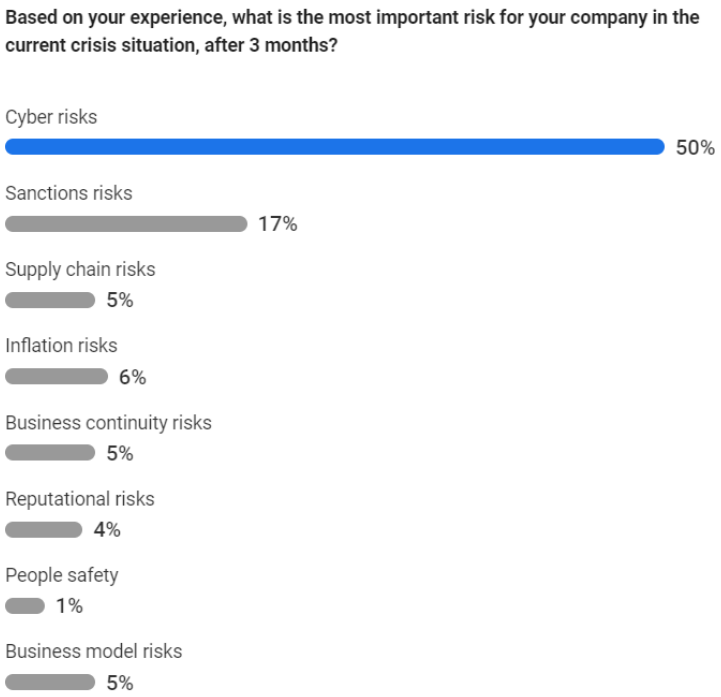
1.General Challenges

During crisis, IA must be part of the crisis management unit in order to be permanently informed about what is going on, to evaluate risks and make sure that the information submitted to the governing body is relevant and complete.

It also helps defining the need for specific audits: where and when ?

Consequently, IA must be agile, flexible, reactive and assist governing body in oversee the impact of crisis. This way, IA can add value to the organisations.

2. Poll



Avenue des Arts 41
1040 Brussels, Belgium
TR: 84917001473652
info@eciia.eu
ECIIA

3. Cyber risks

The current situation

- Crisis has helped to understand risks and likelihood due to political decisions (eg NATO discussions about some new members).
- Currently, the crisis has not materialised so far in big attacks, nothing with sustained impacts.
- There is nothing new but everything can change quickly and the pandemic has helped to prepare for extreme situations.
- Consequently, it is difficult to justify cyber investments until serious events happen…

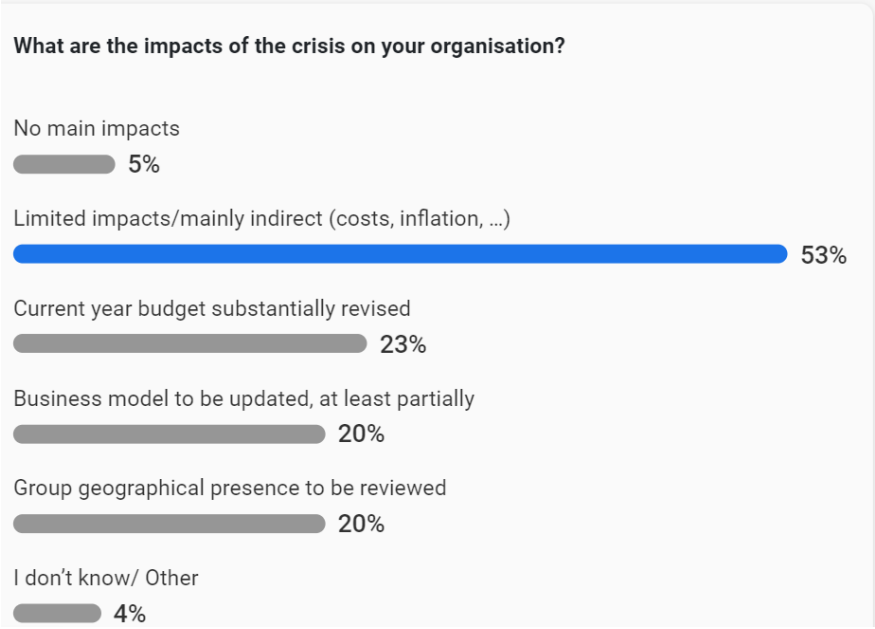
Recommendations

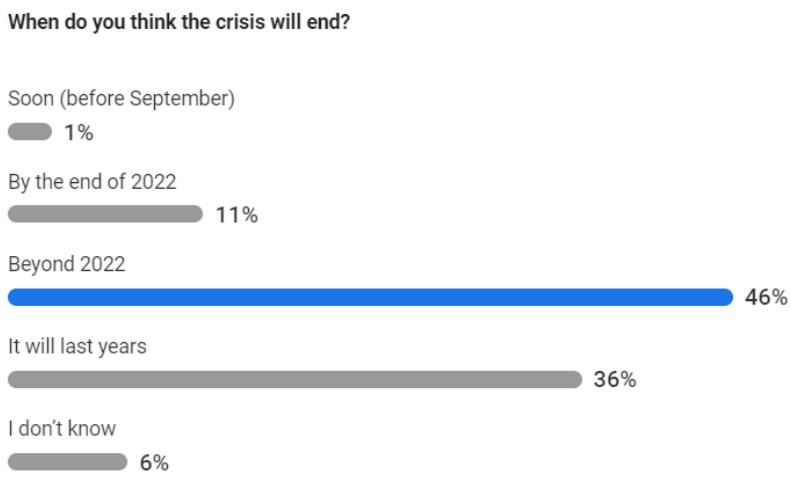
- Make sure you understand where important information is stored, how well it is protected and know how to connect (specially the links with countries in difficult political situations).
- Scan your system regularly : security of system and access rights are sensible, know your supply chain and their security system.
- Test cyber, test permanently : you can create a "hostile team" attacking your company, IA should cooperate in the exercise to assess the incidents 'responses.
- All the staff must be aware and know how to escalate: culture change is key.
- Open communication lines to all government agencies in both ways and also with peers organisations.

Evolution of cyber crimes

- Criminals never miss crises and they will try to leverage on the current crisis.
- There is something different with this crisis: governments are humping lot of money in cyber defence and attacks capabilities….and this might increase the criminals capabilities!
- Internal audit must help organisations to early identify cyber-attacks and the cooperation is key (with governments, other companies,…).

4. Polls





Avenue des Arts 41
1040 Brussels, Belgium
TR: 84917001473652
info@eciia.eu
ECIIA

5.Sanction risks

It is the second risk based on the evaluation above

It is important to assess the sanction implementation

- The implementation depends on the complexity and geography of the group (subsidiary in "crucial" location) and the type of platform managing ICT system (single or various).

It is important to notice that

- We have had 6 waves of sanctions since February (wide range): huge speed of changes.
- The forecast is that the sanctions will increase (types and impact).
- The reputational risk might be impacted (3 authorities: UK, US and European authorities (ECB)). ECB will assess the impact (thematic review or deep dive).
- The challenges for the customers to understand the sanctions.

The role of internal auditors

- IA should play the advisory role (assist the 2d line to make sure they set up adequate process to manage sanctions and the flow is correct and timing reported) and assurance role (independent assessment on sanctions management : framework, systems and processes (IT system), data feeding completeness and accuracy).
- New emerging risks not planned in the audit plan, so flexibility is required.

6.Business model risks

Main impacts on the business

- Micro level: global economy: short and long term effect on geopolitical landscape. In terms of risks, a lot can change in the long term (eg: ESG transition-EU grow less 1% in 2023 , inflation: + 1%..).
  Impact of Russian/Ukrainian products in the economy is not estimated yet (need for alternative suppliers).
- Macro: reshaping of the business model. A case by case approach is needed to take strategical decision about the direct exposure and tailor made solutions must be defined by each business. For the banks, it is useful to have a detailed geographical and sectorial view of the business (loans, investments,…) to evaluate the risks.

Role of internal auditors

- Internal audit must think they are "responsible" of the effectiveness of the IC system: be humble but well informed and discuss the effects of the crisis in details.
- For business risks, make sure new risks are identified, properly managed and reported timely to the regulator , booked in accounting in real time.
- Make sure the impacts on the business plan, strategy are assessed: if not done, other risks might appear

7. Conclusions

- Crisis is now business as usual….Flexibility is crucial for IA: change easily the annual audit plan; permanent risk assessment on the evolution of risks, be part of the crisis units….
- Role of IA: is key and good moment to demonstrate the added value, through our ADVISORY ROLE (in particular in favour of the TOP Management) as well as our ASSURANCE ROLE (in particular in favour of Governing Bodies and Regulators)
- Cooperation with other assurance providers (in particular, the other internal control function) is key: collaborate, share information, try not to overlap
- All risks indirectly impact the bank/company reputation!
- Main risks/impacts of the Russian/Ukrainen crisis expected from attendants (cyber and sanctions based on polls). It's clear to all of the us that the crisis impacts the whole organisation and all processes: lets' not forget any impact!
- Geopolitical Risks have impacts on business models….probably more severe than expected…. (eg: Inflation Risks)