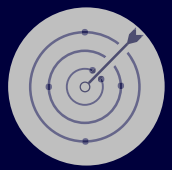
O.R.X

Cyber & information security risk controls and indicators study

Summary report: February 2020

Material risks in focus



Topics covered:

Cyber

Information security

This survey and report is part of our cyber and information security risk (CISR) programme.

We've been working with a group of cyber risk management experts from our member firms to support them in overcoming the challenges they face with cyber and information security risk management. The programme has focused on two key challenges – helping firms understand their risk exposure and enhancing approaches to managing this risk.

After the success of our year-long project, we are developing this initiative into a full service. The service will help cyber risk experts in the second line manage this complex and constantly evolving risk.

Find out more at www.orx.org

Connect with ORX

@ORX_Association

@ORX_association

The ORX cyber & information security programme so far...

Since the start of 2019 we've worked with a group of cyber risk management experts to see how we can best support institutions in their cyber and information security risk management activities.

Defining cyber and information security risk

To improve the management of cyber and information security risk we first need to speak the same language. If we don't have a common understanding of what is or isn't cyber or information security risk, then we will never be able to successfully share data, information and ideas.

This is why one of the first actions for our cyber group was to produce the definitions that underpin all our work in this area.

Download the definitions

How can you best distribute roles and responsibilities?

A follow up to our work on the definitions, our survey on roles and responsibilities established where cyber risk management responsibilities best sit across the three lines of defence, and identified those areas where there is confusion. Working with the group, we developed a model that could reduce confusion and add clarity.

Download the report and distribution model

About this study

Participants in ORX's cyber and information security risk (CISR) management programme identified controls and indicators as a major area of interest and challenge.

To support them in this challenge, we surveyed 22 institutions on the key controls, indicators and external control standards supporting their cyber and information security management activities. This work will enable them to carry out peer comparison and provides industry insight.

The survey was designed in collaboration with our cyber and information security risk working group, and was conducted through our secure Insight platform, allowing participants to securely and anonymously share the cyber controls and indicators they have in place. To ensure consistency in the responses, we aligned our survey with the NIST framework's suite of 98 controls, and asked participants to share other controls and frameworks they use at a control objective level. Participants also provided 120 of their key risk indicators (KRIs).

In addition to the survey, we hosted a number of webinars, bringing together 45 individuals from more than 40 financial organisations. These webinars provided a platform for cyber specialists to share their thoughts on the findings of our survey. The insights provided additional colour and context given in this report.

Despite significant investment, participants are still reporting that controls and indicators are not delivering the expected value and that further improvement is required. ORX is supporting institutions in the ongoing development of cyber controls and indicators by collating a library of controls and indicators for reference and comparison.

Key findings from the survey & subsequent webinar discussions

1. Institutions reference multiple industry control frameworks – often resulting in the use of hybrid frameworks with a high number of controls
2. Controls and indicators differ in levels of maturity
3. Controls and indicators are largely manually operated and monitored, and mostly backward-looking
4. Institutions often lack expertise and good data to support robust and objective CISR management

A library of cyber controls & indicators

Using the information provided by the survey participants, we've created a library of key controls and indicators.

Improve your controls

The library will allow you to compare and benchmark your controls and indicators, and to see the top controls and indicators for major risks. This information will help you gain a better understanding of the overall efficiency of your controls and indicators.

Free for ORX members

The library is freely available to any institution who is a member of ORX. All you need to do to access it is provide information about your controls and indicators. You'll then receive your individual copy of the library which you can use for benchmarking, comparison and analysis.

To find out more, contact:
melanie.lavallin@orx.org

Controls factsheet

Topline survey results

Cyber controls are mostly mature:

63% of participants rate their maturity at the highest level. (See page 5 for definitions of maturity levels).

Participants operate large numbers of controls:

There was a median of 51-100 controls per participant across multiple areas managing CISR.

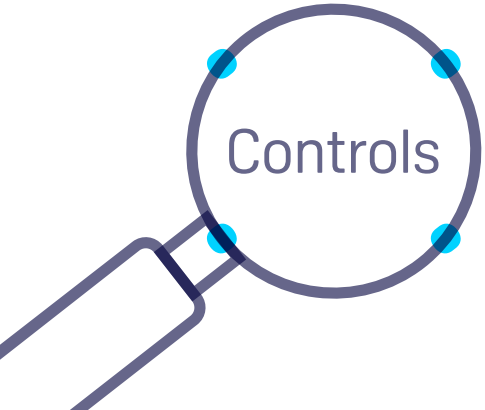
1st line is hands on:

58% of participants report controls developed by the 1st line, lacking 2nd line input.

Control improvements are a priority:

47% of participating firms plan to change their control environment, most others are planning incremental improvement. Changes include:

- Alignment with best practices
- Transferring responsibilities to different lines of defence
- Automation



What makes a cyber control effective?

We asked participants what factors made their controls effective. Here's what they told us:

Centralisation – e.g. control repository or reporting

Consistent documentation

Consistent implementation, including complexity of legacy systems

Automation

Training, including of senior execs

Focused on most material areas of concern

Indicators factsheet

Topline survey results

Indicators are less mature:

Participants generally rated indicators as having lower levels of maturity compared with controls.

Fewer indicators are implemented:

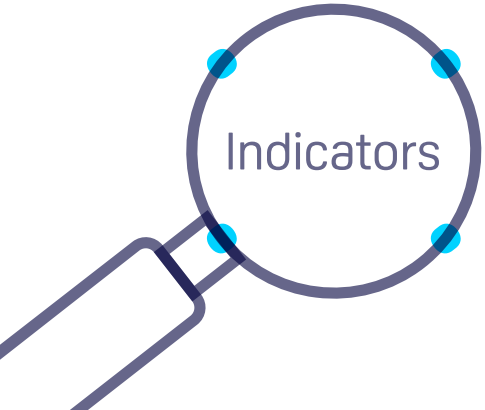
There was a median of 25-50 indicators per organisation across multiple risks.

Indicators are mostly reported to op risk committee:

49% of participants report indicators to the operational risk committee, 25% to the CIO/CISO, 15% to the board risk committee and 12% to the cyber risk committee.

Most indicators are monitored monthly:

78% of indicators are monitored monthly, and 71% are lagging.



What makes a cyber indicator effective?

We asked participants what factors made their indicators effective. Here's what they told us:

- Allow **judgement** and **flexibility** in reporting
- Enable a **targeted response**
- Easy to **measure**
- Easy to **influence** (sensitive to changes)
- Ensure **accountability**
- Have **appropriate scope**
- Are **risk based**

1. Institutions reference multiple industry control frameworks – often resulting in the use of hybrid frameworks with a high number of controls

Survey findings

Survey participants reported aligning their controls with a range of industry frameworks (figure 1). Almost 75% of participants reported aligning their controls with the NIST framework, and felt that the control areas it covered aligned with industry standard control types (figure 2).

80% reported referencing multiple frameworks in operation, on average four, and customising a hybrid to meet their own specific requirements. This often results in institutions operating and managing a high volume of controls, not always focused on the most material areas.

Webinar discussions

These findings were confirmed by our subsequent webinar discussions, where participants stated that, while many external frameworks are available for reference, no single industry control framework is sufficient to meet their needs. Participants felt that different frameworks provided different benefits, and discussed the NIST framework being useful to identify key controls, and the MITRE ATT&CK framework being useful to provide more granular detail to provide comparison and analysis of threat intelligence.

On the other hand, some felt the NIST framework's suite of 98 controls was too in-depth and provided too many controls, making it difficult to focus on and improve the most material controls.

Figure 1: Percentage of participants using the framework

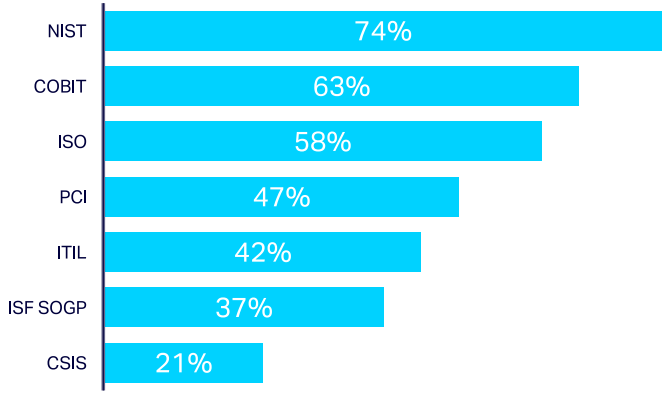


Figure 2: NIST controls areas aligned to control types

NIST control area	Main control type
Identify	Detective/Preventative
Protect	Preventative
Detect	Detective
Respond	Corrective
Recover	Corrective

Conclusion

The findings of our survey and webinar discussions indicate that industry control frameworks alone are not adequate references for institutions to build control frameworks to effectively manage CISR. Institutions therefore recognise the need to further streamline their control environments and the need for a change in mindset to establish effective controls and indicators for CISR management. One participant suggested that to avoid the confusion caused by multiple external frameworks, institutions should focus first on the key risks that could really harm an organisation, before identifying the most material controls. They also identified the need to focus on the most relevant and material controls to assess effectiveness in addition to coverage, rather than considering the two in isolation.

2. Controls and indicators differ in levels of maturity

Survey findings

According to our survey, many participants perceive their controls as more mature than their indicators. 63% of participants rate the maturity of their cyber controls at level 3 (with controls, accountability and ownership in place, embedded within the business, proactively supporting risk management decisions, and continuously reviewed and improved). Conversely, participants rate their indicators as less mature, with 32% reporting them as level 1 (with business unit indicators in place, but lacking a link to risk management and assessment), and 42% as level 2 (with defined and approved indicators in place and assessed aligned with industry standards).

Webinar discussions

Subsequent discussions with participants focused on why controls may be considered more mature than indicators. They felt that while industry control frameworks can provide external examples, guidance and additional detail to support the development of controls, there are fewer industry standards to support institutions setting indicators and thresholds. Additionally, participants felt that indicators should be developed based on more in-depth analysis of their own threats and experiences to understand what should be monitored to prevent cyber events from occurring. As this information is more difficult to obtain, defining the drivers of risks to develop causal indicators and support mitigation can be a challenge. Additionally, participants reference the fact that indicators need to be more dynamic in nature and evolve as threats and exposures change.

Figure 3: How participants rate the maturity of their controls

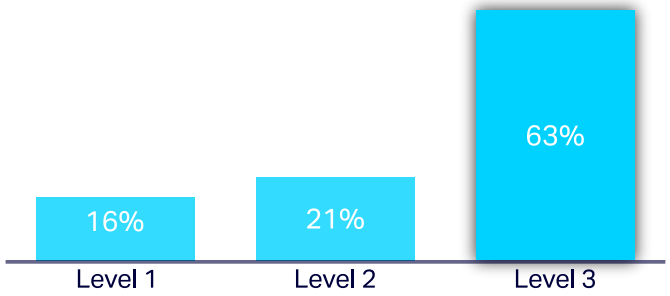
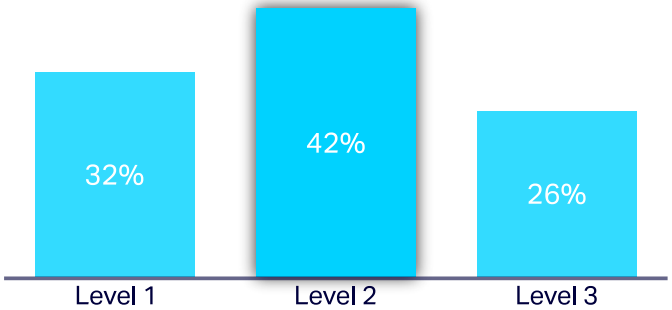


Figure 4: How participants rate the maturity of their indicators



Conclusion

From our survey, it is clear that the lack of external references poses a significant obstacle to the development of mature indicators and appropriate thresholds. Their development will likely be a gradual process, with thresholds being set initially before being monitored and adjusted over time as institutions gain experience in managing cyber and information security risk.

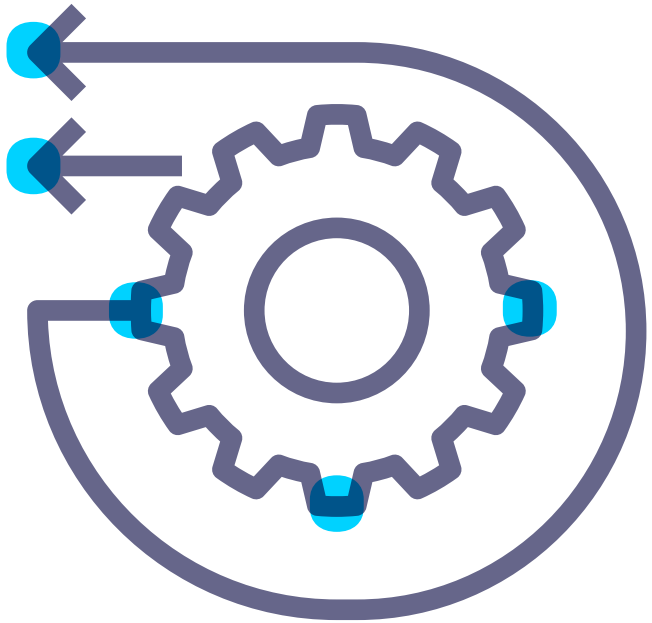
By providing guidance and allowing firms to benchmark against their peers, ORX's control and indicators library may be the external reference point the industry needs.

3. Controls and indicators are largely manually operated and monitored, and mostly backward-looking

Survey findings

Our survey found that participants largely rely on manual processes to operate both their controls and indicators. 94% of controls are not automated by the majority of participants, and many of the processes monitoring controls are also manually operated. This is also seen with regards to indicators, with participants reporting that 61% of indicators are manually operated.

Participants also reported that 71% of their indicators were lagging, in that they were backward-looking or detective. While lagging indicators can be useful for trend analysis or loss reporting, they are less useful for risk mitigation. Another challenge is that they do not incorporate data or information relating to issues which have gone undetected by controls.



Webinar discussions

Participants in our webinar stated that operating manual controls and indicators can present a number of challenges, in that they may be too resource heavy to operate or monitor frequently and effectively. They also felt that while there was a desire to have more effective indicators, the data required to drive them was often not available. Comments were made that the cost of manual operation is often not known, so it is difficult to be able to assess the benefit and return on investment.

Conclusion

The results of our survey and subsequent webinars show that institutions recognise the automation of controls and indicators as being key to operating an effective cyber and information security risk framework. Almost half of survey respondents reported that they plan to change their control environment, with the automation of controls and information flow to indicators among their key priorities. Participants also reported a move towards quantitative measures, and that they are looking to apply weightings to their indicators. However, this requires a level of maturity which many institutions have not yet established.

In order to increase maturity and improve the effectiveness of indicator suites, institutions may need to move towards implementing more real-time, forward-looking indicators.

4. Institutions often lack expertise and good data to support robust and objective cyber and information security risk management

Survey findings

A lack of quality data and relevant expertise is an obstacle to the development of effective controls and indicators, according to the results of the survey. Participants reported that their indicators rely on information that is not easily available, accurate, robust, or of consistent quality. This can be due to factors such as the assumption that data provided by business assessments and third parties is accurate. Because of this, 59% of participants reported setting their thresholds using expert judgement.

Additionally, participants felt that data returned by indicators can be misleading or give a false sense of security or danger when viewed in isolation. For instance, indicators measuring events that happen infrequently can return a value of 0, and should therefore be considered with additional context. Another challenge is ambiguity when thresholds are breached, uncertainty about whether an event meets pre-defined criteria, and what action, if any, to take.

Webinar discussions

During our webinars, some participants expressed that the lack of cyber expertise within operational risk management activities caused further challenges, and some reported that roles and responsibilities for setting and owning controls and indicators were not clear. Furthermore, due to a lack of relevant expertise, institutions felt that while they were operating large numbers of controls, the link between the control and the risk is not always clear.

Conclusion

The lack of expertise in cyber and information security risk management has led to a shift in roles and responsibilities, with 58% of survey participants reporting that their controls are typically developed by the 1st line of defence. Participants discussed an additional reliance on support from security teams, who sit in the 1st line of defence, while it was expected that the 2nd line should be responsible for setting frameworks and standards.

Participants suggested that setting and developing controls and indicators should become a collaborative effort between the 1st and 2nd lines of defence. And, that the placement of ownership for control operation should be with the 1st line to allow for independence and challenge from the 2nd line.

These findings reflect those of our previous study concerning roles and responsibilities in cyber and information security risk management. Among other findings, our survey identified that the roles and responsibilities remain ambiguous, and that many institutions have implemented a 1.5 line of defence to account for a lack of cyber expertise in the 2nd line, which has led to confusion.

To learn more about our survey and its findings, please visit:
managingrisktogether.orx.org/cyber-risk-programme/roles-and-responsibilities

Cyber controls & indicators library

To support good practice in cyber and information security risk management, ORX has created a library of controls and indicators based on responses to our survey. The library will allow institutions to compare and benchmark their controls and indicators against those of their peers, and to gain a deeper insight into industry practice.

We collated a range of control and indicator attributes submitted by participants in our survey, including:

- How frequently they are used
- Whether they are automated
- What primary risks they manage
- Whether indicators are leading or lagging
- Whether they are dependent on a third party
- An assessment of maturity

The library will be made available to firms that provide information about their own controls and indicators. We will align the library to the level 2 risks identified in the **ORX Reference Taxonomy 2019**. The library will be launched in Q2 2020.

Appendix

About ORX's Insight system

Insight is a system that was developed by ORX for the anonymous and secure collection, exchange, storage and distribution of loss data and survey responses deemed to be highly confidential. Insight is protected by leading-edge security measures and is hosted on a secure platform across two data centres.

Industry standard frameworks

The industry control frameworks referenced within this report can be found here:

- NIST
- MITRE ATT&CK
- COBIT
- ISO
- PCI
- ITIL
- ISF SOGP
- CSIS

How to get access to the ORX controls & indicators library

The library is available to all ORX members – all you need to be able to use it is share equivalent information about your own controls and indicators.

To find out more, contact **melanie.lavallin@orx.org**

Shining a light on cyber risk management

O.R.X

Don't get left in the dark. Join the new service from ORX to help you manage cyber and information security risk.

- Share cyber risk data
- Take part in industry-leading research studies
- Improve your understanding of cyber risks
- Learn from other experts and peers
- Open to members and non-members of ORX

Be part of a global community advancing the management of cyber risk

Contact **roland.kennett@orx.org** to find out more

ORX CISR Programme:
Roles and responsibilities

Managing risk together

ORX believes many heads are better than one. We're here to bring the best minds of the international operational risk community together.

By pooling our resources, sharing ideas, information and experiences, we can learn how best to manage, understand and measure operational risk and become less vulnerable to losses.

We work closely with over 90 member firms to develop a deeper understanding of the discipline and practical tools. We set the agenda, maintain industry standards, and garner fresh insights.

ORX is owned and controlled on an equal basis by its members.

For more information about ORX, visit our website at **www.orx.org**

Contacts

Steve Bishop
Head of Risk Information and Insurance, ORX
steve.bishop@orx.org

Melanie Lavallin
Senior Research Manager, ORX
melanie.lavallin@orx.org

www.orx.org

@ORX_Association

@ORX_association