Heads of Internal Audit Service Benchmarking Report

Institute of Internal Auditors
UK AND IRELAND

Control Risk Self-Assessment (CRSA)

Introduction

This report contains the results of the HIAS survey entitled *Control Risk Self-Assessment (CRSA)*. The results include answers from all respondents who took the survey in the 9 day period between 30 April 2008 and 8 May 2008. Sixty six completed questionnaires were received during this time from a potential total of 320 providing a response rate of 21%.

Responses have been received from a broad cross section of private and public sector organisations (70%:30%). While the majority of organisations (approximately 80%) have their headquarters in the UK and Ireland there is a strong international context to the survey, predominantly within the EU, North America and Europe.

Most of the organisations that have taken part (75%) have over 1,000 staff with 25% having 1,000 - 5,000, 25% 5,000-10,000 and 25% over 10,000. The size of the participating organisations is also reflected in annual turnover with over 65% having in excess of £500m, with the largest group (30%) £1bn-£5bn.

The number of participants and the size and scope of their operations provides an established base and valuable cross section upon which to analyse the organisation and practice of control risk self-assessment. The results also highlight some of the practical issues and potential pitfalls associated with implementation.

The extent of CRSA.

Two thirds of organisations currently operate a CRSA programme demonstrating this is a widely used technique to identify and assess risks. A further 14% of all respondents highlighted that they plan to implement a programme within the next year or two. Of those that use CRSA the majority, 44%, apply the approach to 10 or less self-assessing entities, typically subsidiaries or departments. A further 37% extend CRSA to 10 to 50 entities.

While this shows the prevalence of CRSA 20% of all respondents feel that they have either not reached a stage where CRSA can be implemented effectively or they feel there is limited value in its implementation. Analysis of the raw data on the ‘no’ responses does not indicate any specific pattern to sectors or industries.

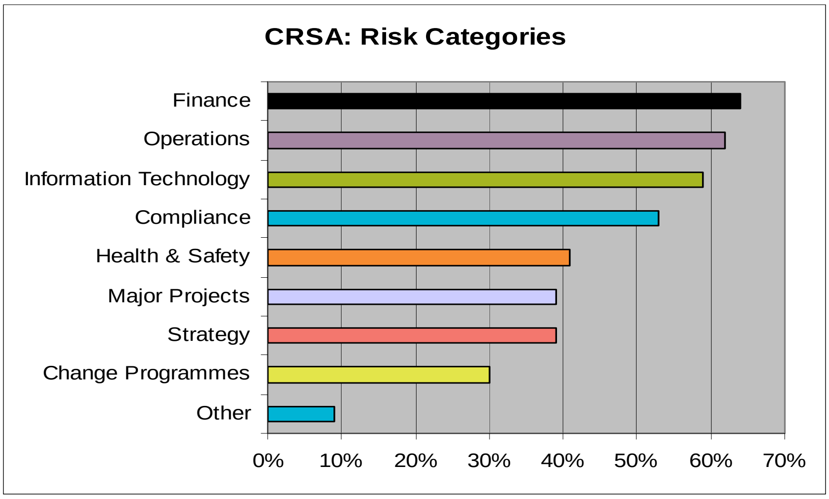
Specific comments on these issues are highlight later in the report.

The identification and assessment of risks.

Only a few organisations, less than 10%, rely solely on a pre-defined standard list of risks to carry out CRSA. The majority, just over half, require individual subsidiaries and departments to identify their own risks. While the remainder, approximately 40%, use a combination of both methods suggesting an element of standardisation with local flexibility to create a top-down, bottom-up approach.

The scoring of inherent risks is essentially pre-determined to provide consistency across the organisation, although 20% appear to have no guidelines.

The starting point of the CRSA is key company objectives in 32% of the cases while 55% let local entities start with their own assessment. This seems to indicate that CRSA is generally more focused upon operational rather strategic risks. This is supported by the table below, which shows that CRSA has an emphasis towards finance and operations as the main categories of risk followed closely by information technology and compliance.



In general each local entity assesses less than 10 key controls per risk area, with no more than 100 in total.

It was hoped that the survey would illustrate how organisations identify risks that impact across a number of local entities and departments and how they approach effective co-ordination. The table below indicates a mixed set of results making it difficult to draw any firm conclusions, but it would appear that greatest reliance is placed upon a central CRSA or Risk Management function to establish some form of coordination.

Response	Count	Percent
Local management identify all risks that impact the organisation regardless whether they can affect them or not within their area of responsibility.	7	10.6%
Local management identify only the risks that it controls.	11	16.7%
Central management identify and address those risks which it can affect and which go across the organisation.	14	21.2%
Risks are identified locally and centrally. It is up to both locations, to make sure that the risks are addressed overall.	22	33.3%
Ask each local manager individually to address risks although this may go beyond their area of responsibility and assuming management will co-ordinate.	3	4.5%
We have clearly mapped in advance who is responsible for which process and the CRSA assessors assesses accordingly. Risks assessed & identified locally vs. centrally can directly be mitigated at the respective levels without need to coordinate.	4	6.1%
The CRSA/ Risk Management Function plays a key role in coordinating and makes sure that the risks are addressed at appropriate level.	24	36.4%
No specific rule for this and it may be unclear.	8	12.1%

Validation and testing of CSRA results

In terms of validation and testing the survey shows that in 32% of cases managers need to confirm they have followed the process correctly and that the results are accurate. Some, but not all, carry out independent validation and testing of the results. Where this is the done Internal Audit are the main assurance providers (41%) followed by the Risk Management/CRSA function (20%). In a few cases only, the risk owner validates (12%) or tests (3%) the results.

Comments

Additional comments and information included within survey by internal auditors have provided useful insight to the relative importance and perceived value of CRSA.

Where CRSA has not been implemented there are two general views. Firstly, there is a group of responses that suggest that CRSA would be useful but priority is being placed on establishing risk management procedures. As one participant described, “It would be too early in the development of the organisation’s risk culture.” A second view is that CRSA has not been implemented to prevent any distraction from the enterprise risk management procedure; with one participant suggesting that there would be ‘no appetite’ for further risk management processes.

Where CRSA is operational there are a number of comments indicating that it is perceived as a low level ‘tick box’ exercise where people ‘respond quickly with little thought to the responses’. Others suggest that it is overly bureaucratic and in danger of being another low-importance exercise. One participant has stated, “It is difficult to keep fresh and dynamic, especially in operational areas.”

Some participants have also questioned the value of CRSA where the process lacks independent validation. One specific comment summed this up concisely by stating “CRSA has the fundamental weakness that it lacks independence compared to internal audit. As such, it is not an alternative to internal audit, and it is regrettable that it is sometimes discussed as if it were.”

There is also a view that CRSA is a useful technique where there is a commitment and culture to support its ongoing operation. ‘We have simplified the CRSA process removed as much jargon as possible and embedded it into day to day management by demonstrating the links to objectives and also to what people actually do on a daily basis.”

Conclusions

CRSA is a widely used technique in the private and public sectors. Two-thirds of the organisations who completed the survey use CRSA to identify and assess risk. The majority of organisations allow local entities to identify their own risks with some inclusion of centrally defined risks along with guidance on assessing/scoring of risks. This lighter touch approach, assessing risks applicable to day to day operations appears to be a perceived recipe for succeeding as highlighted by some of the comments and answers.

The co-ordination of cross functional/ company risks places quite some reliance on management and a central risk management function.

Additional comments included in the survey suggest that some organisations are simply not ready for CRSA and that others prefer not to use it, placing emphasis on enterprise risk management. Problems appear to arise where the process is overly complex and where it is perceived as a low-level operation. Some, but not all, carry out independent validation and testing of the results and participants have challenged the value of CRSA without some form of objective assurance. Where this is done Internal Audit is the most frequently used source.

Institute of Internal Auditors
UK AND IRELAND

Heads of Internal Audit Service Benchmarking Report

Copy of survey issued to Service members

Control Risk Self Assessment

A member of the Heads of Internal Audit Service (HIAS) is currently reviewing his company's Control Risk Self Assessment Process. He is particularly interested to learn how other organisations:

- Decide upon the categories of risk covered by the Control Risk Self Assessment program, if there is one in place.
- Identify and define inherent risks within each category (standard list vs. free format).
- Structure the CRSA program.
- Establish the level of detailed operational risks and controls to be assessed.
- Coordinate the management of risks across companies.
- Control the quality of CRSA through validation and testing.

Your input to this research will be valuable and we would appreciate a few minutes of your time to complete the attached questionnaire.

1) What is your industry sector (choose one from this list):

○ Banks and building societies
○ Insurance
○ Other financial services
○ Food and drink
○ Manufacturing and engineering
○ Pharmaceuticals
○ Media and leisure
○ Retail
○ Telecommunications
○ Utilities
○ High technology
○ Other private sector
○ Voluntary/charity
○ Education
○ Central government
○ Local government
○ Health
○ Other public sector
○ None of the above

2) Where is your organisation's headquarters?

○ UK
○ Ireland
○ Outside UK & Ireland

3) What countries/continents do you operate in (please tick all that apply)

- ☐ UK
- ☐ Ireland
- ☐ Rest of Europe (EU)
- ☐ Rest of Europe (non EU)
- ☐ North America
- ☐ Central America
- ☐ South America
- ☐ Africa
- ☐ Asia
- ☐ Australia/New Zealand
- ☐ Pacific
- ☐ Other (please specify)

If you selected other, please specify

____

4) What is the total number of employees in your organisation? (worldwide total for multi-nationals)

- ○ less than 101
- ○ 101 to 200
- ○ 201 to 500
- ○ 501 to 1,000
- ○ 1,001 to 2,500
- ○ 2,501 to 5,000
- ○ 5,001 to 10,000
- ○ 10,001 to 25,000
- ○ 25,001 to 50,000
- ○ over 50,000

5) What is the turnover or gross revenue spend of your organisation? (provide the worldwide total for multi-national organisations)

- ○ up to £50 million or €62.5 million
- ○ £51 - 100m or €63 to 125m
- ○ £101 - 200m or €126 to 250m
- ○ £201 - 350m or €251 to 437m
- ○ £351 - 500m or €438 to 625m
- ○ £501 - £1bn or €626 to €1.25bn
- ○ £1bn - 5bn or €1.25bn to €6.25bn
- ○ £5bn - £10bn or €6.25bn to €12.5bn
- ○ Over £10bn or €12.5bn

6) Do you have a CRSA or similar Business Risk Assessment programme in your organisation?

- ○ Yes
- ○ No

7) How many self assessing entities does your organisation have? (typically a subsidiary for a private company or a department for a public sector organisation)

- ○ Less than 10
- ○ 10 to 50
- ○ 51 to 100
- ○ 101 to 300
- ○ 301 to 500
- ○ 501 to 1000
- ○ More than 1000

8) How do entities identify inherent risks?

○ Entities are given a pre-defined list of risks
○ Entities are required to define their own risks
○ A combination of the above

9) How do entities score inherent risks?

○ Scores are pre-set for inherent risks
○ Guidelines are provided to score score inherent risks
○ No guidlines are provided to score inherent risks

10) What is the starting point for your CRSA program?

○ Standard processes and assess whether there are key formalised procedures in place.
○ Standard processes and assess whether there are key controls in place to mitigate risks.
○ Key objectives and assess whether there are key controls in place to mitigate the risks.
○ Locally identified risks and assess whether there are key controls in place to mitigate the risks
○ Other (please specify)

If you selected other, please specify

____

11) Which categories of risk does the CRSA program cover?

☐ Strategy
☐ Finance
☐ Information Technology
☐ Operations
☐ Health & Safety
☐ Compliance (legal, code of ethics, policies)
☐ Major Projects
☐ Change Programs
☐ Other

12) In general, how many key controls does one local "entity" identify and assess for each of their risks, objectives or processes ?

○ Less than 10
○ 11 to 20
○ 21 to 30
○ 31 to 40
○ 41 to 50
○ More than 50

13) In general, how many key controls does one local "entity" identify and assess in total?

○ Up to 100
○ 101 to 500
○ 501 to 1000
○ More than 1000

14) How does your organisation coordinate the management of risks across entities?

☐ Local management identify all risks that impact the organisation regardless whether they can affect them or not within their area of responsibility.

☐ Local management identify only the risks that it controls.

☐ Central management identify and address those risks which it can affect and which go across the organisation.

☐ Risks are identified locally and centrally. It is up to both locations, to make sure that the risks are addressed overall.

☐ Ask each local manager individually to address risks although this may go beyond their area of responsibility and assuming management will co-ordinate.

☐ We have clearly mapped in advance who is responsible for which process and the CRSA assessors assesses accordingly. Risks assessed & identified locally vs. centrally can directly be mitigated at the respective levels without need to coordinate.

☐ The CRSA/ Risk Management Function plays a key role in coordinating and makes sure that the risks are addressed at appropriate level.

☐ No specific rule for this and it may be unclear.

☐ Other (please specify)

If you selected other, please specify

____

15) How are the CRSA results validated and tested?

☐ The risk owner formally confirms that CRSA has been performed in accordance with company requirements.

☐ The risk owner validates as part of the CRSA process, but without testing requirements.

☐ The risk owner validates with testing requirements.

☐ Internal Audit validates and tests, as part of its ordinary activities.

☐ There is a specific function such as a Risk Management/ CRSA function, which is responsible for the accuracy.

☐ Other (please specify)

If you selected other, please specify

____

16) Are you planning to introduce CRSA in the future?

○ No

○ Yes, within the next 6 months

○ Yes, within the next year

○ Yes, within the next year or two

17) Is there a specific reason why your organisation has chosen not to introduce CRSA?

____

____

18) Please provide any further comments about CRSA in your organisation or CRSA in general that may be relevant.

____

____

Data Protection Notice

Thank you for completing the survey, your views and opinions are very important.

Your response will be treated in total confidence.

Completed questionnaires will be processed only by the Institute of Internal Auditors - UK and Ireland (IIA) using Vovici EFM Continuum software and will not be disclosed to any other third parties. By submitting this questionnaire you consent to our processing of your sensitive personal data for these purposes

The Institute of Internal Auditors – UK and Ireland (IIA)

The IIA has been leading the profession of internal auditing for over 60 years. We are the only body focussed exclusively on internal auditing and we are passionate about supporting, promoting and training the professionals who work in it.

Every year we help thousands of internal auditors at every stage of their career with training, qualifications and technical resources enabling them to deliver exceptional results for their organisations.

Our *International Standards* and *Code of Ethics* unite a global community of over 130,000 IIA internal auditors. These Standards mean that employers can be sure that IIA members across the world operate with integrity and to the highest levels of professional competency.

About Heads of Internal Audit Service benchmarking reports

The IIA recognises that heads of internal audit need specialist information and support to help them respond to the demands of a competitive and increasingly regulated business climate.

The Heads of Internal Audit Service is a complete and exclusive service designed specifically for the leaders of the profession to keep them up to date and to provide them with introductions to their contemporaries and opportunities to discuss successes and concerns in confidence with their peers. Other services include access to technical updates, a quarterly newsletter, a series of professional forums, and specifically commissioned research.

The benchmarking reports are designed to help HIAS members make the most of the Service's networking opportunities. Service members can pose a question to other Service members to help them identify best practice on a particular issue. Service members can submit a question for consideration as an Enquiry by emailing chris.baker@iia.org.uk or technical@iia.org.uk

Disclaimer

This material is not intended to provide definitive answers to specific individual circumstances and as such is intended to be used only as a guide. The IIA recommends that you always seek independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this guidance.

www.iia.org.uk

The Institute of Internal Auditors – UK and Ireland Ltd
13 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX
Tel 020 7498 0101 Fax 020 7978 2492 Email technical@iia.org.uk

Registered in England and Wales, no. 1474735

Information can be made available in other formats