposition will create the granularity needed to identify specific levels of security for different lifecycle stages, for example, application development using 'dummy' or 'anonymised' data may require less rigorous security measures than operational stages using 'live' customer data.

It is also important to address security throughout the contract lifecycle as well, from initiation through to contract termination, and this can add a further dimension to *Table 1*. The UK National Infrastructure Security Co-ordination Centre (NISCC) has issued guidelines to help build security into contracts, breaking the lifecycle into 14 distinct stages (NISCC, 2006) . Specific contractual information should be gathered for security risk assessments, namely to determine the type of access profiles that third party personnel will have to corporate and customer information, for example, powerful 'root' access for support functions versus 'standard' user access for help desk activity.

Granularity in assessments facilitates the identification of cost-effective security solutions. However, an appropriate level of granularity must be identified and weighed against the cost and usefulness to business-oriented stakeholders and the decisions they must take – see *Figure 2*.

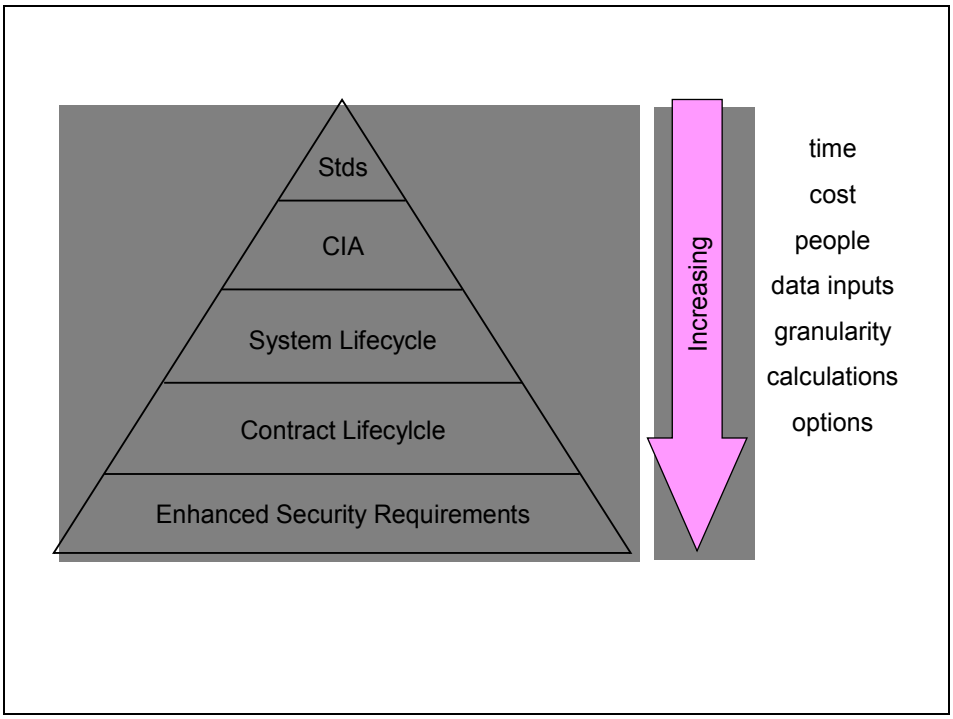


Figure 2: Increasing complexity & cost

Within the UK ICT sector, many factors must therefore be assessed to identify security risks and the resultant requirements or mitigation options, including:

- international Standards, for example, IS027001, BS7799, BS7858;
- corporate security policy;
- regulatory and legal requirements, for example, UK Data Protection Act, US Sarbanes Oxley, UK Telecoms Strategic Review;
- customer security requirements – individual, company and UK Government, including imported privacy markings;
- CNI requirements;
- offshore country-specific factors, for example, political, economic, social, technological and legal environmental conditions;
- vendor environment;
- system lifecycle stages;
- contract lifecycle stages;
- baseline contractual security requirements;
- enhanced contractual security requirements.

The timely capture of these requirements in a form readily useable for input to risk models can, however, prove difficult. Many sources of requirements and system security information from across the business must be identified and consolidated to create the 'big picture' of information security attributes for any given system or application. From BT's perspective, the volume of target systems and applications for offshoring that require security assessments also presents another challenge for the mix. Speed of sourcing can be a business differentiator and agile security responses are required. It must also be remembered that one-off security assessments are insufficient and planned lifecycle and contract changes over time provide an effective trigger for risk management reassessments. These factors drive toward the increased use of automation to speed up assessments.

To summarise, the business will change, as will the suppliers and the competitive, technological and geographic environment in which you operate. Outsourcing security risks have therefore become increasingly dynamic and complex, have major business implications and require both tactical and strategic responses. To be effective, the corporate security function must be able to feed into business risk assessments and decisions. Security requirements could lead to additional costs which provides a further driver for speedy assessment and early inclusion in business cases – an investment to secure operations and future revenue, not an additional 'security tax' which has to be bolted on afterwards.

IDENTIFYING SECURITY RISK MANAGEMENT SOLUTIONS

BT has a long established and comprehensive security infrastructure with security risk management assessments for commercial applications built into system, network and product lifecycles:

- ISO27001/BS7799;
- BT Corporate Security Policy;
- BT Security Evaluation and Certification Scheme (BTSECS);
- Information Assurance Programme.

Existing methods had been applied to assessing outsourcing security risks on a relatively small scale. However, in 2004, driven by new offshoring drivers and business demands, BT reviewed its security risk management portfolio. A key driver was the new strategic BT-HP Alliance and the transfer of the management of BT's mid-range servers and end-user workstations to HP *(Todd et al, 2006)* . At the point at which the security communities from BT and HP became fully engaged, no agreed method existed for the assessment and mitigation of security risk. A suitable, best practice, method was needed to identify and manage security risks, principally from changes to environmental and personnel factors. Given the nature of its business and the range of commercial and CNI security requirements implicit and explicit in its services, BT's Information Assurance Programme proposed an industry and UK Government recognised methodology for the assessment, articulation and mitigation of risk: the *UK Government's InfoSec Standard No. 1 (IS1)* (GCHQ/CESG, n.d.) . A trial was commissioned and demonstrated the effectiveness of *IS1* to key stakeholders. Although *IS1* is designed for assessing government accredited systems it was shown that the method could be used effectively in a commercial environment. Application of the method provides the following benefits:

- use of a verified, independent model approved by UK Government and recognised world-wide as an effective standard, that is, not based on, or biased towards, BT or vendor methods;
- a rigorous framework for conducting risk analyses enabling repeatable evaluations;
- a means of identifying the various factors that comprise ICT risks and options for reducing risk scores;
- a means of comparing relative risk scores;
- a means of recalculating risk scores based on the application of protective measures, that is, the ability to perform 'before' and 'after' risk management analyses.

IS1 is sufficiently flexible to cover most levels of security risk likely to be encountered within strategic partnerships. The method allows the categorisation and quantification of the risk to a specific target in the context of the following factors:

- Impact;
- Environment;
- Population;
- Technical Factors;
- Opportunity;
- Protective Measures;
- Volume of Data;
- Assurance Barriers.

Given that the purpose of the many outsourcing risk assessments is to determine the change in risk attendant upon the changes in the delivery environment the key factors in the above list are Environment and Population. The Environment category encompasses both the corporate and the regional environments and thus enables a clear distinction to be made between outsourced delivery arrangements and off shored delivery arrangements. Population is defined as the people employed within specific functions of the outsourced activity. Risks within this category can therefore be managed through the strict definition of user profiles, the close management of the numbers of people allowed access to the target system and through the rigorous application of employment background checks.

IS1 also provides a standard method for identifying acceptable levels of risk. This is based on the scoring criteria and guidelines for each of the factors that comprise residual risk. Scores below the threshold are deemed acceptable (but could be indicative of having too many levels of protection) and scores above the threshold are indicative of systems with unacceptable levels of risk for which further levels of protection are required. IS1,

therefore, provides a means of identifying additional protective measures and leads directly to the formulation of recommendations to reduce or manage levels of risk.

IMPLEMENTING NEW APPROACHES

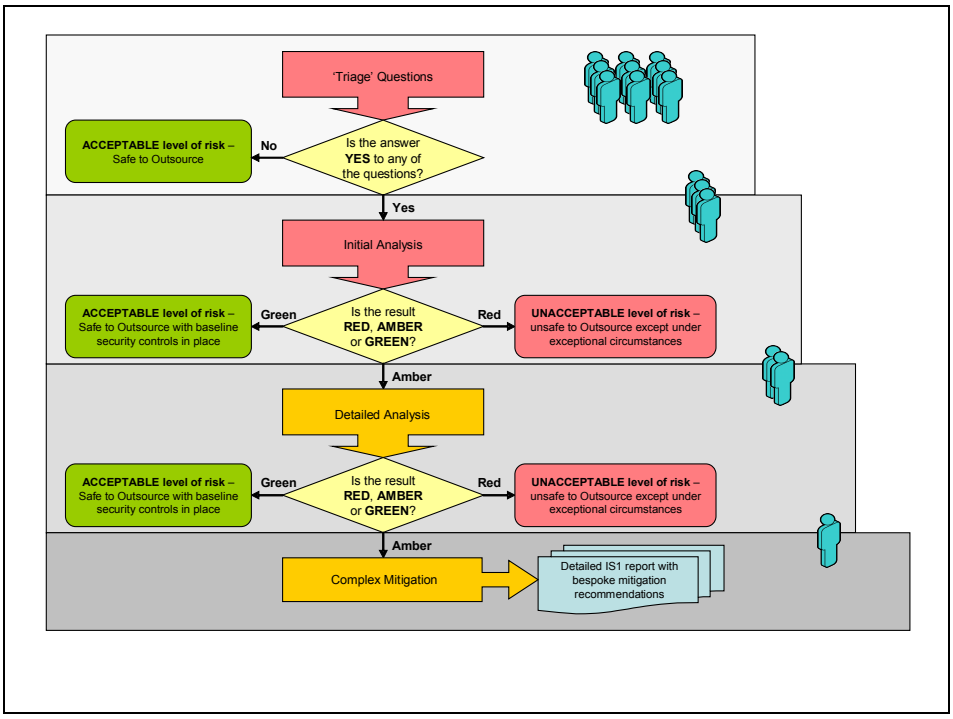
Following its successful application for BT-HP Alliance purposes, BT senior management endorsed the use of an IS1-based method for all outsourcing risk assessments. *IS1* and its standard risk factors would remain at the core but a flexible 'front-end' was needed to capture a large number of inputs and assumptions to drive effective assessments. Automation was necessary to deal with the 'industrial scale' volume of outsourcing requests received by security teams, and to enable consistent and speedy assessments.

Stakeholder engagement and a means of feeding back results to a variety of interested parties were necessary. A 'Red-Amber-Green' (RAG) approach was adopted to facilitate ease of communication and understanding: this notation is widely used in the project management community. Thresholds and descriptions based on *IS1* risk scores were then mapped onto each RAG status – see *Table 2*.

Table 2: Red-Amber-Green status

RAG Status	Description
GREEN	SAFE to offshore providing baseline security controls are in place and maintained.
AMBER	Additional mitigation factors/options may be possible to reduce the RAG to GREEN; more detailed *IS1* analysis required.
RED	UNSAFE to offshore. Additional mitigation is unlikely to be sufficient to reduce residual risk to an acceptable level.

A 'top-down' approach was implemented and the IS1 front-end spreadsheet quickly evolved into a tool for capturing and collating the wide range of data inputs needed to perform IS1 outsourcing assessments with increasing levels of granularity *(Colwill & Gray, 2006)* . Initial inputs are taken from the ICT programmes during a 'triage' stage analysis and these are augmented with input from security professionals in the next stages of analysis. Information from a variety of business impact analysis and security profiling processes are consolidated, together with legal and regulatory requirements, to create a common understanding of Impact Levels (consistent with IS1 definitions) based on data value, sensitivity and potential impacts inside and outside BT. At the same time, inputs relating to other IS1 factors such as vendor environment and potential attacker populations are gathered or estimated. The top-down approach provides early indications on "go/no go" situations and areas where further investigations are required – see Figure 3.



Fiure. 3: Top-down approach

The process and tool provide a means of communicating a summary of risk factors and results to stakeholders. A series of RAG assessments are made based on the data *impact level* and the *type of work* and scale of third party access to the data – *see Figure 4.*

Type of Work	Impact Level 1	Impact Level 2	Impact Level 3	Impact Level 4
Onshore	GREEN	GREEN	GREEN	AMBER
Offshore (Normal Risk)	GREEN	AMBER	AMBER	RED
Offshore (High Risk)	GREEN	AMBER	RED	RED

Figure 4: RAG assessments for varying impact levels

These results provide an *initial* assessment from which to identify priorities and judge whether more detailed analysis involving a greater number of factors is required. The top-down approach provides a key security input to stakeholders at different stages of system and contract lifecycles to develop a picture and understanding of security risks and mitigation options and to help assess potential costs.

Profiling systems and applications by impact level attributes has enabled better categorisation of systems: this, in turn, means that one assessment (covering a large number of systems that fall within a given category) can be conducted to identify common risks and security solutions. At first, significant effort was required to collect the inputs for risk assessments and gaps or potentially contradictory values were identified. However, consistency has been implemented, quality improved and all inputs are now loaded into a secure support database to facilitate speedy assessments and to provide a single source for use by the security community. Extracts into this supporting database from key business databases are also now automated.

The limitations of the front-end tool should be recognised as it is designed as a decision aid for preliminary assessments rather than replacing a 'full' *IS1* analysis. However, it does mean that opportunities for potential outsourcing savings can be identified early in the project lifecycle. The use of assumptions to drive certain factors, such as vendor environmental conditions, has proved necessary but all assumptions can be challenged and changed on a case-by-case basis where additional input is either available or desirable. A series of on-site vendor audits in India was conducted to verify key *IS1* environmental assumptions and provide assurances on the levels of compliance to BT's security requirements, including recruitment background checks. Where there is any doubt, or results require sensitivity analysis, a full *IS1* assessment will be recommended, even for 'Green' results.

IS1 results can, where necessary, be complemented by other tools and methods to construct more detailed risk profiles based on specific vulnerability, threat and exploitation factors, for example via BT's Information Assurance Risk Model – *see Figure 5*.

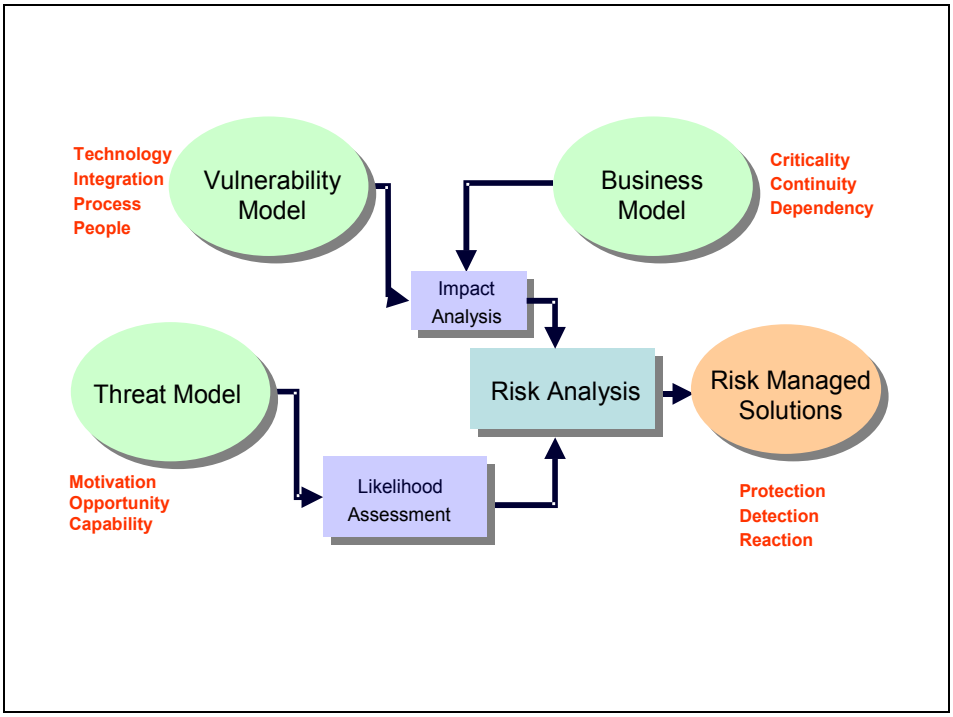


Figure 5: Information Assurance Risk Model - specific assessments

This can include specific regional threat assessments and will normally require input from the experts and external agencies (for example, NISCC in the UK) for certain factors such as threat agent 'motivation' and 'capability' – *see Figure 6*. Analysis can then concentrate on 'opportunity' factors and attack scenarios to assess a range of potential attackers attempting to exploit a set of known vulnerabilities.

BENEFITS REALISED

Many benefits have been realised from the implementation of new security risk management approaches. These benefits have been recognised by a wide range of stakeholders: customers, security teams, internal audit and compliance teams, ICT programme directors, vendor management teams and vendors themselves. Business processes have been improved to create better, timely, linkage between security and ICT programmes. There has been a significant increase in security awareness and the potential impacts of security failures, including the liabilities that *individuals* may face. Security is only one input to commercial decisions, though it is now recognised that it is an essential input that can influence risk appetites.

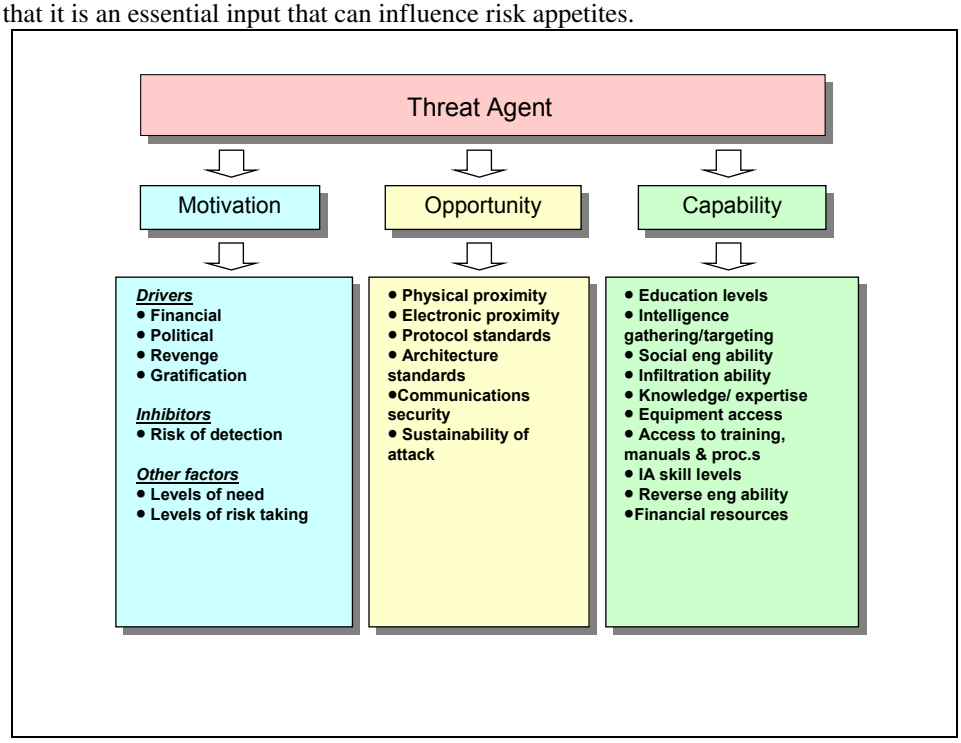


Figure 6: Information Assurance Threat Agent Profiling

The wide-scale review of data sources and security attributes for input to *IS1* has led to new means of capturing and consolidating security-related data, improving its quality and making it available for the security community. This has stimulated new approaches to categorising systems by their security attributes and to the understanding of data in terms of its value and impact to BT and stakeholders.

A firm linkage has been established between security risk management and business risk, compliance and governance frameworks to help develop the 'big-picture' view of corporate risk and assess potential aggregation effects across contracts – *see Figure 7*.

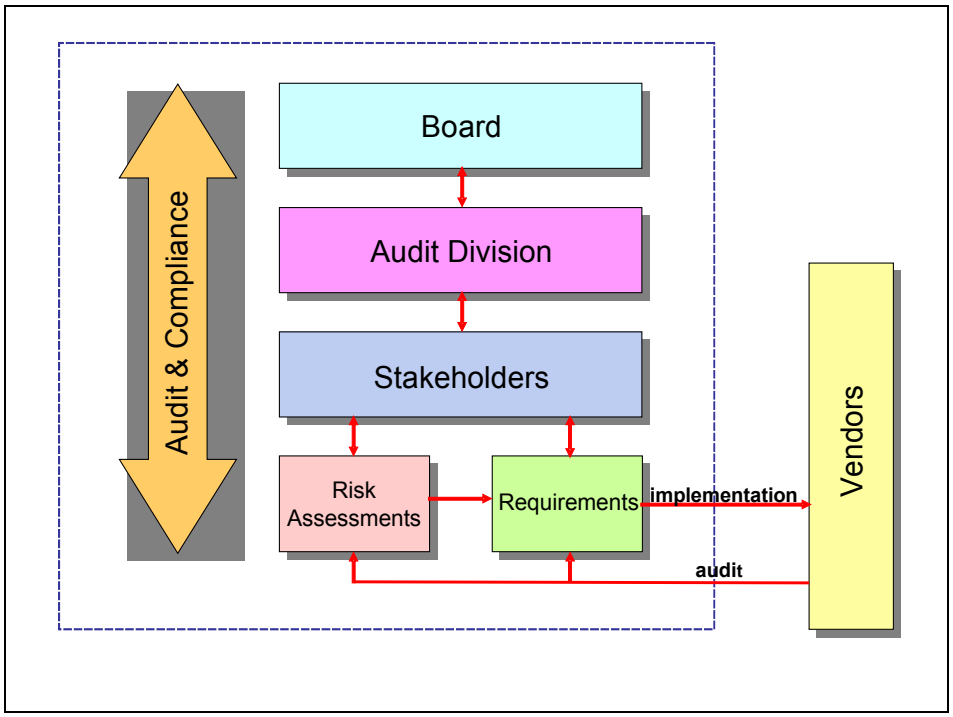


Fig. 7: Governance Model

The new processes have been rolled out with senior management endorsement, supported by education and awareness programmes. The approach, method and governance model facilitates reassessments when circumstances change and can drive the follow up of recommendations, implementation of mitigation measures and compliance audits – within BT and the vendor community. Effective risk management is an iterative process and the business cannot rely on one-off risk assessments.

The output from the risk assessments has enabled the identification of common risk mitigation options, risk management strategies and areas where security requirements can be enhanced. This has shifted security responses from one-off 'tactical' measures to a more 'strategic' perspective - *see Figure 8* - and has led to the raising of baseline standards within the strategic framework contracts.

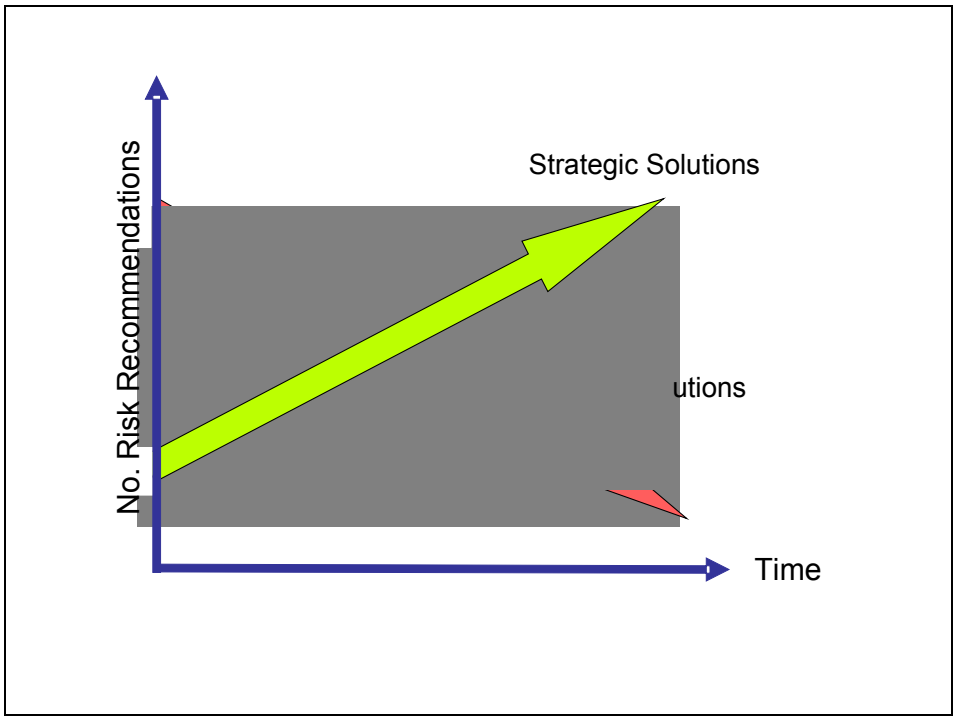


Figure 8: Evolving strategic solutions

The core set of security controls (people, physical, logical) now have an emphasis on protective monitoring and audit. Ongoing compliance is policed through the presence of a BT security relationship manager based in India. Audits of vendor sites have been used as opportunities to demonstrate commitment to security, raise security understanding and develop secure partnerships – for the benefit of all parties. This, in turn, will have a positive impact on sector and country levels of security, for example promoting the adoption of international standards such as ISO27001.

CONCLUSIONS

BT's security community has successfully reviewed its approach to security risk management to introduce a new risk model and supporting processes. These have been effectively integrated with system and contract lifecycles, decision-making processes and compliance and governance frameworks and have publicised senior management endorsement. An emphasis on identifying and *managing* key outsourcing security risks has been accepted and established.

Outsourcing business drivers have stimulated innovation and automation for collecting input for risk assessments, performing the calculations and disseminating the results. The involvement of stakeholders at every stage was a crucial success factor to gain commitment and to improve the quality of input and ownership of results. Stakeholder involvement should be the norm but the additional people identified (further down the 'chain' than usual) helped highlight and resolve a number of issues during early assessments, for example, details of end customers, particularly "no offshoring" clauses.

The ability to identify the key risk factors applicable to outsourcing, namely, specific environmental conditions, the number of third party personnel involved in the contract and the level of 'trust' given to these personnel, provide factors that will drive mitigation strategies. From a plethora of potential security requirements, focus can be taken on key security controls and responsibilities and the means of maintaining these over time and across contracts. It also now relatively straightforward to identify situations, for example, based on the consolidated impact value of the data, where it is known that no current cost-effective outsourcing or offshoring solutions exist.

The importance of protective monitoring and audit regimes has been highlighted for BT and its outsourcing partners - from both a compliance and assurance perspective and to create effective engagement to raise security thresholds and discuss security issues. Further work is planned to integrate compliance and audit processes to provide effective and quicker means of providing evidence and assurances.

Many lessons have been identified:

- assess security risks and specify requirements <u>before</u> implementation (!) - "lift and shift" is an ideal an seldom a secure reality;
- apply focus - identify and manage the key risks over time;
- ensure that security requirements, including roles and responsibilities, are a key feature of contracts;
- specify rigorous recruitment background checks;
- you may be "giving away" data confidentiality so prepare for this;
- 'CIA' failures will happen at some stage - contingency plans are vital (including public relations and customer management responses);
- know your processes - identify boundaries and interfaces, roles and responsibilities, and key control points;
- determine criticality and business impact - *don't expect the supplier to do this for you!;*

- identify and maintain control of authorisation processes, checks and balances and, where necessary, security, compliance and governance functions;
- don't give away functionality and ask for it back later;
- lifecycle approaches must be taken because requirements will change over time;
- define security 'exit strategies' because contracts will terminate (possibly with very short notice);
- audit - and then audit again;
- use an on-site, or in-country, security manager to police compliance – where feasible;
- use global standards (for example ISO27001) and don't try to "re-invent the wheel";
- check thoroughly for sub-contractors;
- engage stakeholders from the earliest stages of security assessments;
- communicate security risks to senior management from the outset - there may be costs and delays;
- identify liabilities – your company (and possibly *you*, as an individual) will still be in the firing line;
- communicate benefits and penalties to suppliers - future revenue and reputation is at stake;
- actively build partnerships and relationship with key suppliers - it is in the interests of both parties and the sector as a whole (this should include security awareness);
- encourage, and work with, regional security initiatives.

More challenges for security teams are appearing on the horizon. The topic of security will continue to rise in significance for stakeholders as their appreciation of the value of their information and the need to access it where and when they need it increases. Globalisation and outsourcing, coupled with the requirement for more open networks and interconnection, will continue to increase and result in corporate infrastructure fragmentation and the breaking down of traditional boundaries and security controls. We will be faced with a new wave of 'insiders': how will we distinguish third party personnel from our own employees and implement appropriate trust models? In line with this, security models must evolve: 'de-perimeterisation' *(Bleech, 2006)* will shift the focus from the infrastructure to the client, application and eventually the data level. The security community must prepare business-oriented solutions to these challenges and raise its profile to Board-level processes and thinking.

REFERENCES

Ahmed, Z. (2006) Outsourcing exposes firms to fraud, URL http://news.bbc.co.uk/1/hi/business/4094894.stm

BBC (2006a) Man held in HSBC India scam probe URL, http://news.bbc.co.uk/1/hi/business/5122886.stm

BBC (2006b) Are overseas call centres a fraud risk?, URL http://news.bbc.co.uk/1/hi/uk/4122772.stm

BBC (2006c) India call centre 'fraud' probe, URL http://news.bbc.co.uk/1/hi/uk/4121934.stm

BBC (2006d) Fear over India call centre fraud, URL http://news.bbc.co.uk/1/hi/business/3593885.stm

BBC (2006e) Credit card chaos in India, URL http://news.bbc.co.uk/1/hi/business/3569743.stm

Biswas, S. (2006) How secure are India's call centres? URL, http://news.bbc.co.uk/1/hi/world/south_asia/4619859.stm

Bleech, N. (2005) What is Jericho Forum? URL, http://www.opengroup.org/projects/jericho/uploads/40/6809/vision_wp.pdf

Colwill, C. & Gray, A. (2006). Creating an Effective Security Risk Model for Outsourcing Decisions, BT Technology Journal 25(1)

DTI (2005). Technology Partnership Initiative News Issue 47, 10/05

GCHQ/CESG (ND) UK Government's Infosec Standard No. 1: Residual Risk Assessment Method (IS1)

Knights, M. (2006). Computer Weekly: "A More Sophisticated Approach", 11/7/06

Kobayashi-Hillary, M. (2006). Computing: " Offshoring is Changing the focus of IT", 5/6/06

Leigh, J. (2004). Security News: "Managing outsourcing security risks", 18/11/04

Morgan, R. & Bravard, JL. (2006) Computer Weekly: "How globalisation alters your world", 8/8/06

NASSCOM (2006). NASSCOM, URL http://www.nasscom.in/Default.aspx?

NISCC (2006). Good Practice Guide. Outsourcing: Security Governance Framework for IT Managed service Provision, 8/06

Out-law.com (2006) The Register: "Outsourced data must be protected, says privacy chief", 12/7/06.

Thibodeau, P. (2005). Computerworld: "Firms in India seek better background-check system", 18/4/05

Thomas, D. (2004) Computing: Security must be key part to outsourcing, 18/11/04

Todd et al (2006). Security Risk Management in the BT-HP Alliance, BT Technology Journal 24(4)

Underwood, G. (2006). Computer Weekly: "How the four Ps pay off", 28/2/06

COPYRIGHT

British Telecommunications PLC ©2006. The author/s assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors