How effective is internal auditors' cyber security assurance?

Introduction

The European Confederation of Institute of Internal Auditors recognises cyber security (CS) as **one of the top five business risks**. The recent global pandemic has only intensified it by telecommuting, expanding work environment with videoconferencing software, adding personal devices, and private WiFi networks to organization's systems. Despite orchestrated efforts in CS risk management, the number of successful attacks is still growing.

Principles of sound risk management warrant that **cyber security risk management is organised in the three lines model**. Business units together with the information technology function represent the first line. The information security risk management represents the second line of cyber security. An independent assurance that CS risk management strategy, policies, procedures and controls are effective if is provided by the third line the internal audit function (IAF). Yet, many IAFs lack expertise and resources in the area of cyber security.

This eBrochure reports the findings of a joint research project of the University of Queensland (Australia) and the University of Split (Croatia) about the effectiveness of cyber security risk assurance. We developed an **original Index of CS assurance effectiveness** and measured it on a large-scale international sample.

183 of Chief Audit Executives (CAE) and IT auditors from 20 different countries, organizations of various sizes and industries participated in the survey from the end of May 2020 till the beginning of August 2020.

What constitutes effective assurance of cyber security risk management?

Survey methodology

We measure CS assurance effectiveness with a process approach that is based on the premise that **internal audit is effective** if the procedures of **planning, performing and reporting** on audit findings on cyber security (CS) risk management **follow standards, professional guidelines and best practices.**

An effective **planning** requires that IAF assesses the existing CS risks and considers emerging risks, changes in regulation and industry trends. The IAF should proactively identify the risks of an organization and the controls that mitigate these risks, map regulatory requirements to facilitate compliance by default, inform the organization which controls are already in place and develop a plan to implement missing controls based on their cost effectiveness.

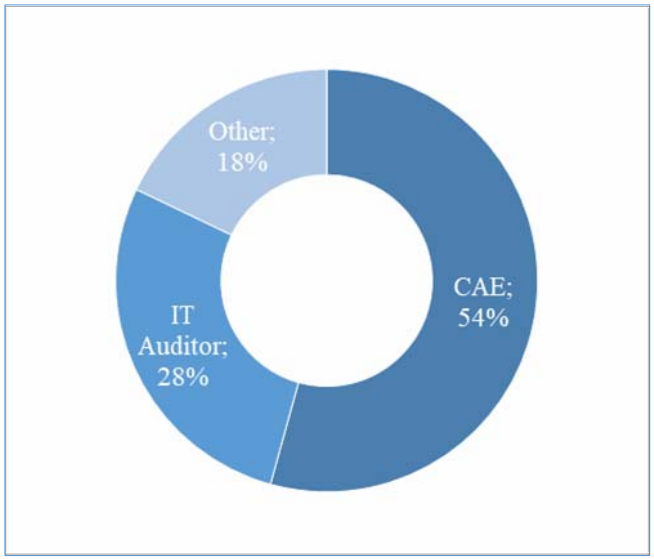
Performing engagement relates to comprehensiveness of audit evidence - the breadth of review - and to the reliance on a number of audit procedures through which evidence is acquired - the depth of review.

We define effective **reporting** as a provision of a comprehensive report on CS risk management effectiveness to the Board and its Audit or Risk Committee.

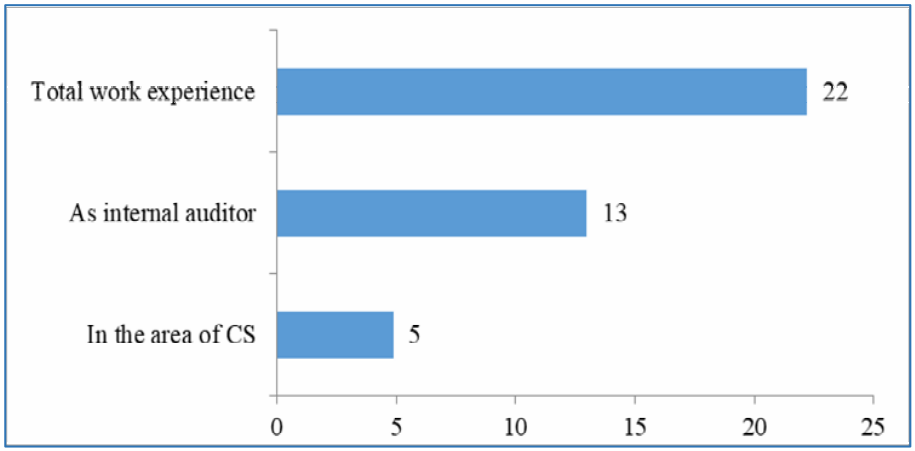
To measure how effectively internal auditors perform cyber security risk assurance, we developed an Index covering each of the three phases with a variety of indicators. More detail is provided below.

Participants' profile (1)

Current work position in internal audit (n=151)



Average work experience (in years): as internal auditor, total work experience, and in the area of cyber security (n=151)



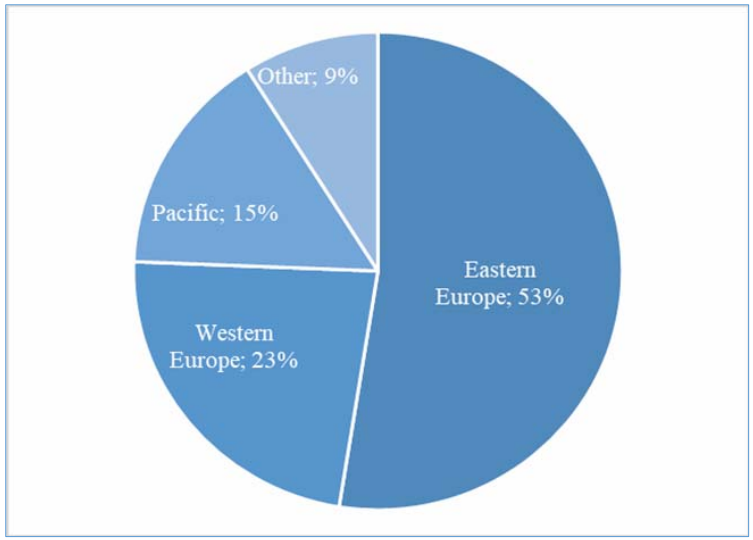
The survey was distributed to **19 IIA Affiliates and 3 ISACA Chapters in Europe** and **1 ISACA Chapter in the USA** via monthly newsletters or emails to the members of respective institutes.

183 participants completed the survey. However, the total number of respondents on the specific question is varying because of the missing data problem. The participants who completed the survey received their score of effectiveness of cyber security assurance at the end of the survey. They can compare this score with this overall report.

The participants have on average 22 years of work experience and at 13 years of experience in internal audit and 5 years of work experience in the area of cyber security. However, 31% of the participants do not have any work experience in cyber security.

Participants' profile (2)

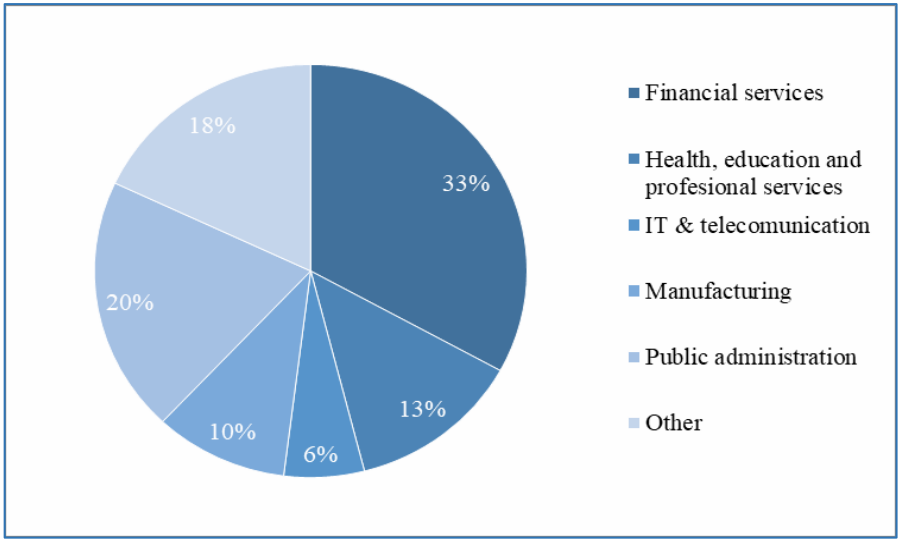
Distribution of the participants by Region (n=156)



The majority of the respondents are from **Western and Eastern Europe (76%)** and 15% respondents from Australia and New Zealand.

** Other includes all other countries that could not be assigned to a specific region because of small frequencies, such as Israel, US or Vietnam.*

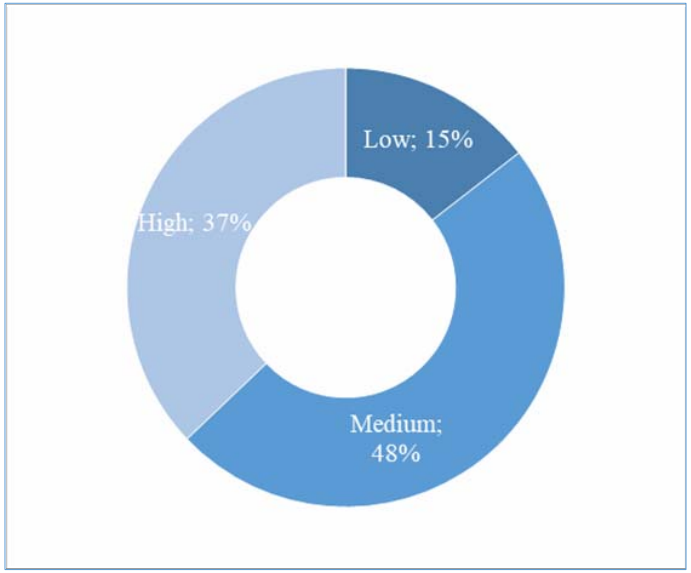
Distribution of the participants by Industry (n=159)



Over a third of participants work in financial services (33%). The size of organisations varies considerably from less than 20 employees to more than 10,000 employees.

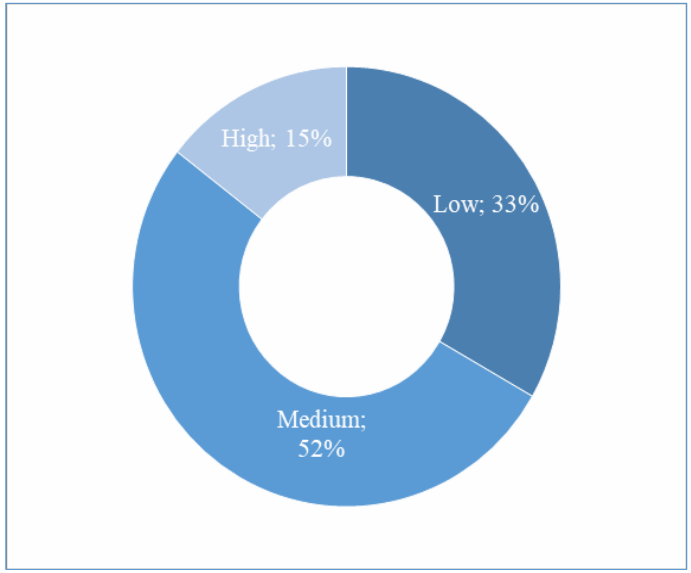
Participants' profile (3)

The level of IT technology deployed (n=154)



The majority of the participants' organisations have **medium (48%) and high (37%) levels of digitalisation.**

Cyber security risk appetite (n=154)

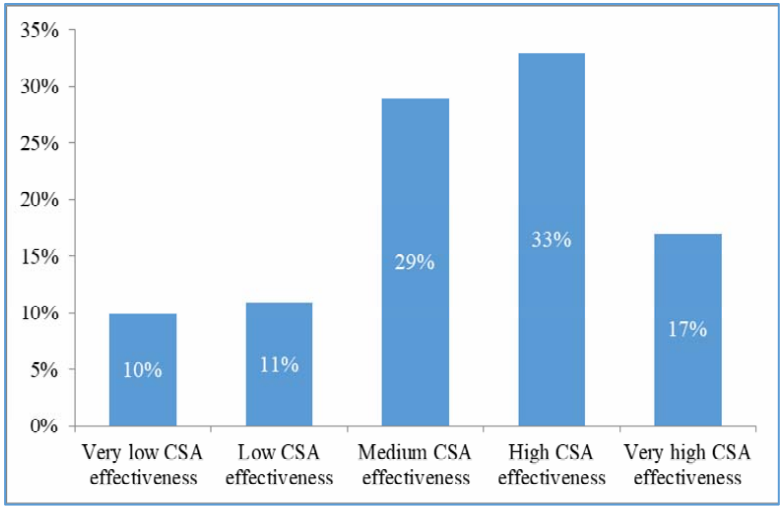


Thirthy three percent (33%) of participants assesses CS risk appetite of their organisation as low.

Findings

Effectiveness of cyber security assurance (CSA) CSA Index

Level of CSA effectiveness (n=181)



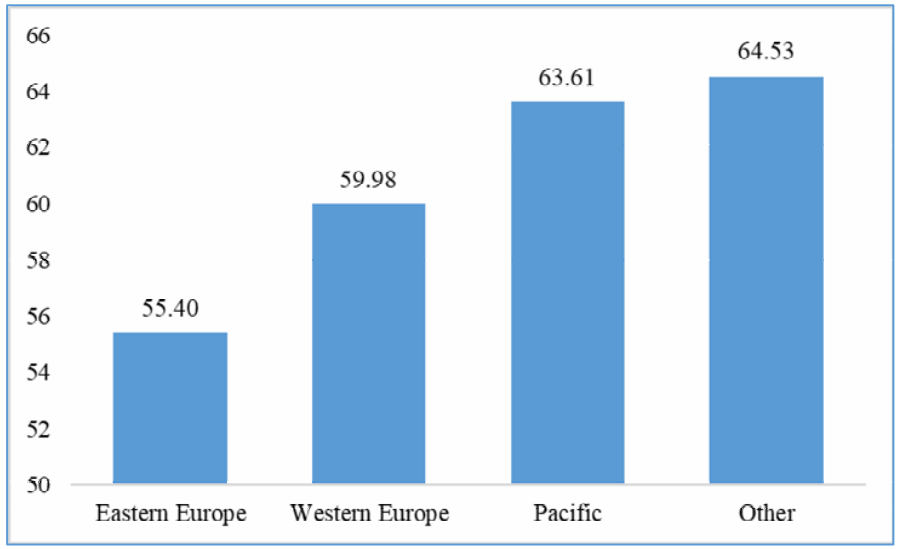
Level of CSA effectiveness	Index
Very high CSA effectiveness	81-100
High CSA effectiveness	61-80
Medium CSA effectiveness	41-60
Low CSA effectiveness	21-40
Very low CSA effectiveness	0-20

The average score of the overall CSA Index is 58 on a scale from 1 to 100. For the majority of organisations (50%) in this survey the CSA Index is higher then 61 indicating **high and very high effectiveness.**

The Planning phase is performed most effectively with the highest mean (64) while the **Performing** and the **Reporting** phase have means of 54 and 55, respectively.

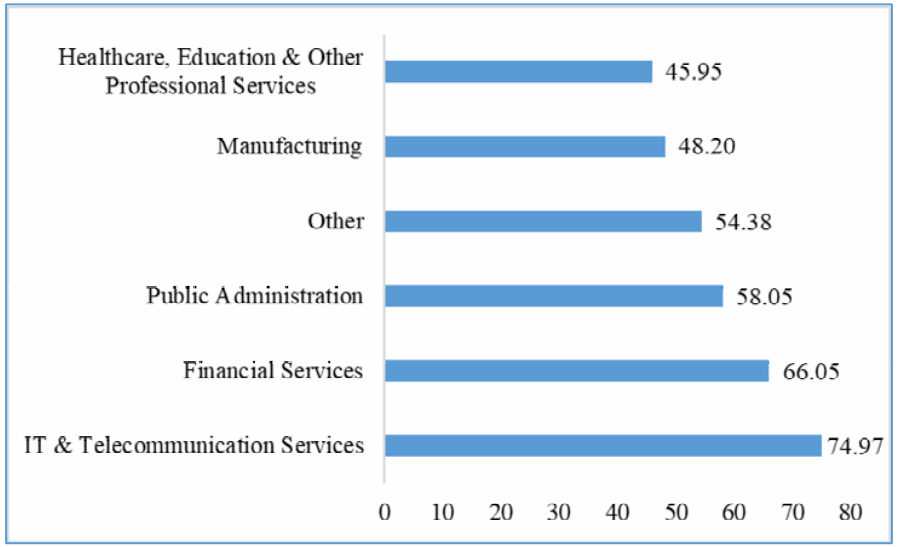
CSA Index *vs* Region & Industries

CSA Index by Region (n=156)



We found **no significant difference** in the Index among the **analysed regions**.

CSA Index by Industries (n=159)



IT & Telecommunication sector has the highest average CSA Index (75), followed by Financial services (66).

Would you like to know your CSA?
Click here: Cyber Security Assurance Index

Planning cyber security assurance

IAF's proactiveness and strategic planning

Planning is the first component of the CSA index. The more proactive and strategically oriented the IAF is, the better risk assessment it makes and the more accurately it plans its activities. We measured a number of indicators about proactiveness of the IAF and its strategic orientation in terms of understanding industry benchmarks and organisation's exposure, reliance on risk-based approach in planning, assessment of the alignment between overall and cyber security strategy of the organisations and some others (for more detail, see below).

Overall, the majority of participants indicated **moderate proactiveness and strategic orientation regarding cyber security risk assessment.**

The extent the statements below correspond to your practices (1 not at all, 2 slightly, 3 moderately, 4 considerably, 5 completely)

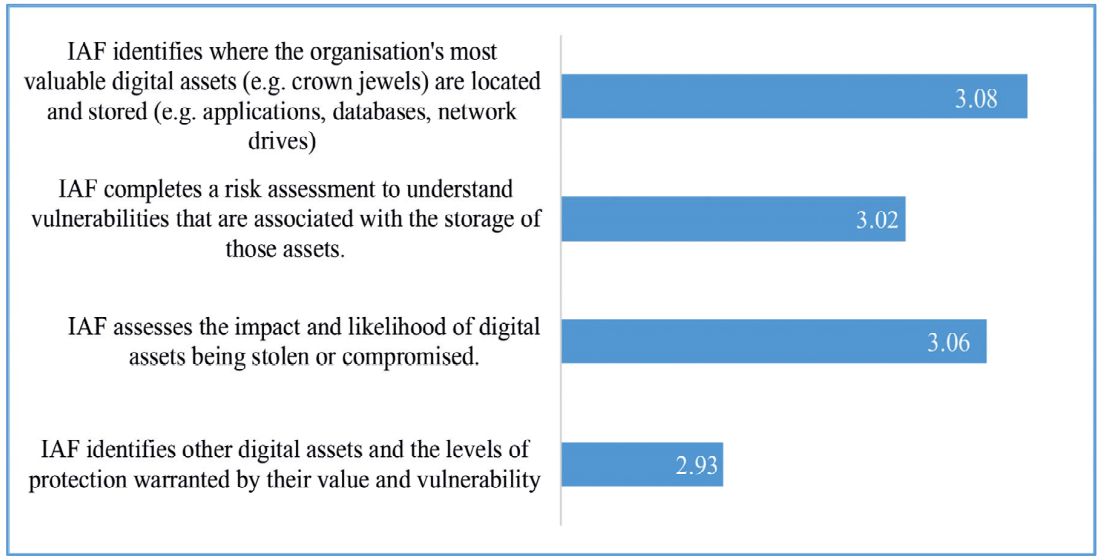
IAF's intial risk assessment

We measured how well the IAF **identifies the risks of an organisation and the controls** that mitigate these risks with a number of indicators, such as whether it **identifies the organization's crown jewels** and establishes what it would mean if they were compromised and whether it completes a risk assessment to understand vulnerabilities associated with the storage of most valuable digital assets.

Practices in assessing risks vary among organizations. Some IAF rely on the assessment of risks by the second line, whereas some IAF assess risks on their own. **Risk assessment dictates the frequency of internal audits of CS.**

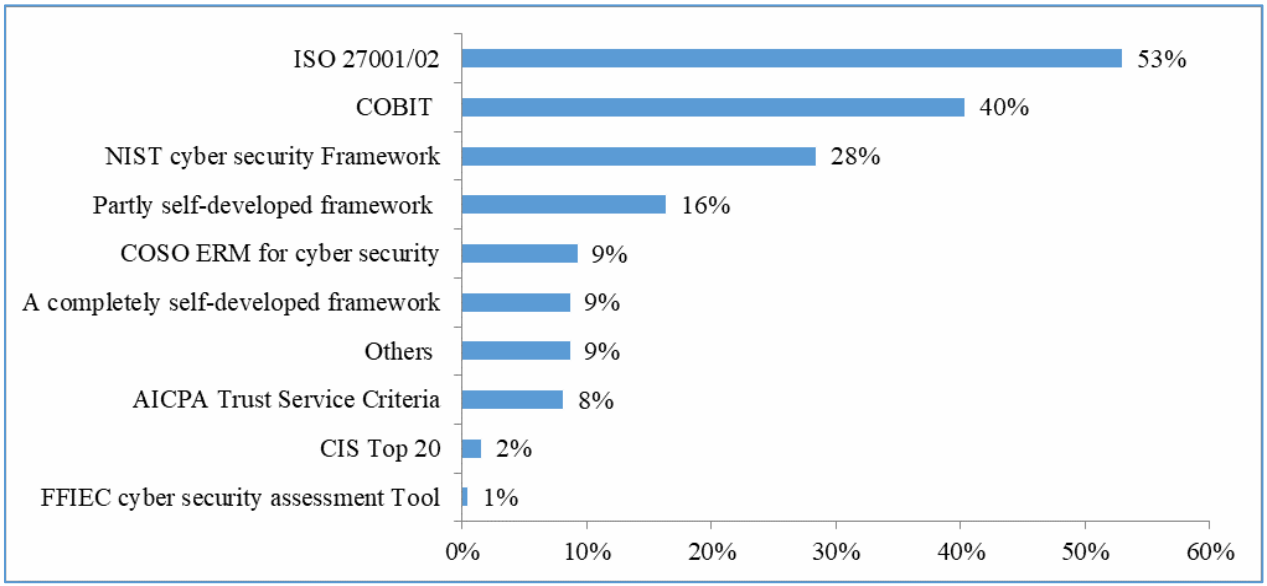
Participants indicate **moderate involvement of IAF in risk assessment.**

The extent the statements below correspond to your practices (1 not at all, 2 slightly, 3 moderately, 4 considerably, 5 completely)



Cyber security frameworks

Cyber security frameworks used



Cyber security frameworks set out the standards that an IAF audits against and are helpful in establishing the audit universe.

The use of any cyber security framework exhibits greater effectiveness of audit than no reliance on CS frameworks. **Eighty two percent (82%) of our participants use one or more frameworks in developing CS audit plan**.

Organisations predominantly use **ISO 27001/02** (53%), **COBIT** (40%) and **NIST** (28%). Some organizations (16%) use **partly self-developed frameworks**, which are mostly based on the above three frameworks.

Performing cyber security assurance

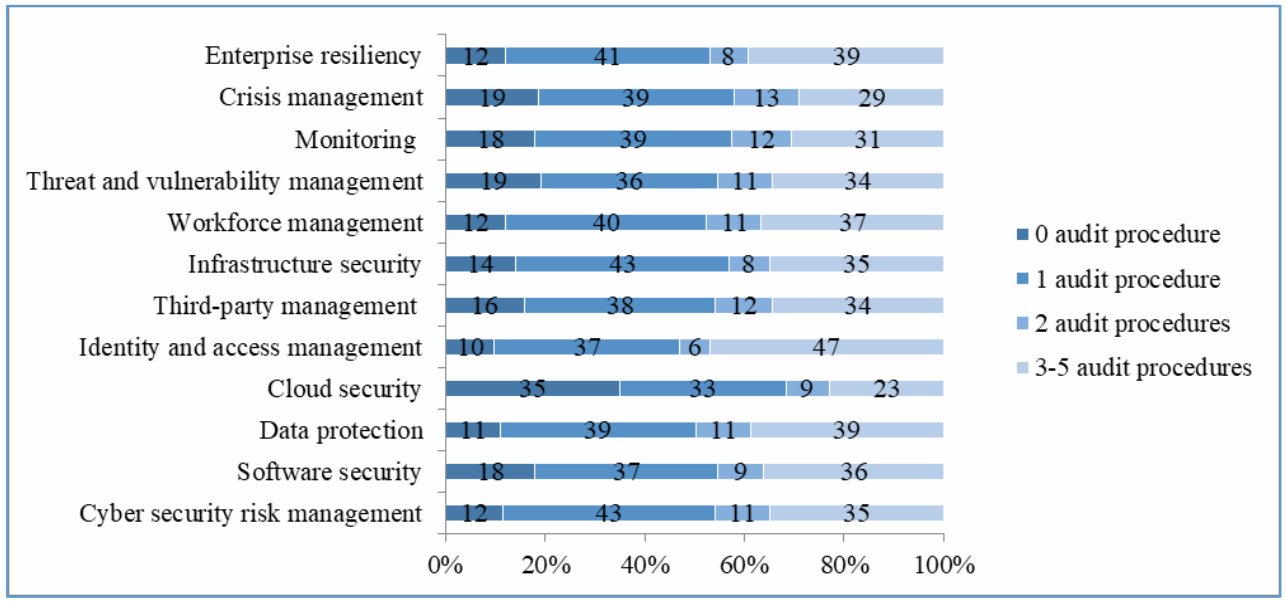
Areas of review

Performing engagement is the second phase and relates to not only how comprehensively audit evidence is collected but also to the audit procedures with which this evidence is acquired.

Cloud security is the least extensively reviewed CS area, whereas Identity and access management and Data protection are most frequently audited areas.

For an internal audit to be considered effective, competent and sufficient evidence must be gathered to construct an informed decision. As the figure shows a variety of procedures are used for each of the CS areas.

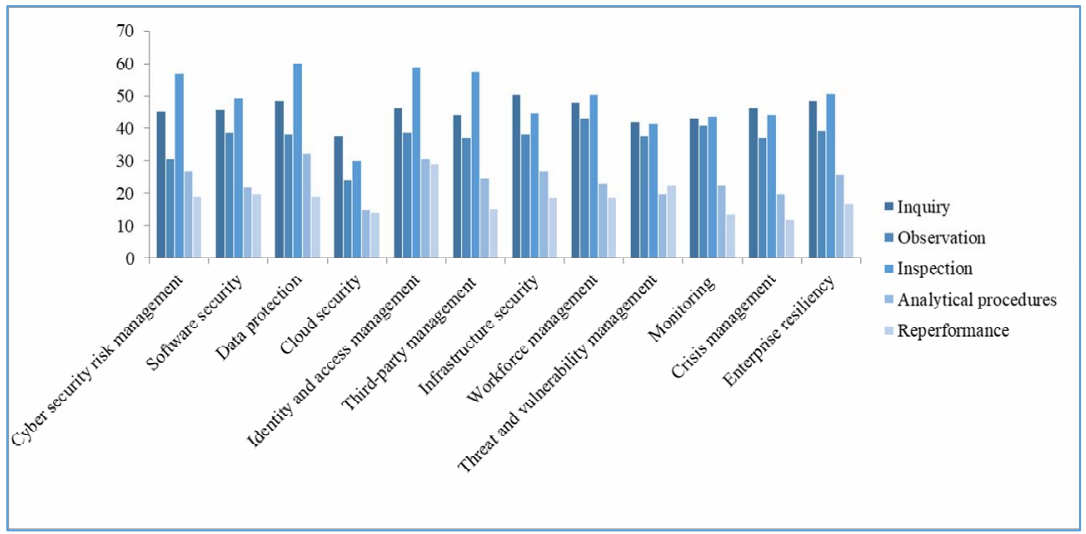
Performing CS assurance – number of procedures (n=183)



Audit procedures used

The International Standard on Auditing (ISA) identify a range of procedures for collecting evidence (ISA 500): **inquiry, observation, inspection, analytical procedures, reperformance.** Some procedures may not be sufficiently reliable to be used on a stand-alone basis for an effective CS audit. For instance, if the IAF collects the evidence by only interviewing the first and the second line roles (i.e. by inquiry), that might be efficient, but less effective as reperformance of controls. Sufficient evidence is normally collected by a combination of different methods to suffice the quality of evidence by the Standards.

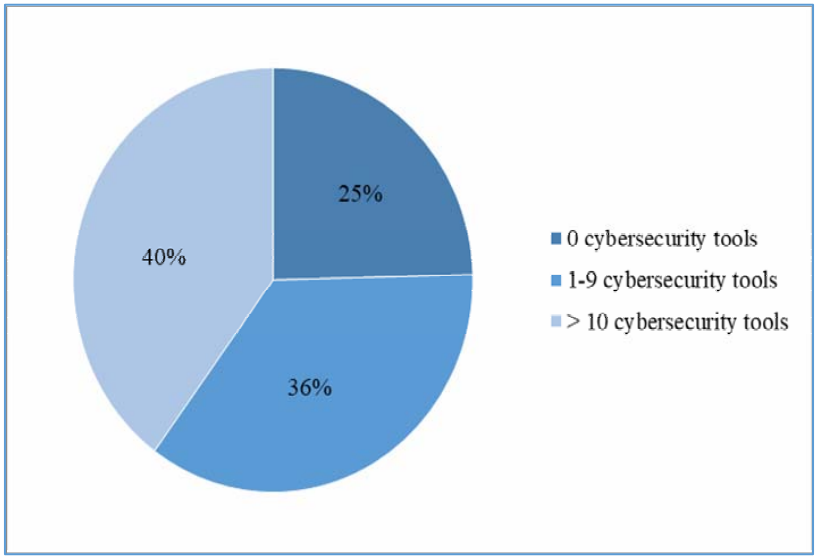
Performing CS assurance – type of procedures (n=183)



Inspection is the most frequently used procedure, followed by inquiry and observation, while analytical procedures and reperformance are not frequently used.

Cyber security tools checked

Number of cyber security tools checked (n=183)

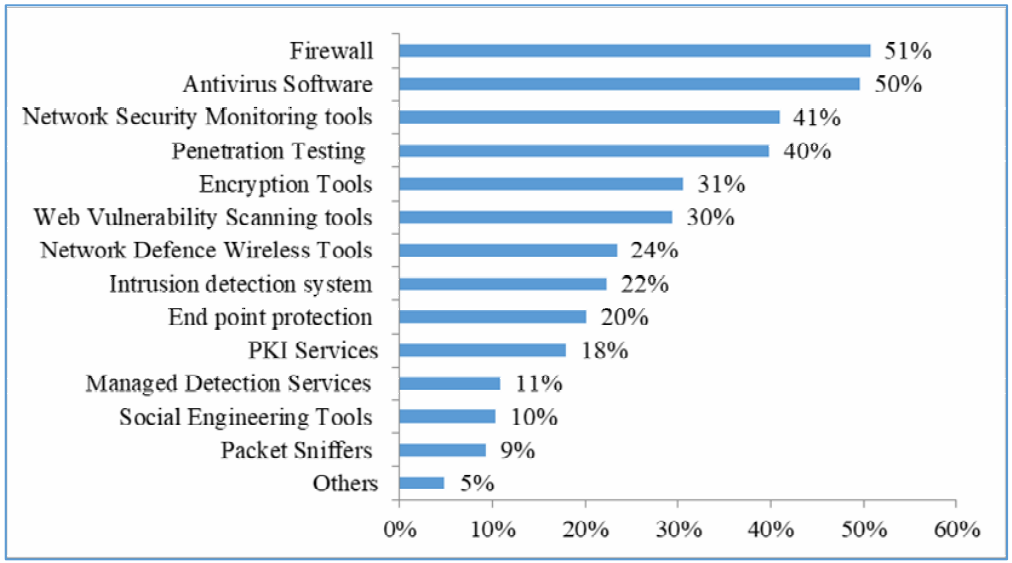


Internal audit function should **check the usage and effectiveness of cyber security tools** used by the second line.

Twenty-five percent (25%) participants indicated that they do not check any cyber security tool, while 75% of the participants check one or more cyber security tools in an audit cycle.

The largest number of respondents check the usage and effectiveness of **firewalls, antivirus software, network security monitoring tools and penetration tests.**

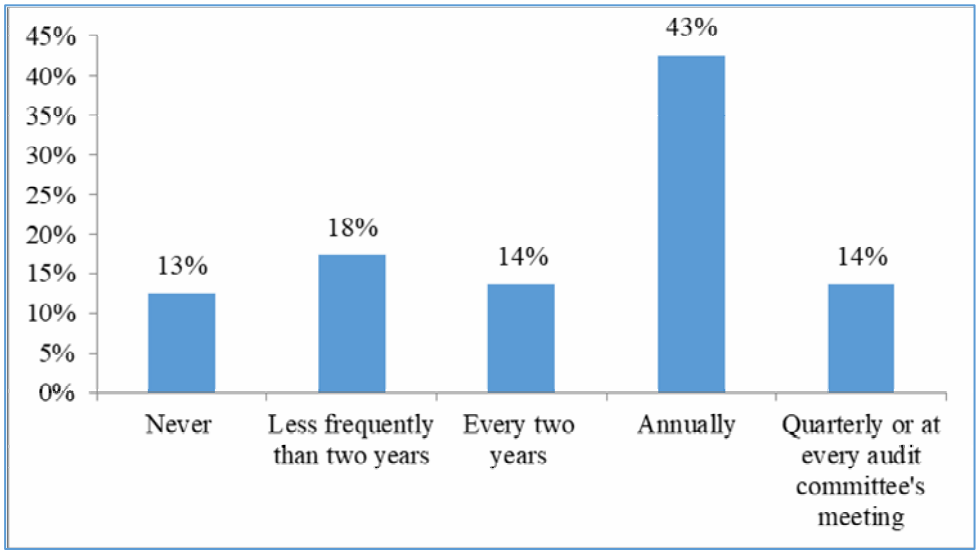
Type of cyber security tools checked (n=183)



Reporting about the effectiveness of CS risk management

Frequency of the IAF communication

Reporting to the Board (n=183)

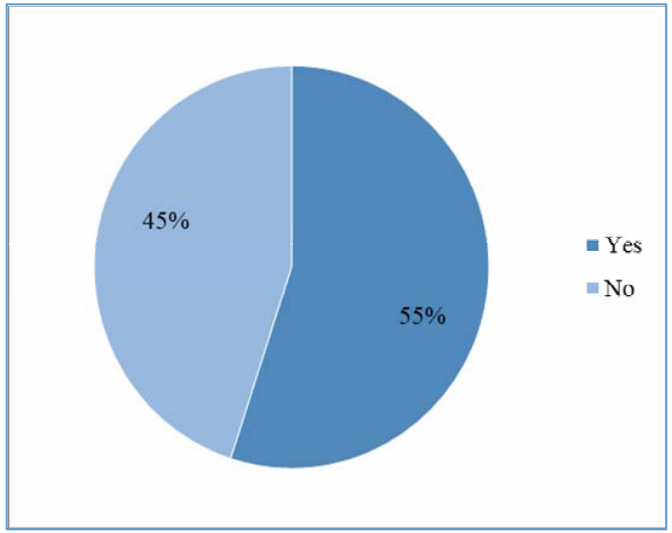


The most important part of comprehensive cyber security assurance is to **provide an independent report that cyber security risk management strategy, policies, procedures and controls are comprehensive and in line with organisation's risk appetite to the Board.**

Forty three percent (42%) of the IAFs report to the Board annually and 14% report quarterly or on every audit committee's meeting. **Thirteen (13 %)** do not report on cyber security risk management at all.

Independent and comprehensive opinion to the Board

Overall opinion to the Board (n=183)



Reporting on the comprehensiveness of cyber security risk management to the Board is especially **challenging because of technical terminology**.

The report to the Board should be accurate, objective, constructive, complete and timely (Standard 2420 – Quality of Communications).

Fifty-five (55%) internal audit functions issue an independent and comprehensive opinion to the Board.

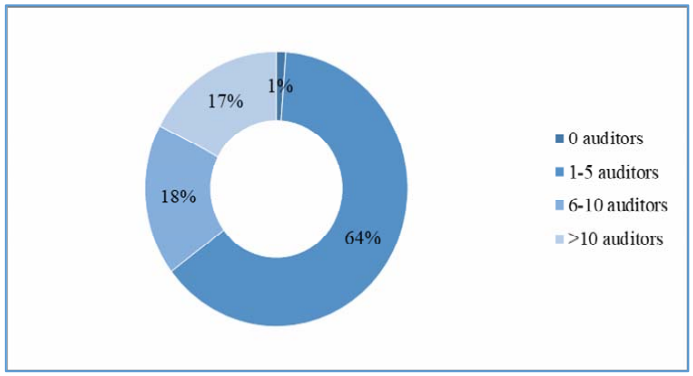
However, some IAFs issue such a report despite not performing the planning and the performing phases of CS assurence comprehensively and effectively. The correlation between the planning and the performing phase is weak.

This indicates that the **overall opinion regarding CS risk management is not as strongly related to the preceding phases of the assurance process as one would expect it to be**.

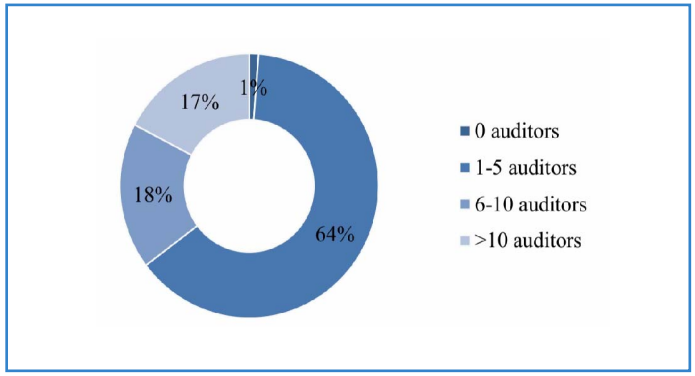
Resources for cyber security assurance

Internal & IT auditors activities

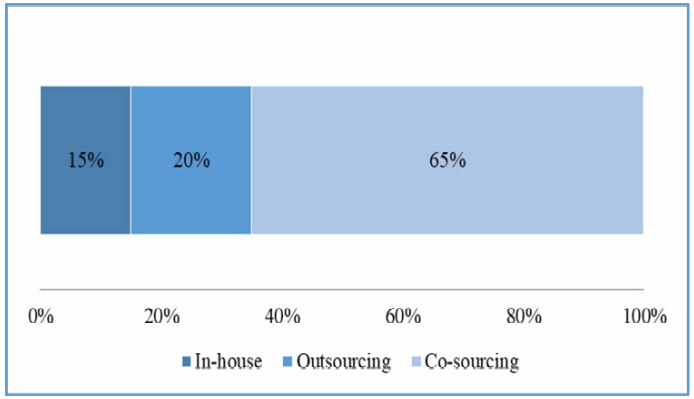
Size of the internal audit department (n=173)



Number of IT auditors (n=173)



Cyber security audit outsourced (n=133)



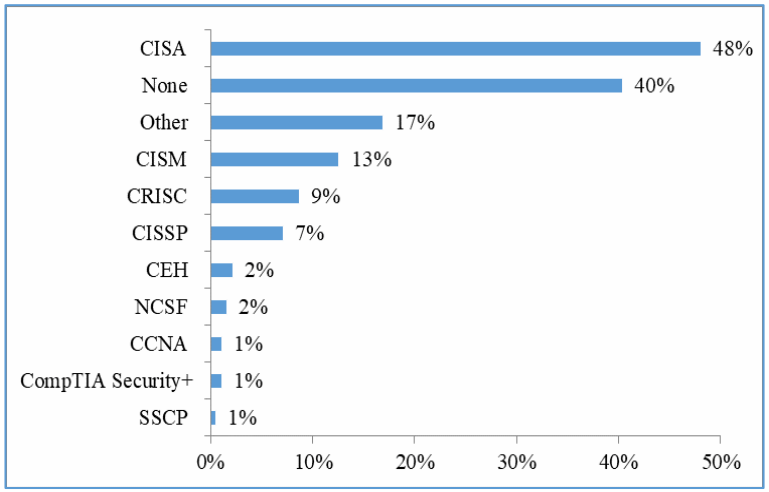
Our research confirms findings of previous research that **competencies** of a large proportion of internal auditors in the area of CS are still lacking.

Forty one (41%) of the IAFs have no auditors with professional certification related to CS, 31% of auditors have no experience in working in the CS area, and 41% have no IT Auditors.

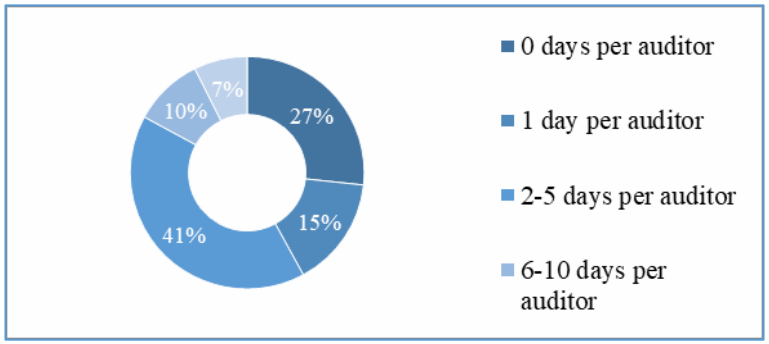
Because of lack of in-house skills, **20% of participants use outsourcing** and 65% use cosourcing as a method to perform CS assurance.

Certifications, CS training & budget for cyber security

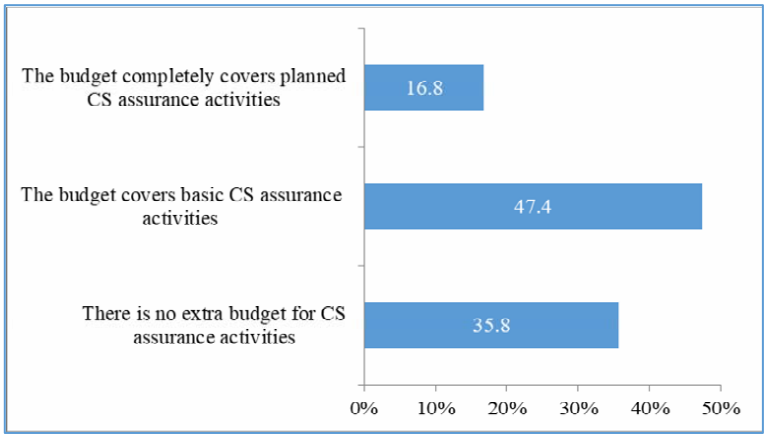
Certifications



Cyber security training (n=176) (number of full days per auditor)

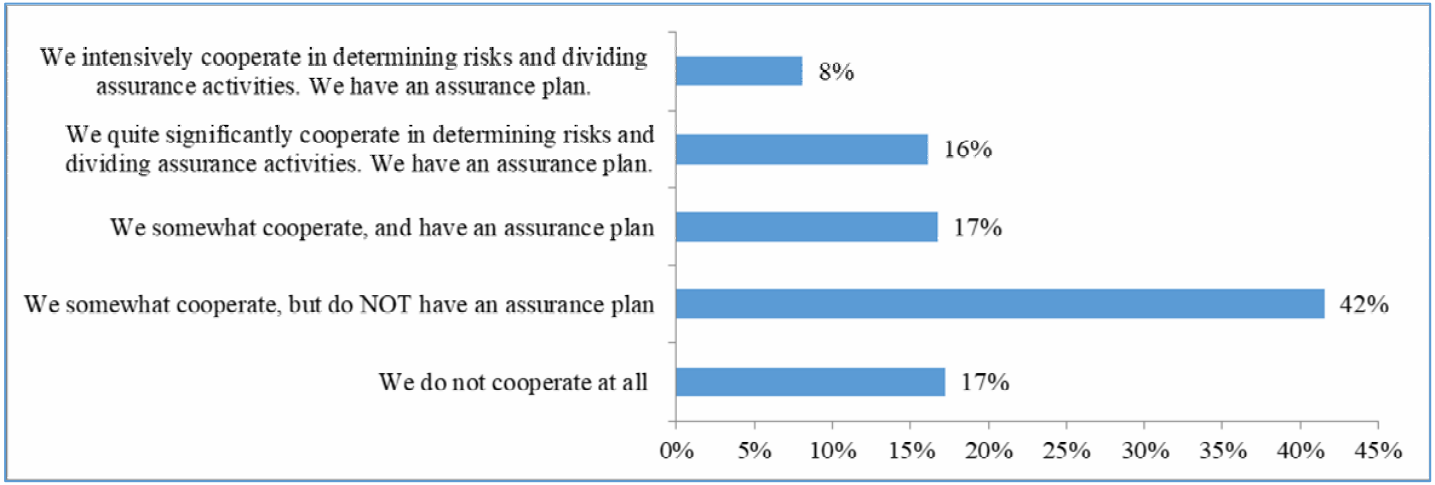


Evaluate the budget for CS assurance activities (acquisition of tools, software, training, services, consulting etc.) (n=173)



Cooperation with the 1st and 2nd line

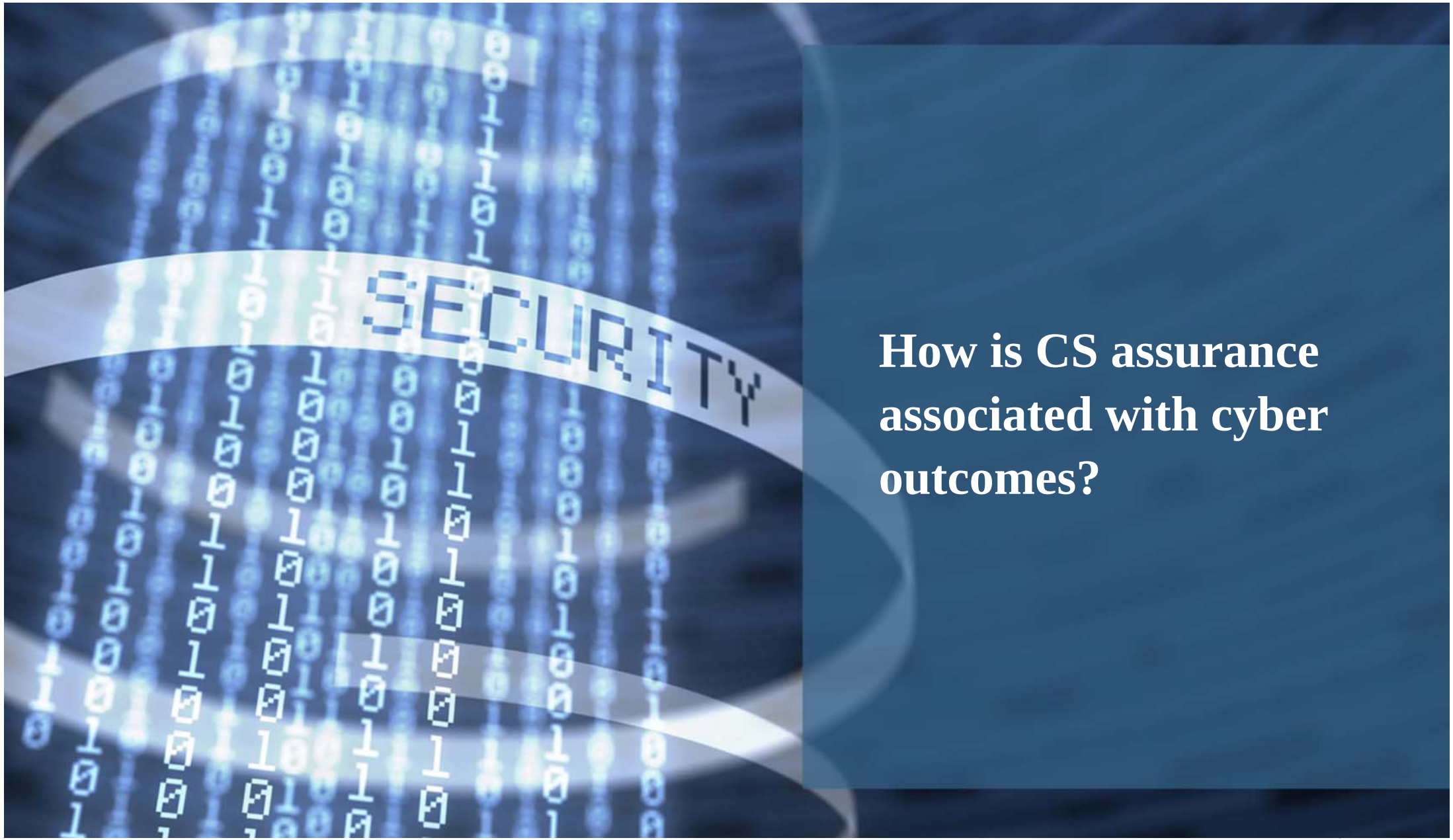
Cooperation with the 1st and 2nd line as per the assurance map (n=173)



Effective cyber security assurance is provided in collaboration with the first two lines.

Only 8% of respondents intensively cooperate with the first and second line in determining risks and dividing assurance activities. Forty-two percent (42%) respondents do not have an assurance plan, and 17% of them do not cooperate at all with first and second line of defence.

Assurance map is a collaboration and coordination plan between different assurance providers (third line internal audit, and second line e.g. compliance, information security etc.) to tackle the organisation's risks without duplication and as efficiently as possible.

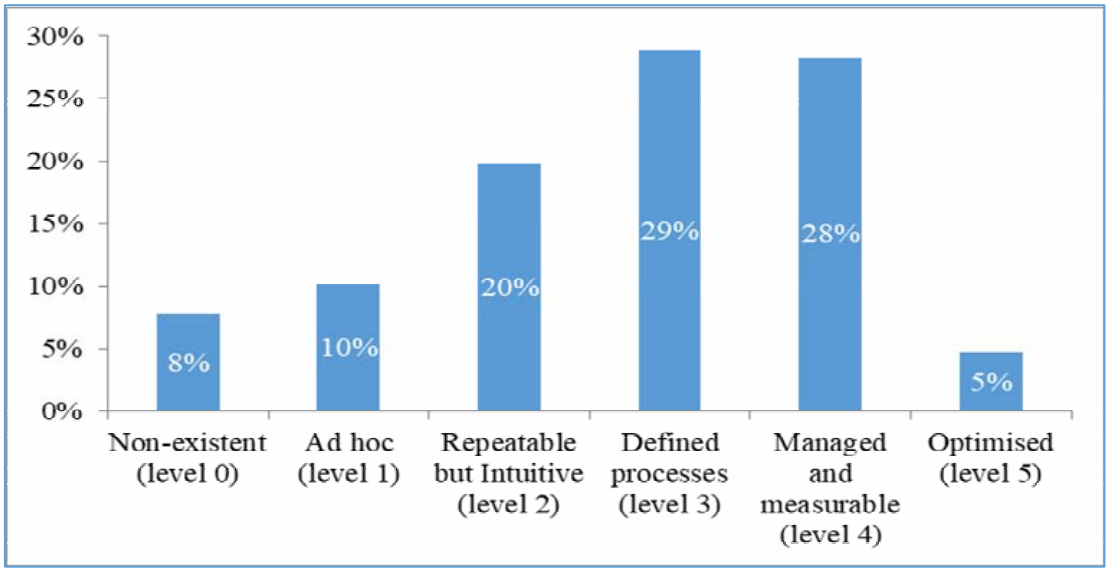


How is CS assurance associated with cyber outcomes?

Association between CSA Index and Maturity level of CS risk management

One of the limitations of a process measure of internal audit effectiveness is that such a measure is based on the premise that the internal audit is effective if procedures are carried out properly, regardless of the needs of stakeholders. However, proper evidence that a process measure indeed measures effectiveness of CS assurance would be if it is positively associated with the requests of stakeholders and related to corporate outcomes. The most important need of stakeholders (in our case, the Board) is to understand how the company's CS processes compare to good practices and compliance to frameworks. This is gauged by CS risk management maturity.

Evaluate the maturity level of cyber security risk management (n=166)



Maturity models are used as an instrument to measure how systematically organizations carry out their CS risk management. We measured it **based on the COBIT4.1 description of process maturity.**

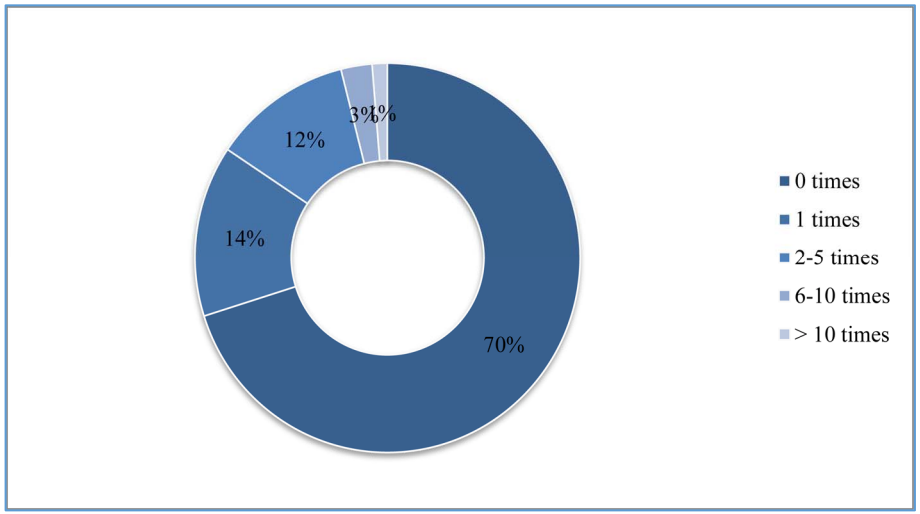
The majority of the organizations have **Defined (29%) and Managed (28%) level of cyber security risk management maturity**, while extremes like Nonexistent (8%) and Optimized (5%) are rather infrequent.

Our results show that the CSA Index has a significant positive effect on CS maturity. On average organization with a CSA Index of 80 is 5 times more likely to have a High maturity level than an average organization with a CSA Index of 20.

Association between CSA Index and CS incidents

Despite acknowledging that CS assurance is not the only line, effective CS assurance should contribute to higher effectiveness of the first two lines and increase the probability that cyber risk and controls are being effectively managed, and, ultimately, decrease the probability of cyber attacks.

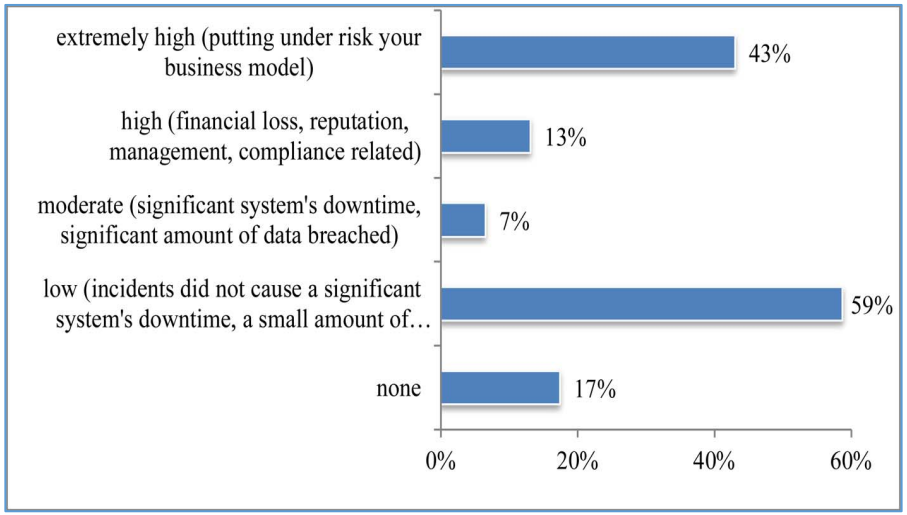
Cyber security incidents (n=150)



70% organizations did not have any successful cyber security attack.

Our results show that the CSA Index has no positive effect on CS incidents.

Cyber security consequences (n=45)



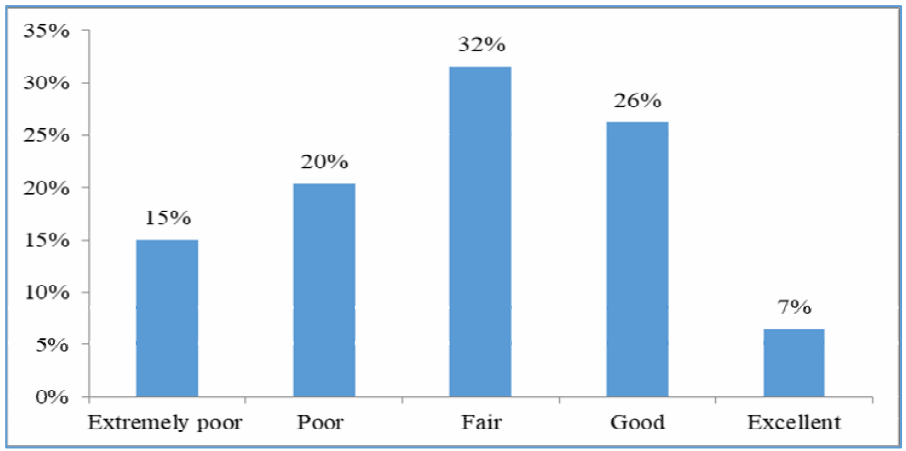
45 organizations reported successful attacks in the last year. The consequences for these 45 organizations were in the majority of cases (59%) estimated as being of **low magnitude** (incidents did not cause any significant system downtime with only a small amount of data breached).

There were **only 8 organizations for which respondents reported high or extremely high effect of the cyber security attack.**

Governance of cyber security assurance

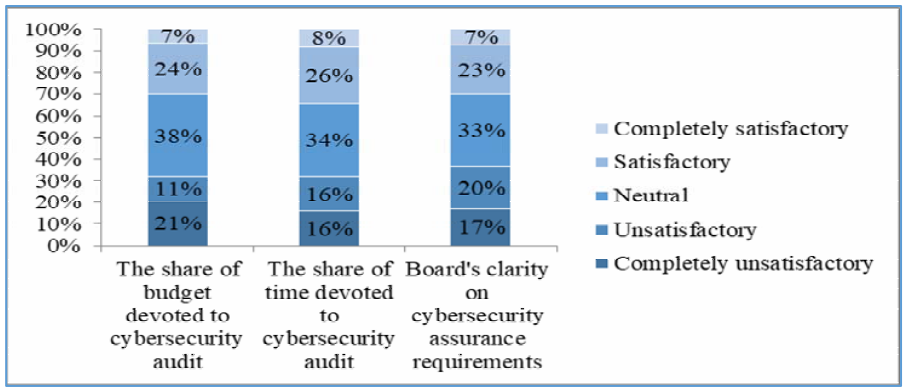
Board support to the IAF

Board's support provides to cyber security internal audit (n=166)



Thirty-five (35%) of participants evaluate the level of support that the Board provides to internal audit function in relation to cyber security audit as **poor and extremely poor.**

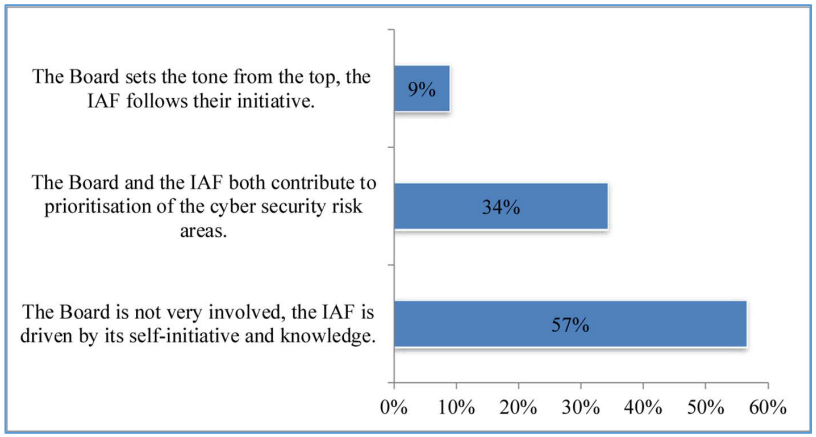
Board's support to cyber security assurance (n=166)



The share of the budget devoted to CS audit, the share of time devoted to CS audit and Board's clarity on CS assurance requirements has been evaluated mostly as neutral with high share of **unsatisfactory or compeletely unsatisfactory responses.**

Recipients of the IAF's CS assurance report

Mandate from the Board to CS audit (n=166)

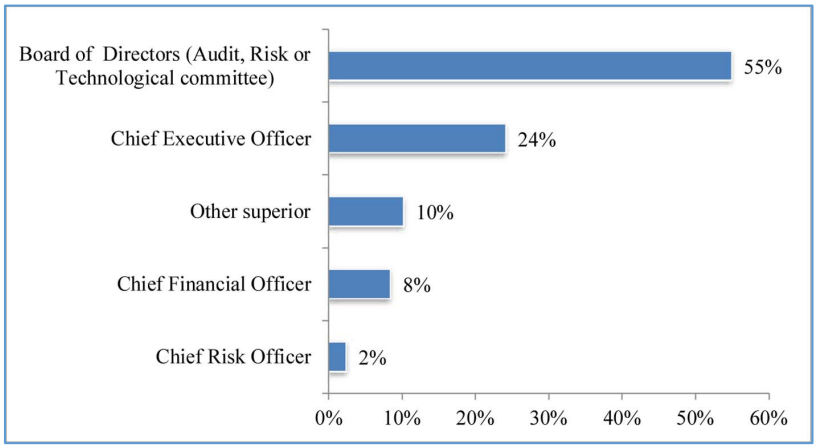


The involvement of the Boards in assurance of CS is very low, as only 9% of the boards set the tone from the top, and as many as 57% of auditors are driven by self-initiative and knowledge.

Ony 55% of the IAFs report directly to the Board.

20% of IAFs report to the level even below CEOs, normally to CFO or CRO.

CAE functionally reporting (n=166)



Authors

Marko Čular, PhD

University of Split,

Faculty of Economics, Business and Tourism

mcular@efst.hr

Sergeja Slapničar, PhD

University of Queensland,

Business School

s.slapnicar@uq.edu.au

Matej Drašček, PhD, CIA, CRMA, CFSA

President of IIA Slovenia

matej.drascek@gmail.com

Tina Vuko, PhD

University of Split,

Faculty of Economics, Business and Tourism

tina.vuko@efst.hr

Find your score on how effective cyber security assurance is in your organisation!

If you agree to participate to find your Cyber Security Assurance Index, please click this link:

Cyber Security Assurance Index

Images: Shutterstock

How effective is internal auditors' cyber security assurance?
Self-published (Online Brochure)
Designed by: Prensa Ltd