



ExecIA LLP

Excellence in Information Assurance

# Information Risk Management Maturity

*Providing the bigger picture  
so you can deal with the  
details more effectively*

## Results of the 2010 Survey

## Introduction

This report has been produced as a result of a survey conducted jointly between CA, Comsec and ExeclA; using the ExeclA Controls Assessment (ECA) tool.

The survey asked respondents to select their current and target capability maturity in 31 areas of information assurance risk control. The control areas were selected from international standards and best practices such as ISO27001, COBIT and ITIL. The capability maturity levels are designated as follows:

0. Processes not present or required.
1. Ad-hoc, undocumented processes used.
2. Documented processes in place, but not always fully communicated.
3. Processes fully documented, communicated and deployed appropriately.
4. Fully documented processes, with regular training, enforcement and monitoring.
5. Processes documented and automated; with full training, enforcement, monitoring and audit.

About 20 UK respondents took part in the survey. These were all from large or very large organisations in a range of sectors; including banking and finance, retail, transport, IT services and government. The analysis below summarises the most interesting findings from the survey.

## Strategic, Operational and Tactical Controls

The control areas within the survey were divided into three groups: strategic, operational and tactical. **Strategic controls** enable an organisation to align its information assurance to business and governance requirements. **Operational controls** deliver effectiveness and efficiency. **Tactical controls** are the fundamental building blocks of information assurance, often technical in nature. Figure 1 shows the average current and target capability maturity scores on three axes that correspond to the three groups of control areas.

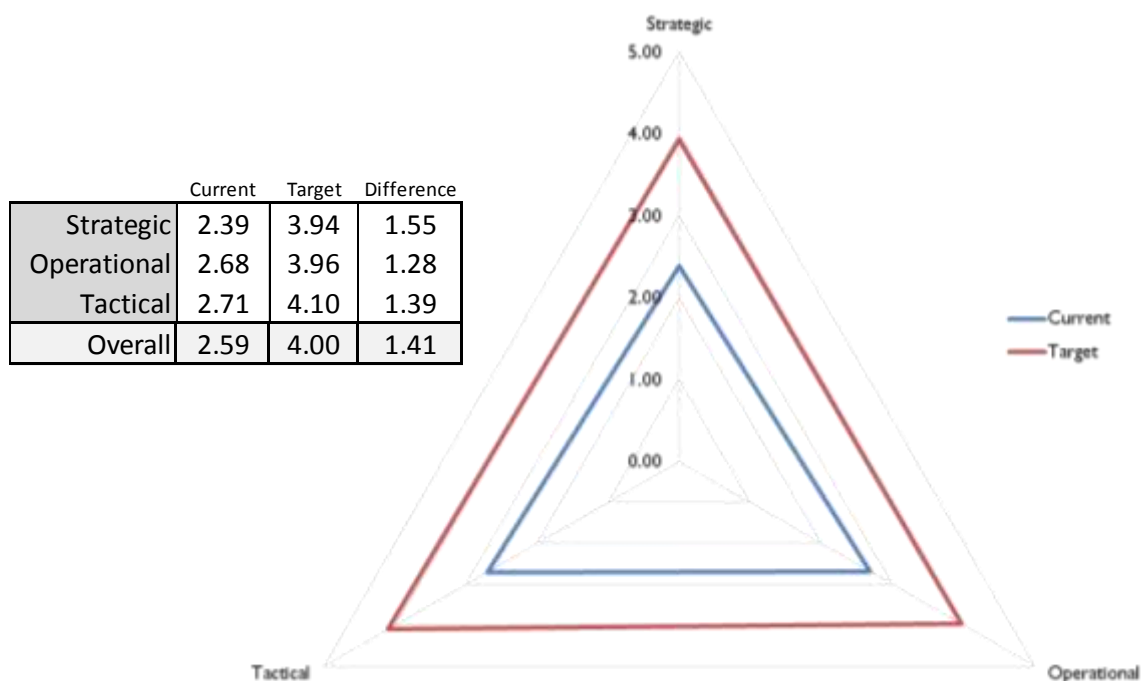
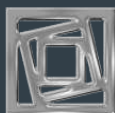


Figure 1: Overall Results for Strategic, Operational and Tactical Current and Target Capability Maturity

On average, it is clear that organisations show most capability maturity in the tactical control group, less in the operational and least in the strategic. This finding supports the common observation that most organisations have initiated their information assurance development by implementing the more simple technical controls; but are still relatively immature in their management of more complex strategic issues.

In terms of targets, the difference between tactical and strategic is only half that of the current difference (0.16 as opposed to 0.32). The implication is that organisations are seeking to bring the three control areas into better balance.



## Maturity and Targets for Control Groups

Not only did organisations assess strategic controls to be, on average, less effective than operational and tactical; figure 2 shows that 83% of respondents assessed strategic as their least mature control group as a whole. This emphasises the potential problems that organisations are likely to face; given the need (all other things being equal) to put strategic controls in place before operational and tactical.

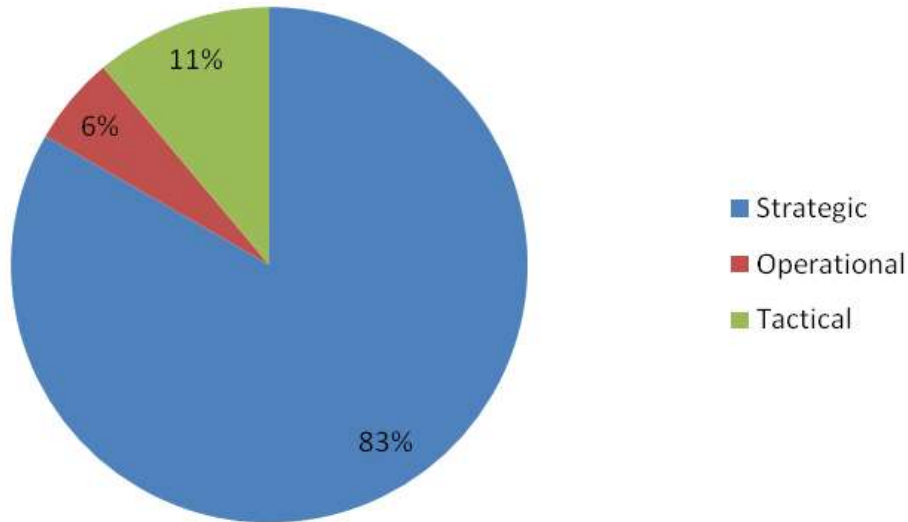


Figure 2: Percentage of Respondents with Strategic, Operational and Technical as Least Mature Control Group

In terms of their targets for maturity, figure 3 indicates that organisations are completely balanced between the three control groups. On the face of it, this appears to be admirable. However, it could also indicate potential future problems; given that the gap between current and target capability maturity in the strategic group of controls is greater than that in the other two groups. Unless additional resources are given to meeting the strategic control targets, above those for the other two groups, achievement is likely to fall short. It may therefore be that organisations should consider selecting more realistic targets for their strategic control group.

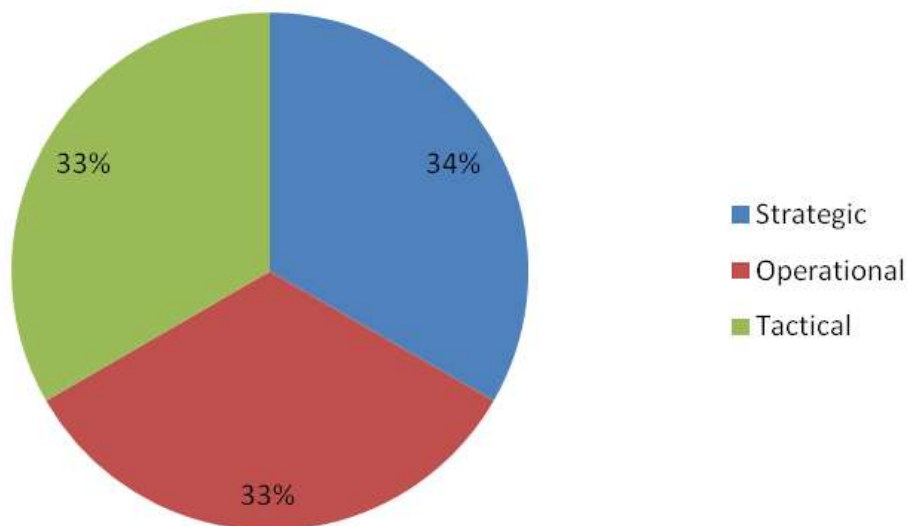


Figure 3: Percentage of Respondents with Strategic, Operational and Technical as the Highest Ranked Target Group



## Maturity and Targets for Individual Controls

Figure 4 shows the top ten control areas assessed by respondents as being, on average, most mature.

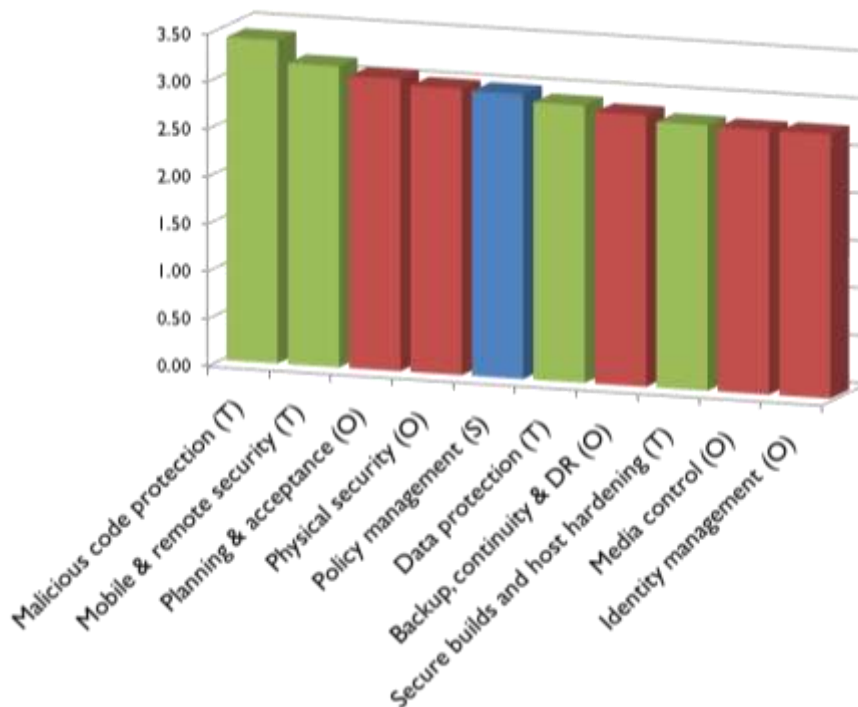


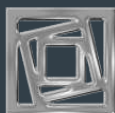
Figure 4: Top 10 Most Mature Control Areas

As expected, figure 4 shows that 9 of the **most** mature controls are either operational or tactical. Malicious code protection is probably the best-understood technical control area, and it is therefore no surprise to find it as most mature. The fact that mobile and remote security is in second place reflects the emphasis that has been placed on this area in recent years; following high-profile information breaches related to it. It is interesting that policy management is the only strategic control that appears in the top 10; reflecting the fact that most organisations begin to tackle information assurance by putting appropriate policies in place.

On the other hand, as figure 5 shows, of the 10 **least** mature control areas, 7 are in the strategic group. The single tactical control area (access) not only presents many technical challenges; but also involves strategic issues related to human resources and the requirement for coordination throughout the organisation. Similarly, the two related operational controls (incident handling, monitoring and response) are complex issues with strategic ramifications in terms both of coordination and human resources.

As organisations move towards utilising “the cloud” for the delivery of IT as a service; many of the controls shown in figure 5 will increase in importance. Specifically:

- Access controls;
- Metrics and audit;
- Business alignment and governance;
- Architecture and planning;
- Compliance management.



Information Risk Management Maturity 2010 Survey Summary

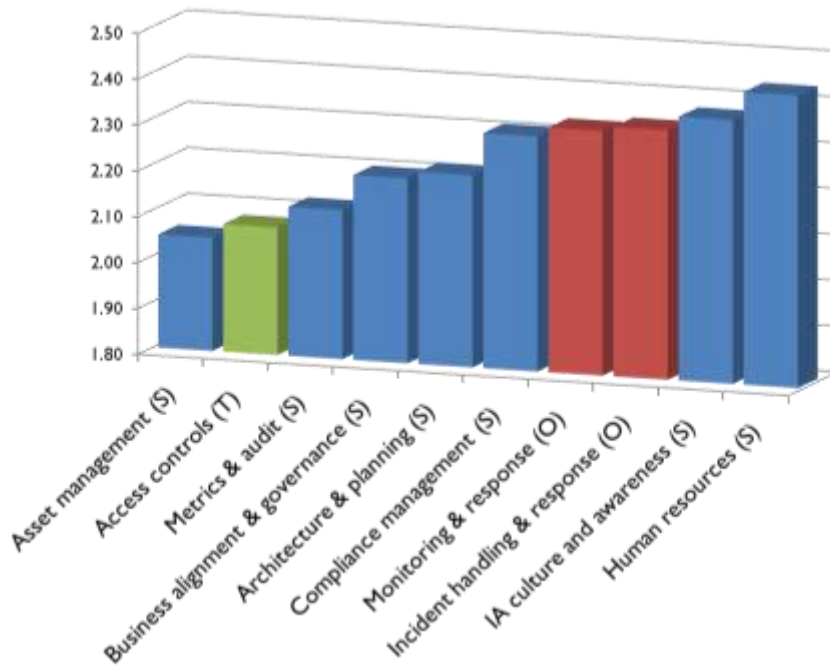


Figure 5: 10 Least Mature Control Areas

Figure 6 reflects the target setting preoccupations of the responding organisations; showing the control areas that were given the 10 highest maturity targets. In view of previous observations it is unsurprising that only one strategic control area appears in the top 10. Once more this shows that generally organisations are more prepared to tackle issues of a technical nature than those that are strategic.

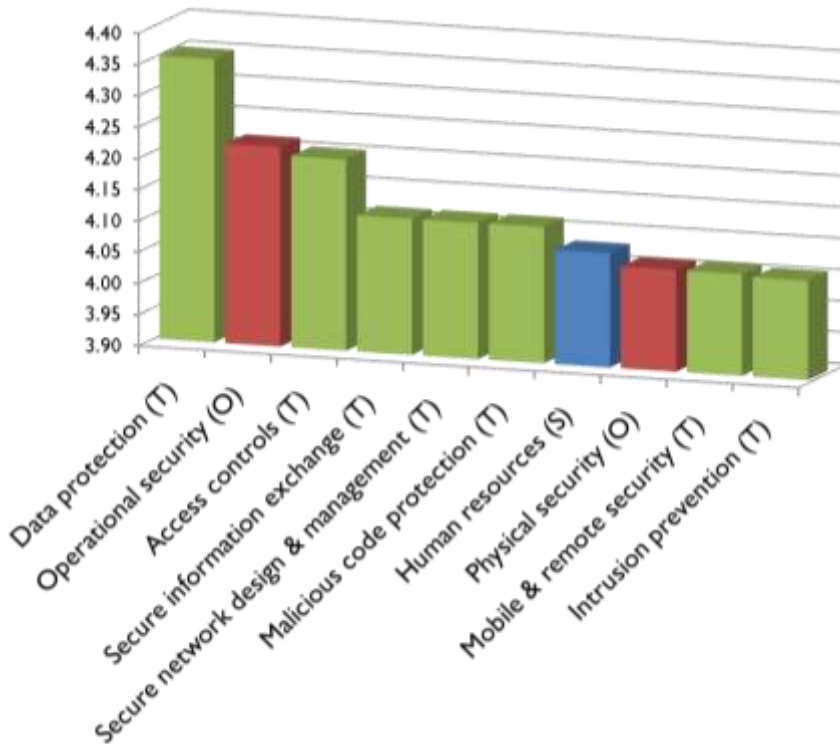


Figure 6: Top 10 Target Control Areas

For example, the presence of data protection in first place is likely to reflect an attempted technical response to the legal and regulatory challenges currently posed by personally identifiable information (PII) issues; at the expense of tackling relevant strategic problems such as compliance management. However, the ranking of operational security in second place is likely to indicate organisations' realisation that this control area underpins many operational and



tactical controls. Access control has already been noted as a maturity issue; so it is understandable that organisations are keen to target it. Perhaps less understandable is the absence of vital, and immature, strategic areas such as asset management and metrics and audit. It is also perhaps an indication of continued over-reliance on technical controls that malicious code protection appears at number 4 on the list.

## Control Gaps

Table 1 shows the ten control areas that have the largest gaps between the average current and target maturity scores. Here strategic control areas comprise 4 of the top 5. In general the list reflects those issues highlighted in figures 5 and 6.

Analysis of the top 10 gaps for each of the organisations which took part in the survey has revealed a surprising degree of consistency. The gaps of at least 30% of the control areas for all organisations were the same as those in the list below, with one organisation having 100% of its top 10 control gaps as in the table below. On average the organisations responding to the survey shared 58% of their top 10 control gaps with the average list shown below. The implication of this is that most organisations have similar information assurance issues in common. Information sharing on this subject is therefore likely to prove productive.

Rank	Control Area	Average Current Maturity	Average Target Maturity	Difference
1	Access controls (T)	2.08	4.21	2.13
2	Asset management (S)	2.05	3.97	1.92
3	Metrics & audit (S)	2.13	3.97	1.85
4	Incident handling & response (O)	2.34	4.03	1.69
5	Architecture & planning (S)	2.22	3.88	1.66
6	Human resources (S)	2.44	4.08	1.64
7	Compliance management (S)	2.31	3.94	1.63
8	Operational security (O)	2.59	4.22	1.63
9	Intrusion prevention (T)	2.44	4.06	1.62
10	Remote & extranet coverage (T)	2.45	4.06	1.61

Table 1: Gap between Top 10 Current and Target Capabilities for the Average Organisation

## Recommendations

The results of this survey have served to confirm a number of observations that information assurance practitioners have made concerning the organisations with which they have worked. These observations can be used to suggest the following recommendations:

- Organisations should give more emphasis to the implementation of important and fundamental strategic controls; in particular to asset management.
- Organisations should consider their target maturity levels, particularly for strategic controls, in order to ensure that these are realistic and achievable.
- Organisations should consider if technically-based controls are necessarily the appropriate solution to an issue; strategic and process-driven controls (such as better compliance management) may be more effective.
- Organisations should give serious consideration to the importance of implementing controls (such as metrics and audit) that will enable them to monitor and measure the effectiveness and efficiency of their information assurance management.
- Organisations should consider employing information sharing mechanisms in order to improve the management of common information assurance issues.



- Organisations should consider the expenditure of resources on developing a well-articulated and clearly communicated action plan for the implementation of information assurance controls; in order to avoid unnecessary and duplicated effort.

## Conclusions

Effective information assurance enables the right people use the right information at the right time; giving a significant competitive advantage to any organisation in which it is implemented.

This survey has shown that organisations can understand their information assurance maturity by answering a relatively small number of key questions. All respondents were able to complete this survey in less than two hours. By entering both their current and desired maturities they were able to develop a rapid overview of both their present information assurance management and their future needs. The results enable them to develop a prioritised action plan for the improvement of information assurance management in their organisation.

The survey data also provides potentially valuable benchmarking for organisations. Individual survey respondents are able to compare the average data given in this report with their own survey results. This enables them to understand the position of information assurance management in their organisation in relation to that of partners and competitors.

However, before committing significant resources to an action plan; it is advisable for organisations to develop further in-depth analysis of the 31 control areas. This will help to pinpoint the most cost effective ways to improve information assurance controls to maturity levels that are both realistic and appropriate.

Information protection will be increasingly critical as organisations' IT infrastructures change to support technologies and methodologies for new business processes; particularly those within "the cloud". This emphasises the vital role that can be performed by information assurance metrics that are automatically gathered, so that risks can be continually assessed. Only in this way can organisations ensure that their IT environment is evolving to meet the levels of information assurance that are essential to meet their changing business needs.



## About ExecIA LLP



Based in the UK, but working globally, ExecIA has been formed to deliver a series of capabilities built around our years of experience in IT security, programme and IT operational management. This experience has been gained in the commercial and government sectors; both as users and suppliers.

ExecIA's approach is to help customers understand their information assurance risk and risk control measures in the context of their business. In particular:

- How your organisation's risk controls ensure that vital business information is available, shared appropriately and used efficiently.
- The effect on your business of better management of risk controls.
- The value of a prioritised action plan to implement improvements to risk controls.

ExecIA brings together IT operations, IT security, IT risk and business stakeholders to identify objectives, risks and prioritised actions. Better communication and the development of a common view is a major step towards information assurance improvement.

This survey is based on a detailed consulting tool, which we have designed to support the processes described above. The full version of the tool has more than 200 additional in-depth questions allowing for a rigorous analysis of each of the information assurance control areas. The in-depth questions are mapped against various standards, such as ISO27002 and HMG SPF; helping you to concentrate on those areas most important for good governance and compliance.

## Contact Us

For more information on how to improve information assurance:



[www.execia.com](http://www.execia.com)



[contact@execia.com](mailto:contact@execia.com)



Richard Archdeacon 07881 521 460

