Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Insurance Ireland CRO Forum

CBI IT & Cyber Questionnaire Findings

IT & Cybersecurity Risk

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

As the Insurance Industry continues their digital transformation this opens up additional risks and challenges.

Central Bank Focus

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Aim of Regulatory IT/Cyber risk initiatives:

- Raise standards of governance and management of IT risks
- Drive senior leadership engagement on IT & cybersecurity risks
- Increase firms' resilience to IT failures and cybersecurity incidents

2017 focus:

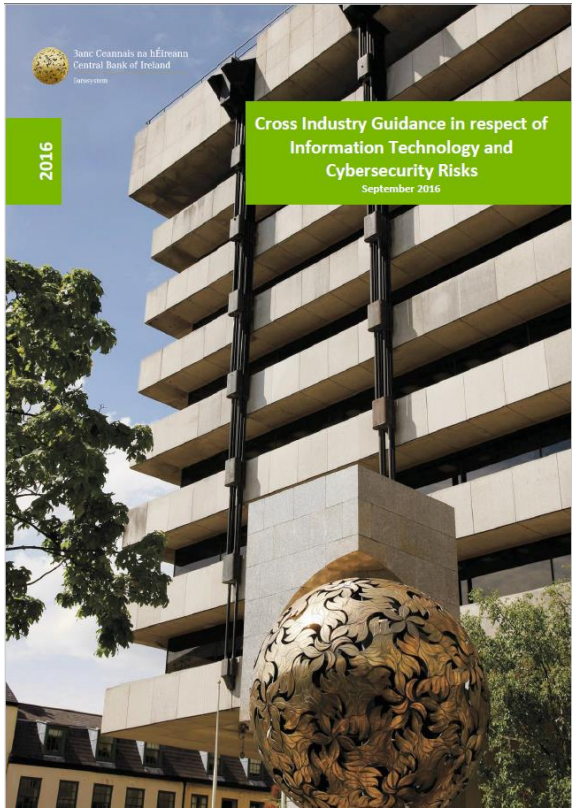
- The Auditor Assurance Framework for High Impact firms
- The ongoing supervisory dialogue with Medium High & Medium Low firms
- Encourage information sharing on IT & Cyber incidents with supervisors

Background to Questionnaire

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Introduction

- 47 questions spanning Governance, Risk Management, Cybersecurity and Outsourcing
- Based on the Cross Industry Guidance
- Findings based on 75 responses
- A, B or C responses



Governance - Key Considerations

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Governance - Sample Findings

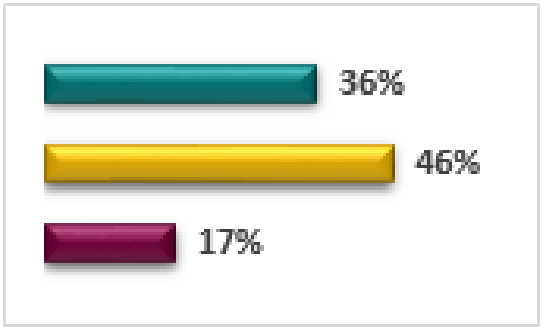
Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Q1. Does your undertaking have a Board approved IT & Cybersecurity strategy and framework?

Yes

No, but it is being submitted for approval within 6 months

No



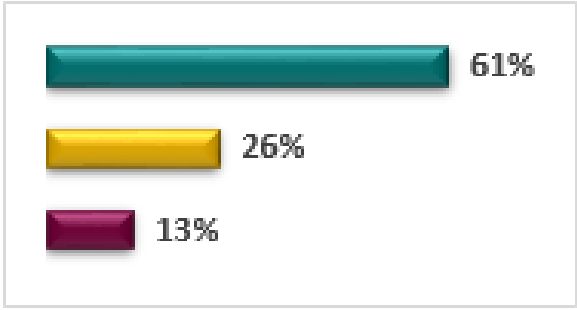
See **section 1.1.1** of the Cross Industry Guidance

Q5. Are developments of IT and Cybersecurity risks reported to the Board?

Yes, regular reporting of IT and Cyber risks

Yes, the Board receives updates on major IT projects

Limited reporting on IT issues



See **section 1.1.4** and **1.2.1** of the Cross Industry Guidance

Risk Management - Key Considerations

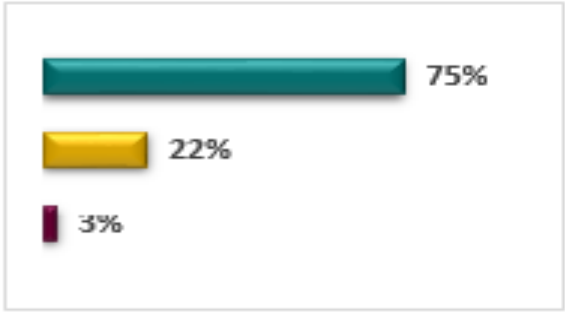
Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Risk Management - Sample Findings

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Q13. Does the undertaking have a process to identify your organisation's critical functions and processes?

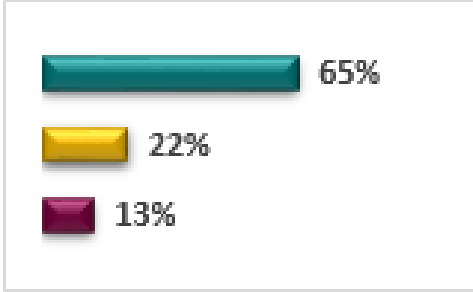
Yes, and this is annually verified	75%
Yes, this activity has been undertaken but it is not considered a routine, repeatable process	22%
No, but this will be in place within 6 months	3%



See **section 2.1.9** of the Cross Industry Guidance

Q14. Has all IT supporting the delivery of those critical functions and processes been identified?

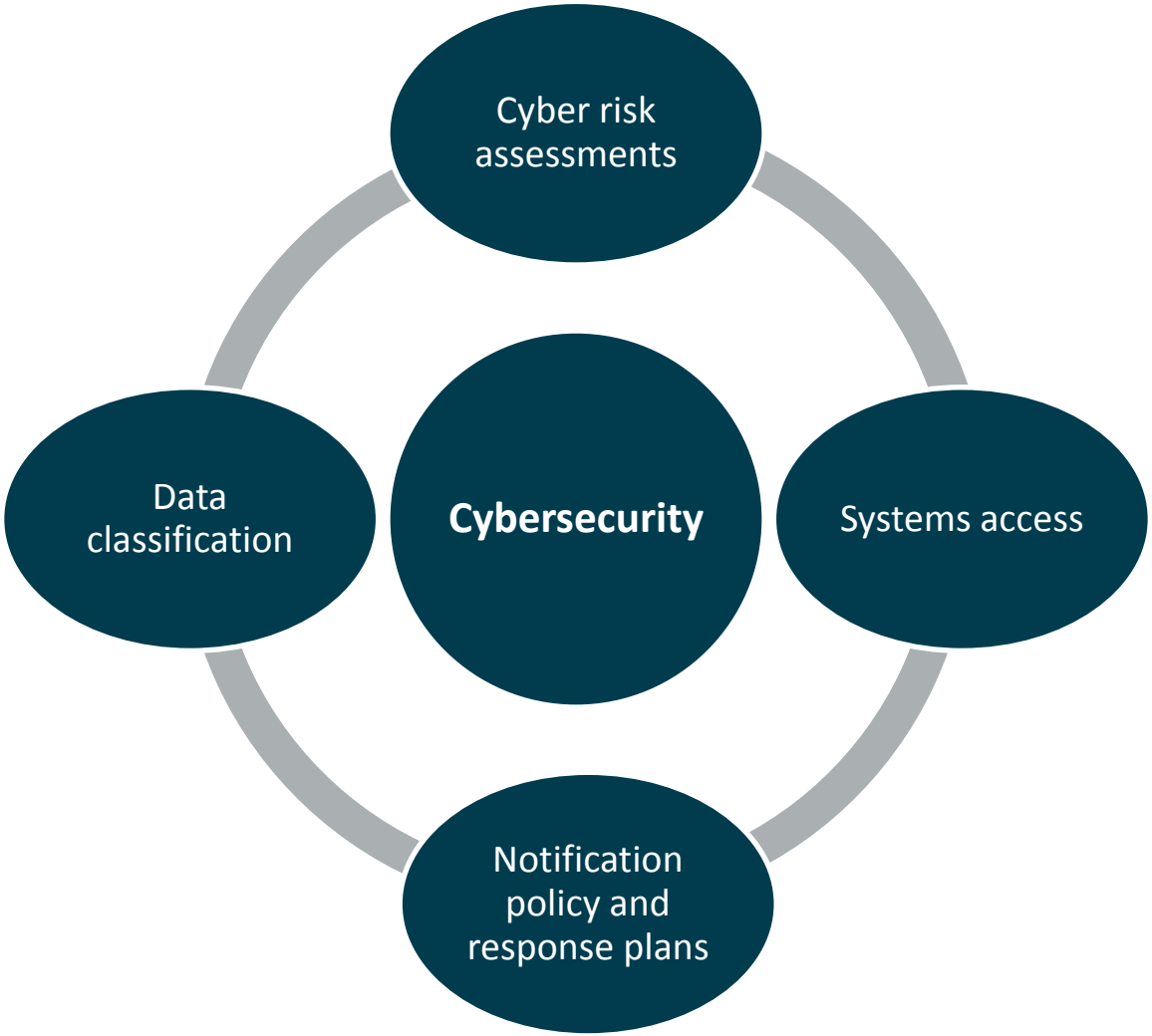
Yes, and this is annually verified	65%
Yes, this activity was undertaken but has not been repeated recently	22%
No	13%



See **section 2.1.5** of the Cross Industry Guidance

Cybersecurity – Key Considerations

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem



Cybersecurity – Sample Findings

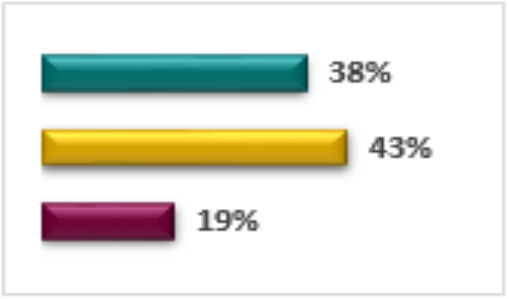
Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Q35. Is there a process in place to classify data enabling the firm to identify sensitive, valuable and critical data?

Yes, and this is annually verified

Yes, this activity has been undertaken but it is not considered a routine, repeatable process

No



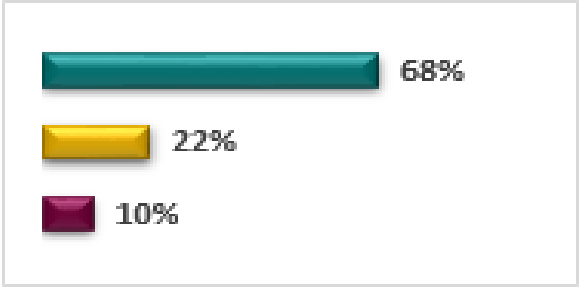
See **section 3.7** of the Cross Industry Guidance

Q39. Describe your cybersecurity incident notification policy?

All critical breaches are to be reported to law enforcement, customers and the regulator

Critical breaches are reported internally only

There is no formal breach notification policy



See **section 2.1.8** and **3.10** of the Cross Industry Guidance

Outsourcing - Key Considerations

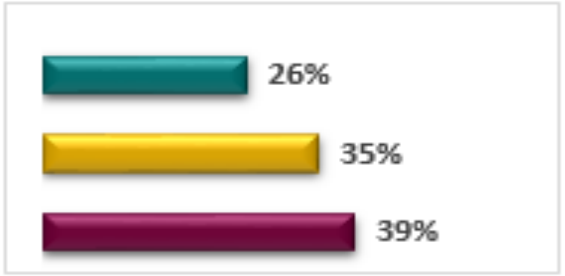
Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Outsourcing - Sample Findings

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Q45. Does the undertaking have an exit management strategy in place in case the SLA is terminated by either party?

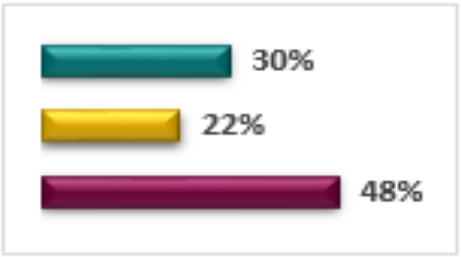
Yes, it is approved by the Board and is subject to regular review	26%
Yes, this activity was undertaken but has not been repeated recently	35%
No	39%



See **section 4.4** of the Cross Industry Guidance

Q47. Do you ensure that third parties with access to your systems have adequate cybersecurity practices?

Yes, training is provided, MI is collected and there is regular testing of controls	30%
Yes, training is provided, and compliance is assumed	22%
No, it is assumed that third parties have adequate cybersecurity practices	48%



See **section 3.8** of the Cross Industry Guidance

Concluding Remarks

- Firms encouraged to familiarise themselves with the guidance
- Strengthening required to raise standards & increase firms' resilience
- Encourage greater Board engagement
- Allocation of time and resources
- Continued focus by the Central Bank

Thank you