BMA
BERMUDA MONETARY AUTHORITY

Bermuda Insurance Sector Operational Cyber Risk Management — 2023 Report

Contents

About the Authority

The Bermuda Monetary Authority (Authority or BMA) was established by statute in 1969. Its role has evolved over the years to meet the changing needs in Bermuda's financial services sector. Today, it supervises, regulates and inspects financial institutions in the jurisdiction. It also issues Bermuda's national currency, manages exchange control transactions, assists other authorities with detecting and preventing financial crime and advises Government on banking and other financial and monetary matters.

The Authority develops risk-based financial regulations that apply to the supervision of Bermuda's banks, trust companies, investment businesses, investment funds, fund administrators, money service businesses, corporate service providers, insurance companies, digital asset businesses and digital asset issuances. It also regulates the Bermuda Stock Exchange and the Bermuda Credit Union.

Background

This report is based on the enhanced 2022 Bermuda Solvency Capital Requirement (BSCR) cyber filing returns. The BMA issues this communication to provide insights on the information obtained in the 2022 year-end filing from insurance managers, commercial insurers, brokers and agents.

Insurance Sector Operational Cyber Risk Management Code of Conduct (Code)

The final version of the Code was published in October 2020. The Code came into effect on 1 January 2021 and became enforceable on 1 January 2022.

The Code is designed to promote the stable and secure management of IT for entities within the insurance sector. The Authority is not adopting a 'one-size-fits-all' approach. It expects cyber risk controls to be proportional to the organisation's nature, scale and complexity. The BMA acknowledges that some entities will use a third party to provide technology services and may outsource their IT (e.g., to an insurance manager).

Executive Summary and Key Findings

The Authority is pleased to see continued strengthening of cyber risk controls across the insurance sector overall.

The Authority notes that 95% of all insurance entities now have a cyber risk policy in place and approved by the board. Additionally, 96% of all insurance entities confirmed that their cyber risk programme status is communicated regularly to the senior management team and board. Likewise, 95% of all insurance entities reported that they have clearly defined roles and responsibilities for each of the Three Lines of Defence (3LOD).

The analysis of filing return data has identified several areas that still require further improvement; these are:

1. **Network security Defence in Depth (DiD) controls** (a multi-layered approach) — the following controls are some examples of network security controls:

   - **Regular firewall ruleset reviews**
   - **Network segregation**
   - **Regular penetration testing**
   - **Regular vulnerability scanning**

   The 2022 data suggests that some entities would benefit from reviewing their network security controls. The ability to detect vulnerabilities and misconfigurations is related directly to the frequency of network security testing. Entities should review the frequency of their vulnerability scans. Any new internet-facing service should be subject to a penetration test before going into production. From a security testing perspective, an annual penetration test may not, by itself, give assurance on the security of the external perimeter.

   Where there are more than one network security controls missing, the risk is compounded. For example, if an insecure port is opened in error on a firewall and rulesets are not regularly reviewed, the open port will only be discovered when the next external vulnerability scan or penetration test is conducted. The longer it takes to identify the issue, the probability of the open port being exploited increases, potentially leading to an incident.

2. **Data classification** — data should be classified and protected in a manner commensurate with its sensitivity, value and criticality. The information must be classified in terms of its value, regulatory and legal requirements, sensitivity and criticality to the organisation. Once data is classified, the corresponding security controls must be applied to protect it. The most critical data should be subject to the most stringent security controls.

   Only 73% of respondents have completed the classification of their data. This is only a small improvement over the 66% figure reported in the 2021 BSCR returns, still much lower than regulatory expectations. Classifying data is a requirement of the Code and entities should review the status and progress of their data classification initiatives.

3. **Third-party cyber risk management assessment** — managing cyber risk from third-party service providers and IT hardware and software supply chains is an important part of cyber risk management. Contractual clauses should be in place to ensure cyber risk requirements set by the insurance entity are met by its service providers, considering regulatory requirements.

   The Authority notes that many organisations now use IT services through a Software as a Service provider (SaaS). Third-party service providers must be subjected to third-party risk reviews by the entity.

   Only 83% of entities have reviewed the cyber risk associated with their third-party IT providers in the last 12 months, which is a small improvement over the 79% reported in the 2021 BSCR returns.

The registrant must ensure oversight and clear accountability for all outsourced functions as if these functions were performed internally and subject to the registrant's own governance and internal controls standards. The registrant must also ensure the service agreement includes terms on compliance with jurisdictional laws and regulations, cooperation with the Authority and access to data and records in a timely manner.

4. **Data Loss Prevention (DLP) controls** — incidents resulting in data breaches often lead to financial loss and reputational damage. DLP controls can be configured at different layers of a network, for example, email, internet proxy server and restrictions on port access on end-user devices. DLP controls reduce the risk of accidental and malicious data exfiltration from a network.

   DLP requirements should be assessed against data criticality and regulatory and contractual requirements. Furthermore, 83% of entities stated they have DLP controls in place, compared to 80% in 2021. Although it is a marginal improvement, the figure is still much lower than regulatory expectations.

5. **Contracted fourth-line IT security expert service** — in the event of a major cyber incident, these Subject Matter Expert (SME) services would typically provide expert assistance in mitigating impact and recovering to normal business operations. In 2022, only 85% of all insurers reported having such a contract in place. Entities may wish to review their access to an IT security SME service as part of their incident and crisis management plans.

6. **Annual test of Business Continuity Planning (BCP) and IT Disaster Recovery (DR) plans** — annual testing of BCP and DR is a fundamental component of resilience testing and a requirement of the Code. In 2022, 87% of entities reported completing these tests over the last 12 months. Entities should review the frequency of their BCP and DR testing.

Notification of Cyber-Reporting Events to the Authority

The Insurance Amendment Act 2020 came into force on 5 August 2020, requiring notification of cyber-reporting events to the Authority. Complete guidance on the requirements is given in section 6.5 of the Code.

It should be noted that only cyber-reporting events resulting in a significant adverse impact on the regulated entity's operations, policyholders or clients must be reported to the Authority. When in doubt about whether an event is reportable, registrants should consult with the Authority for guidance.

A principal representative (for insurers) and an appropriate officer (for insurance managers and intermediaries) must notify the Authority within 72 hours of when there is either a determination or confirmation of an event.

An incident report containing known details of the incident, the root cause, actions taken to minimise the impact and any actual adverse impact to the organisation must be submitted within 14 days of the initial incident notification date. If the full root cause is not known by the 14-day submission, the Authority may request further information or the full root cause report when the entity concludes investigations.

Cyber reporting events are treated in complete confidence. The Authority analyses reported events, and this data is used as one of the inputs for cyber risk profiling. The Authority places high importance on keeping up to date with the fast-changing nature of cyber risks and their potential impact on registrants and the insurance sector as a whole.

Key findings from cyber events reported from 2022 to report publication date

1. Email continues to be targeted successfully by malicious attackers. When email systems are compromised and the data stored in email has not been classified, this can lead to a situation where it is not known what data has been breached, if any PII has been accessed and who the data belongs to. A retrospective classification and investigation of email data must then be carried out, which can be very complex, costly and time-consuming. This highlights the need to classify data and ensure it is protected with security controls commensurate with its criticality.

2. Many entities now use SaaS services and the Authority has seen an increasing number of incidents impacting these SaaS providers. This has resulted in impacts to entities. For example: the loss of (PII) that the entity had entrusted the SaaS provider to store and process securely.

3. Phishing and social engineering attacks have also been reported, reflecting ongoing malicious activity making use of this attack vector.

Next the Authority will:

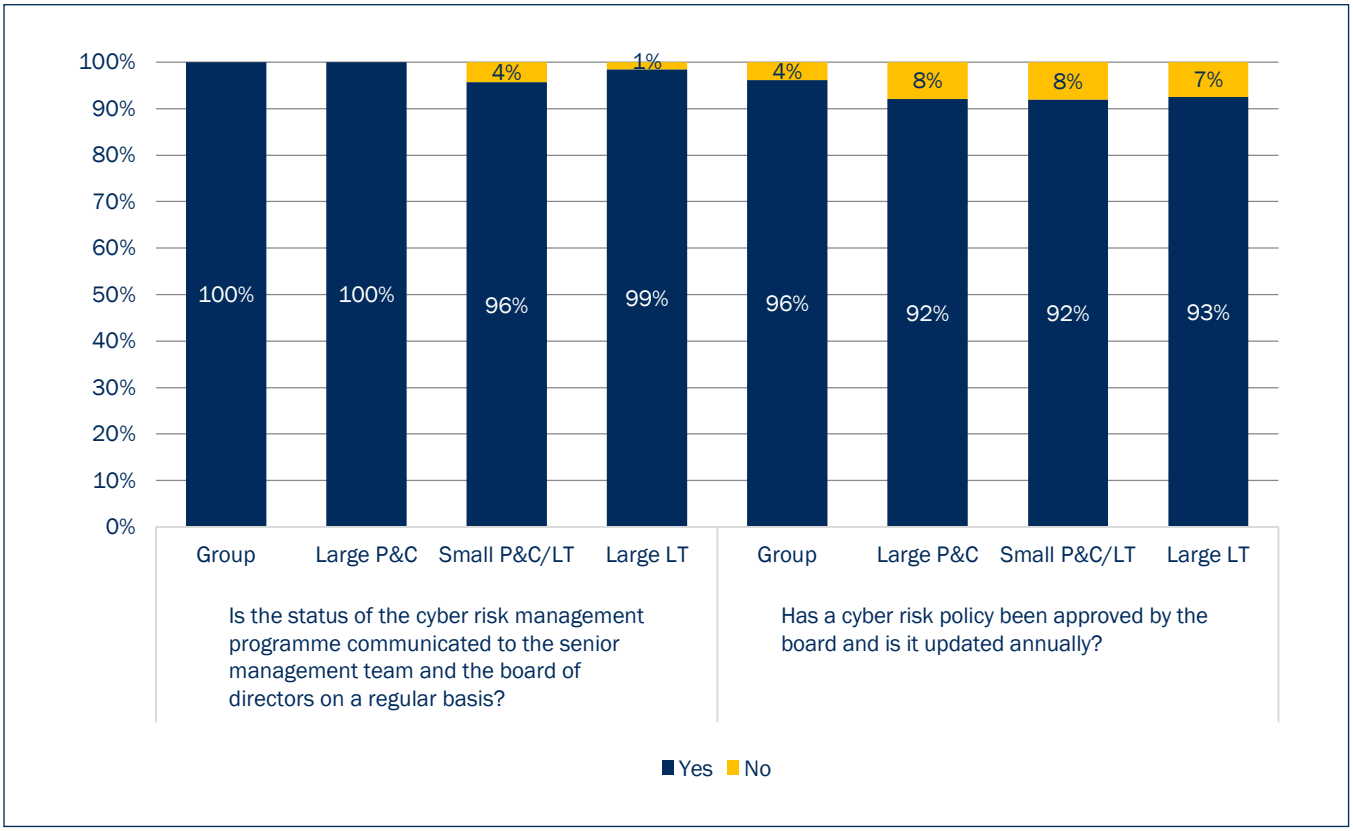
- Continue to monitor the evolving nature of the cyber risk threat landscape
- Continue to assess cyber risk filing returns
- Propose and introduce ways to streamline the cyber risk filing return
- Continue to review cyber reporting events to further understand the risk profile of individual insurers and the sector as a whole
- Review registrants' compliance with the Code as part of the supervisory review process
- Continue to consult proactively with the insurance sector
- Continue to require that companies clearly detail operational cyber risk in the Commercial Insurer Solvency Self-Assessment/Group Solvency Self-Assessment process

1 Analysis of Filing Return Data 2022 — Commercial Insurers

This section is based on the 2022 BSCR cyber risk filing returns (Schedule Ve) for commercial insurers only. The filing return data has been categorised by the size and the market of the respondent, namely Group, Large Property and Casualty (Large P&C), Small Property and Casualty and Long Term (Small P&C/LT) and Large Long Term (Large LT).

Some figures quoted in the paragraphs below are the computed average of all entries for all types of commercial insurers. The graphs illustrate statistics broken down by respondent type.

1.1 Board Oversight of Cyber Risk

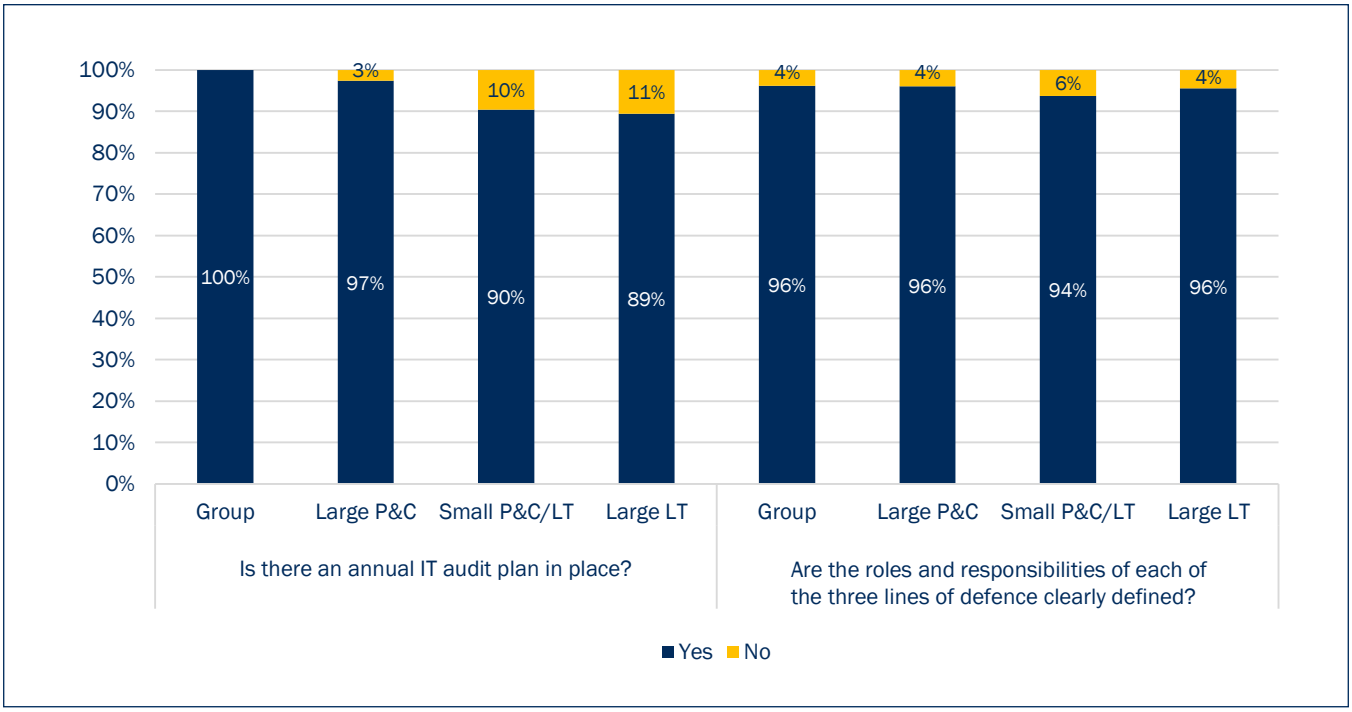


Over 99% of commercial insurers confirmed they communicate regular cyber risk management programme status updates to the board.

In addition, 93% of commercial insurers reported that the cyber risk policy had been approved by the board and updated annually.

The Code mandates that the board of directors and senior management team have oversight and accountability for cyber risk.

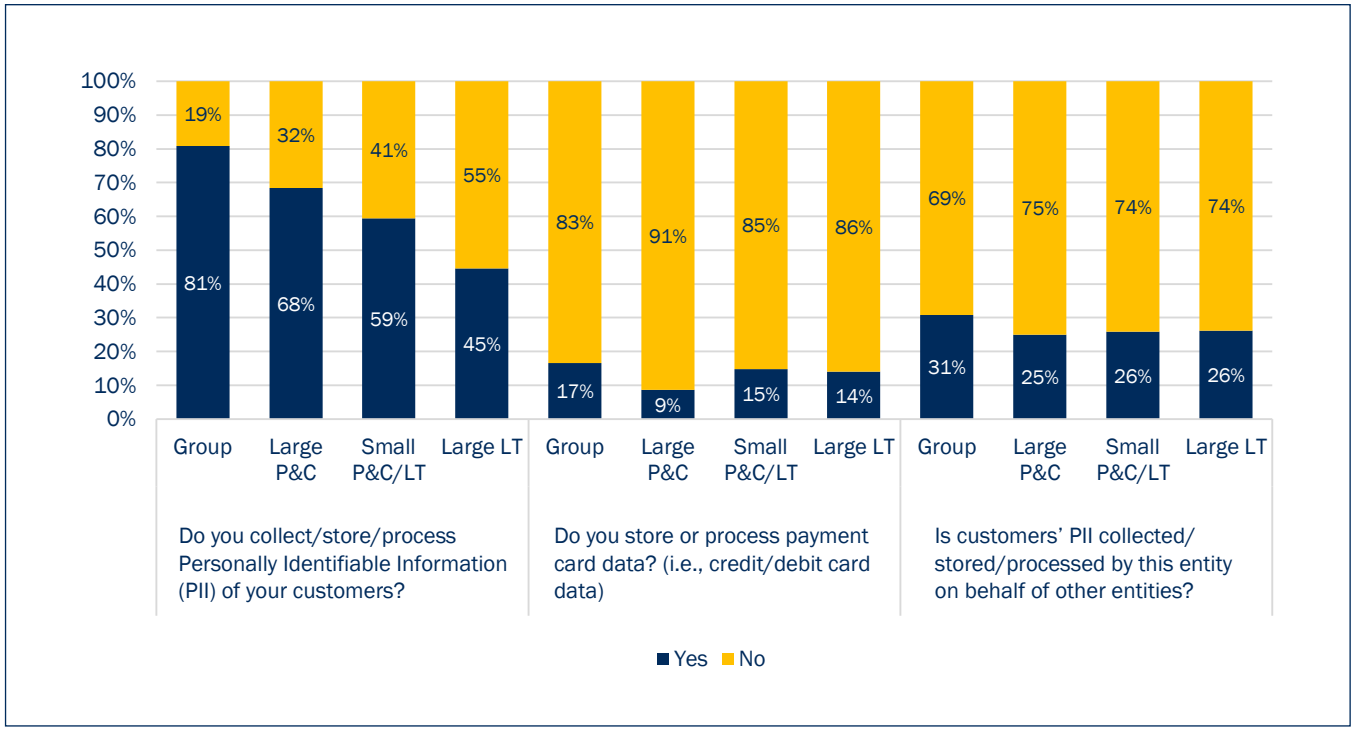
1.2 Three Lines of Defence



Similarly, 96% of commercial insurers reported that they have clearly defined roles and responsibilities for each of the three lines of defence (3LOD).

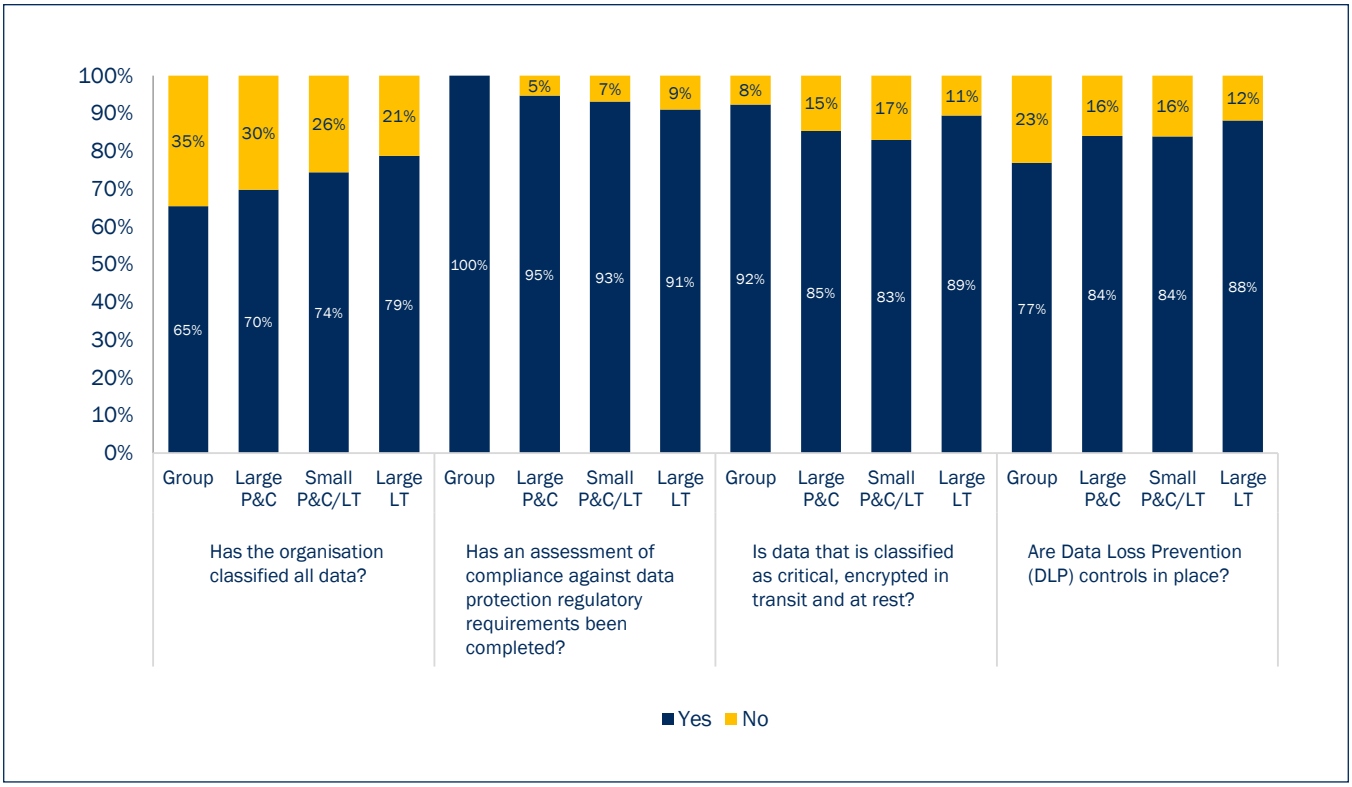
However, for both Small P&C/LT and Large LT commercial insurers, less than 90% of entities reported that they have established an annual IT audit plan, which is a requirement of the Code.

1.3 PII collected, stored and processed



This data shows that 63% of commercial insurers collect, store or process PII. In comparison, 14% reported they store or process payment card data, whereas 26% of commercial insurers reported that they collect, store or process PII on behalf of other entities.

1.4 Data Security Controls

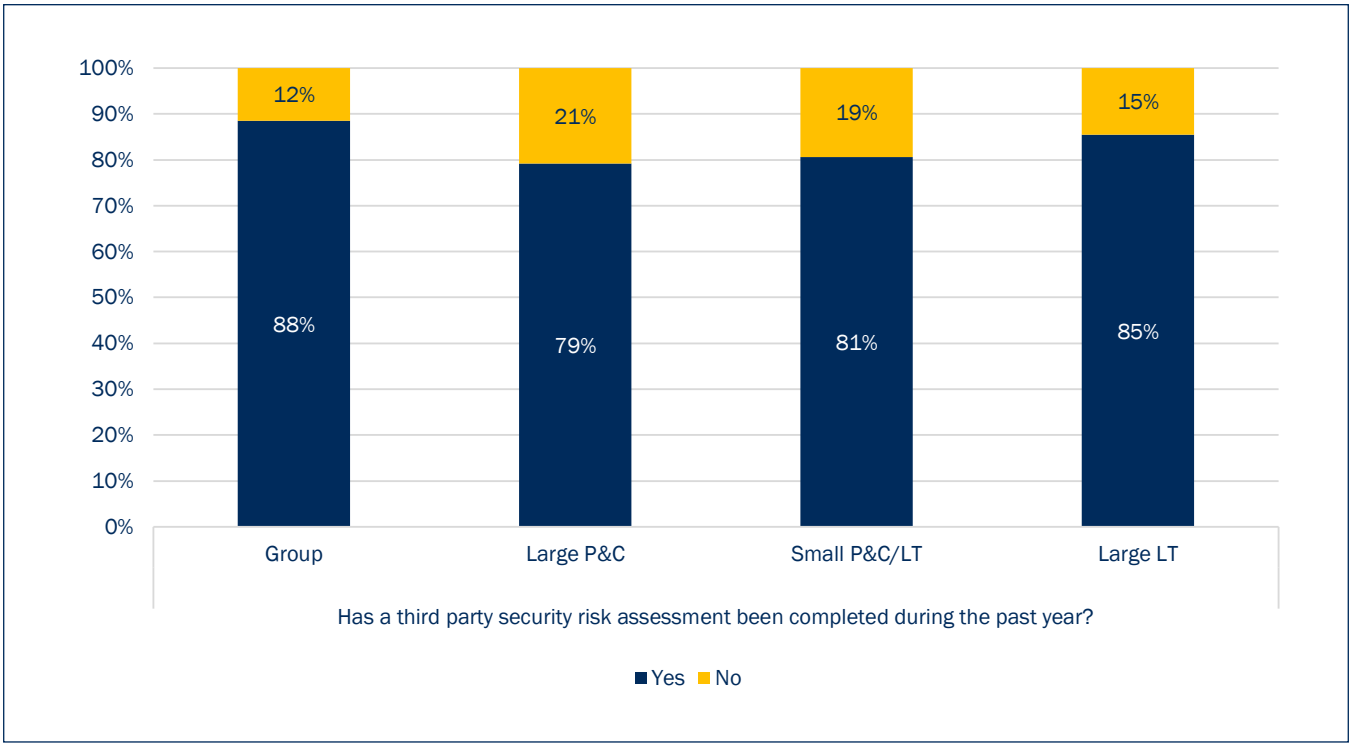


Only 72% of commercial insurers reported that their data has been classified, which is lower than anticipated and is noted as an area for improvement.

Nevertheless, 94% of commercial insurers have undertaken an assessment against data protection regulatory requirements; however, this has not translated to DLP controls being in place. Only 83% of commercial insurers reported having DLP controls in place. This is considered low and commercial insurers should review their risk exposure.

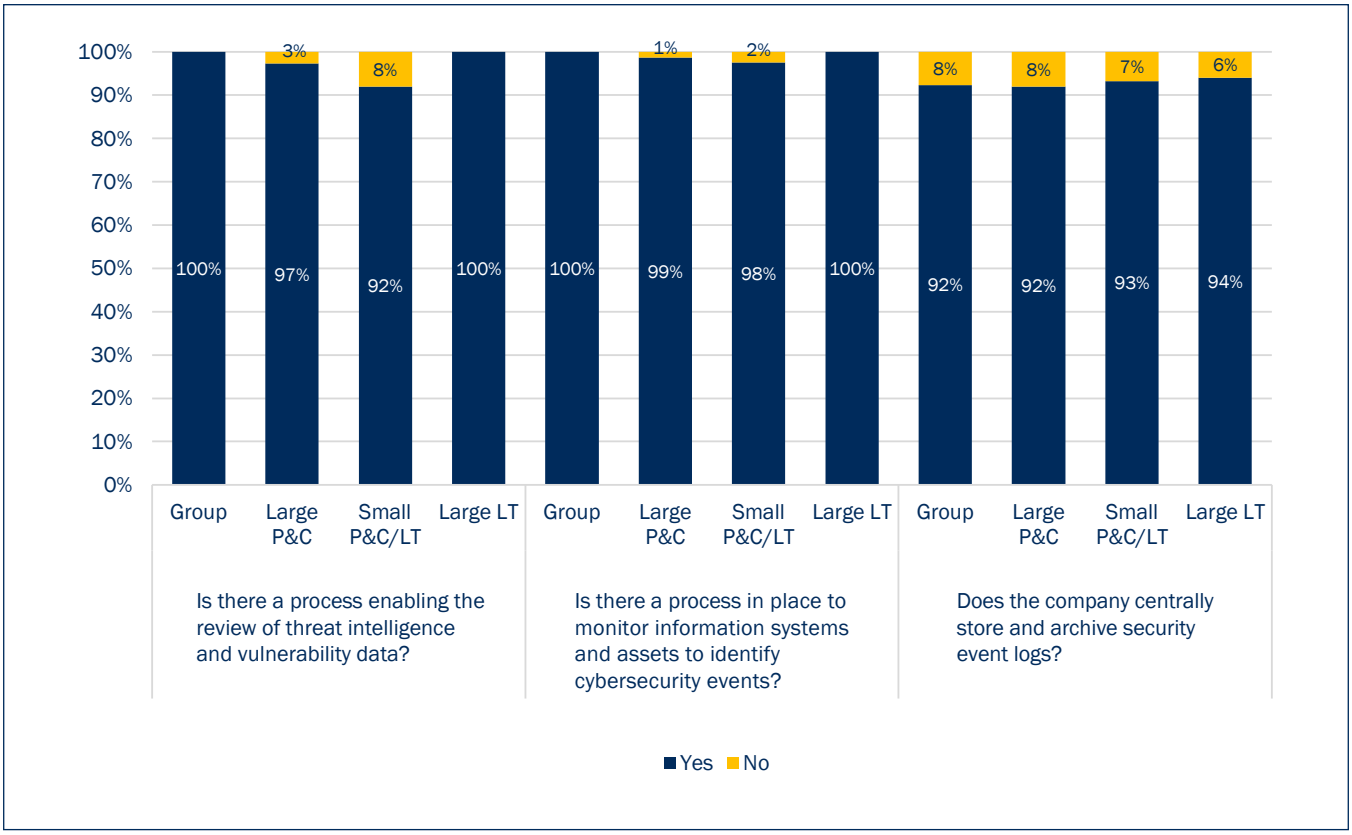
In 2022, 87% of commercial insurers encrypt critical data in transit and at rest. The Cyber Code requires that non-public data is encrypted in transit and at rest. Entities should review their compliance with this requirement.

1.5 Third Party Risk Assessment



In 2022, 83% of commercial insurers have undertaken third-party security risk assessments in the past year. This is considered low, and entities should review the status and effectiveness of their third-party risk assessment process.

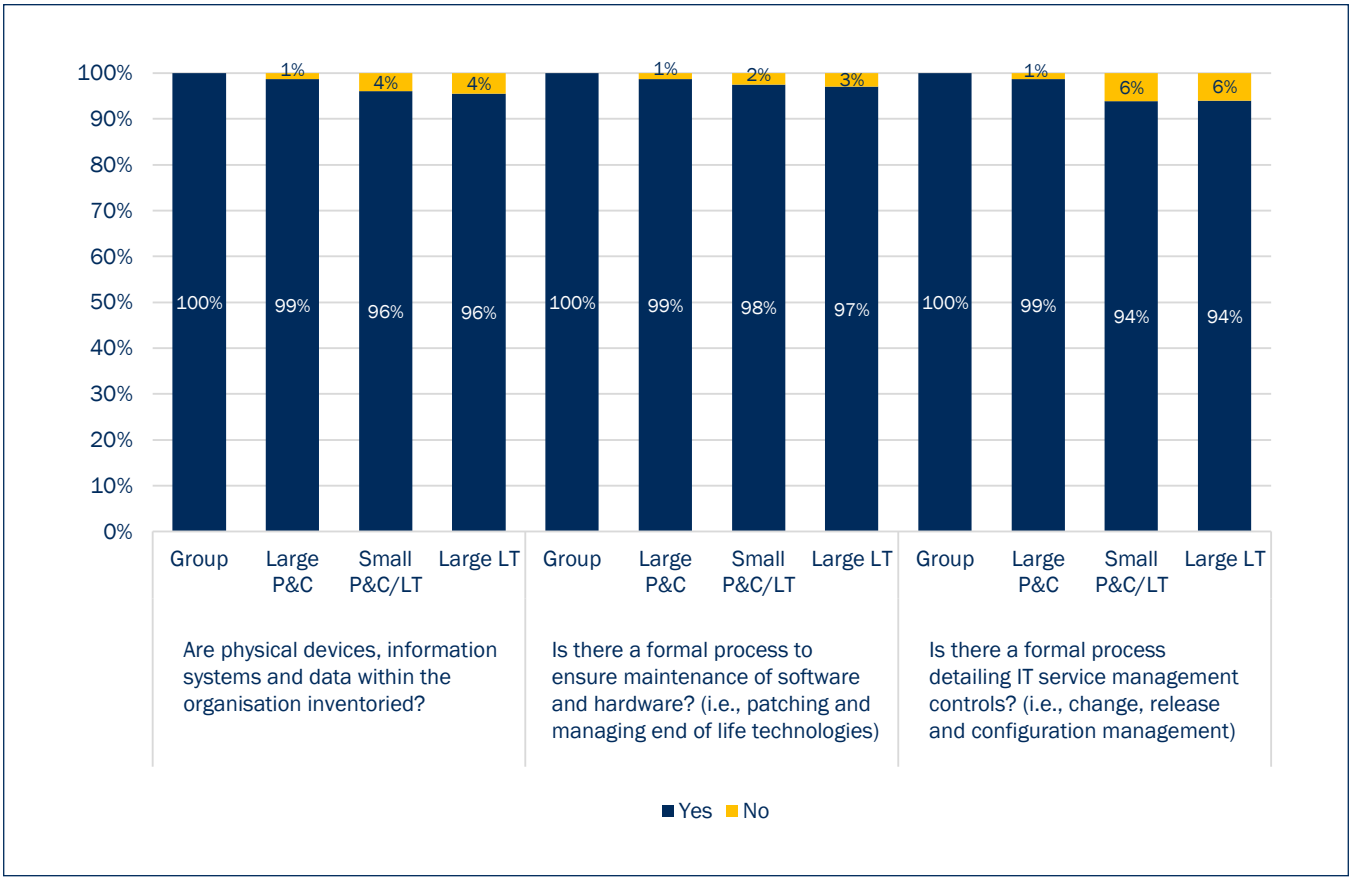
1.6 Detect and Protect Controls – threat intelligence and event monitoring



Moreover, 97% of commercial insurers reported that they review threat intelligence and vulnerability alerts, while 99% of commercial insurers have reported that they monitor security events. It was noted that 93% reported they have a central archive of event logs.

Security event logs must be available so that they can be monitored, which is a proactive detective control. If an incident occurs, then an inspection of event logs may be used to determine the root cause. Entities should also ensure they have the ability to monitor, centrally store and archive security event logs.

1.7 IT Service Management Controls

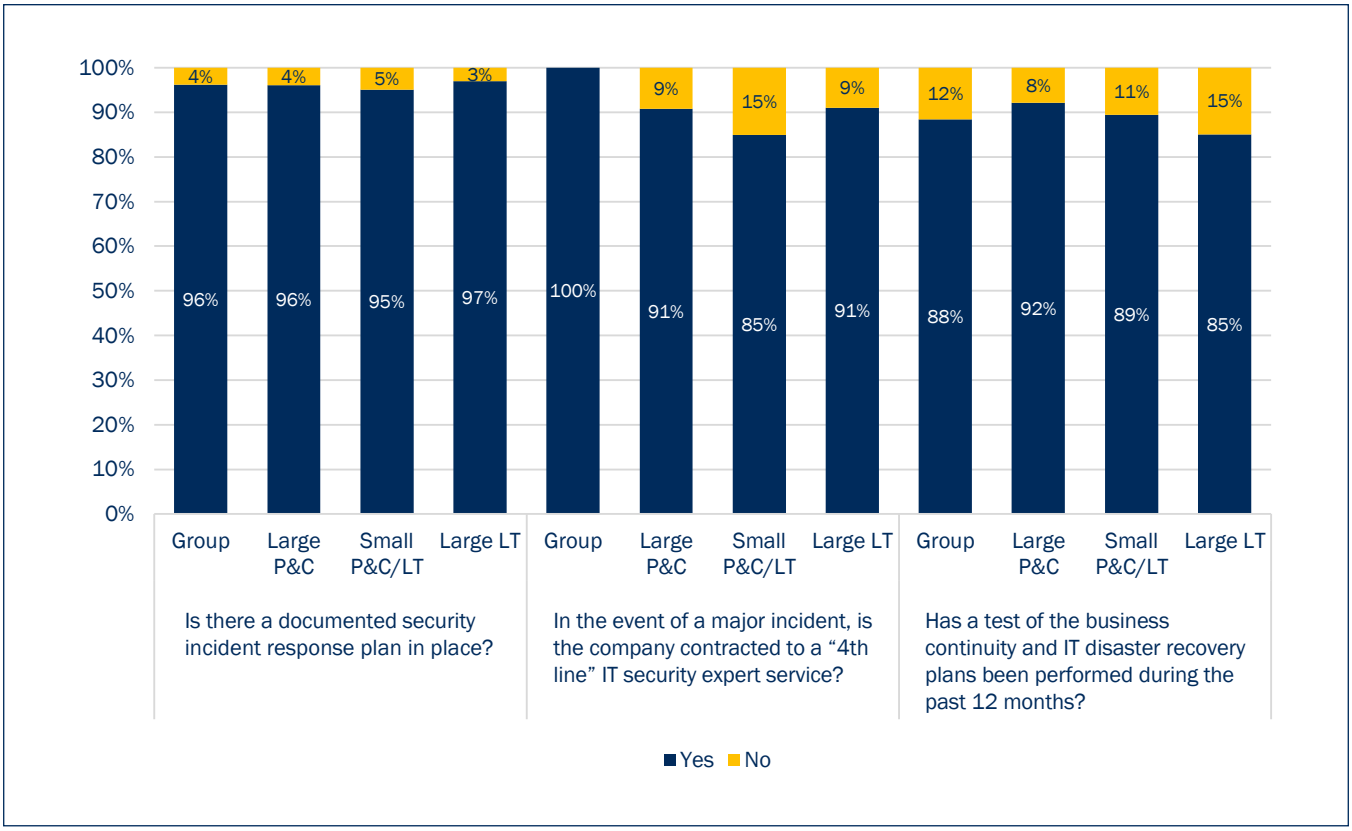


IT service management processes should be in place to assist in the management of stable and secure IT systems.

In 2022, 97% of commercial insurers reported that they have an asset inventory in place and 98.5% of commercial insurers reported that they have a formal software and hardware maintenance process in place.

Likewise, 97% of commercial insurers reported that they had service management controls in place.

1.8 Respond and Recover Controls



Additionally, in 2022, 96% of commercial insurers reported that a documented security incident response plan was in place.

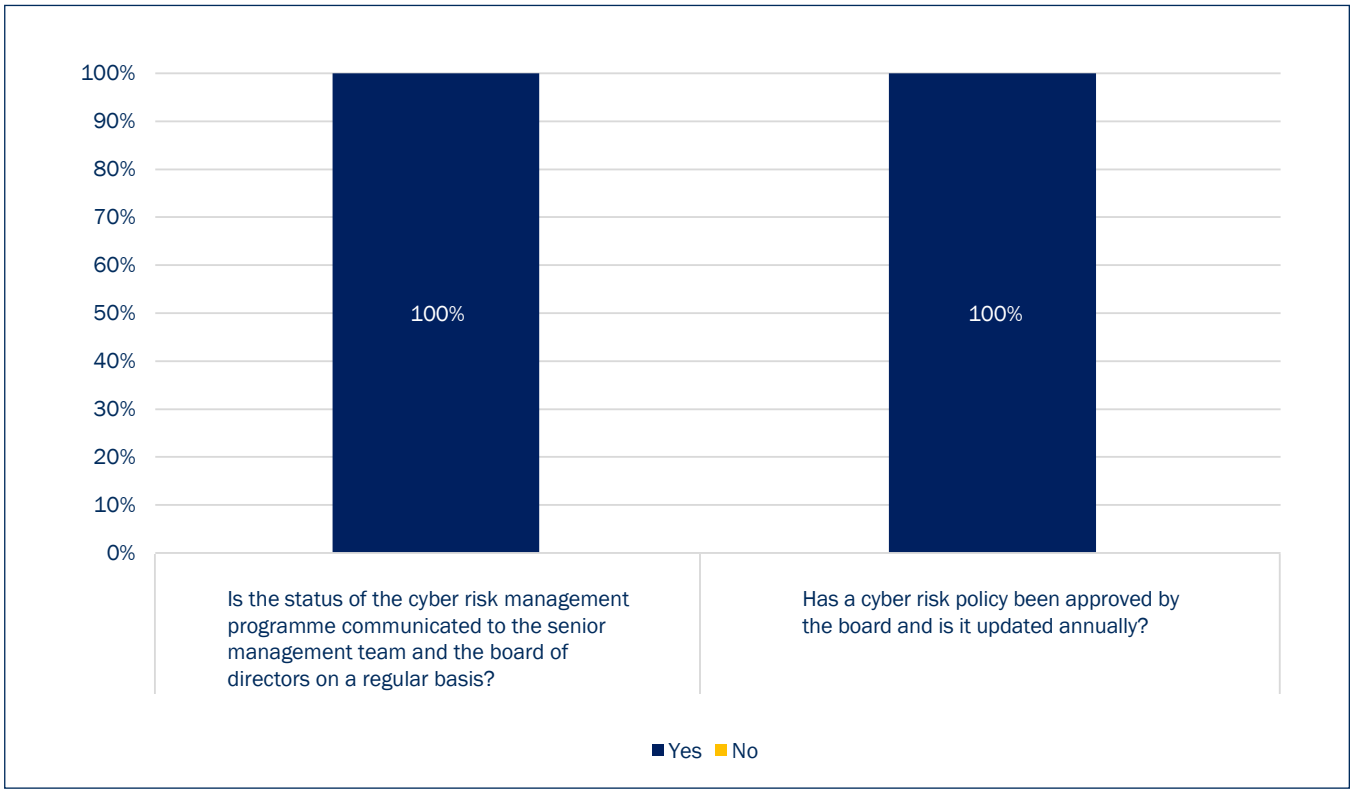
In the event of a major cyber incident, a contracted SME IT security service may be able to assist with incident response and recovery of IT services; 92% of commercial insurers reported that they had such a contract in place.

In fact, 12% of Groups and 15% of large LT entities have not tested their BCP and DR plans over the last 12 months.

2 Analysis of Filing Return Data 2022 — Insurance Managers

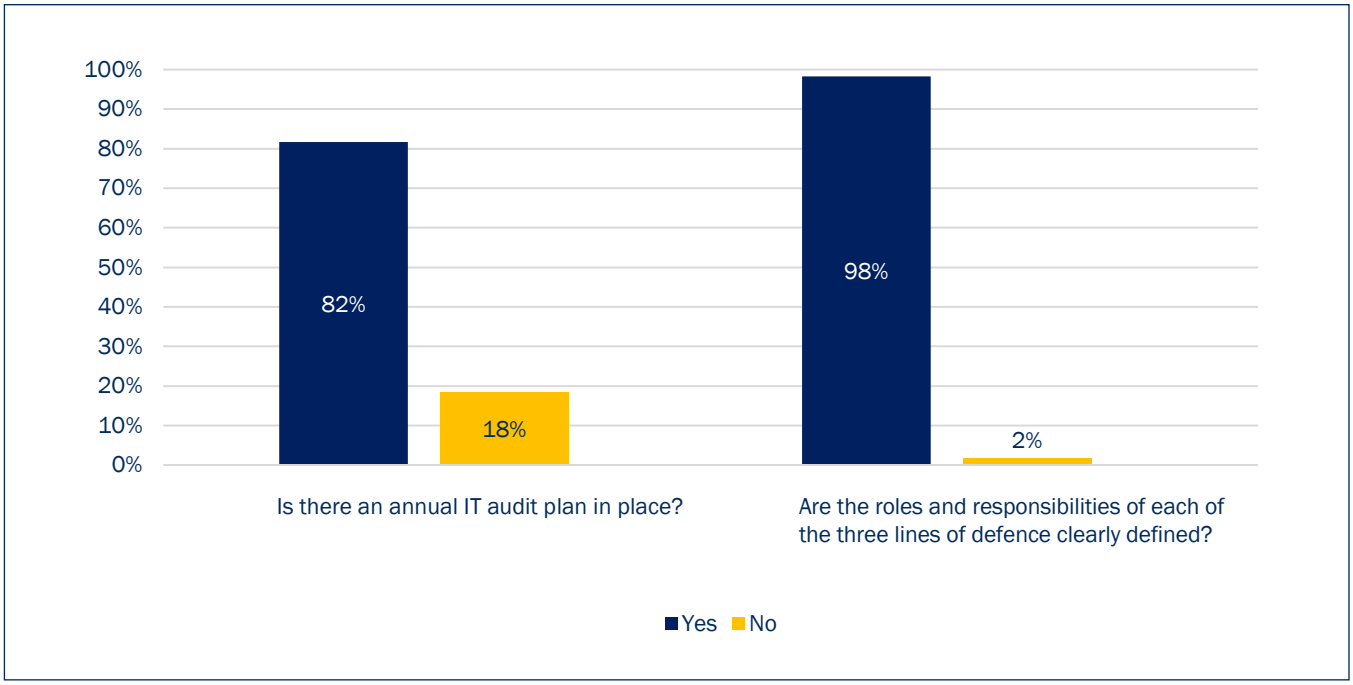
This section assesses data from the 2022 BSCR cyber risk filing returns (Schedule Ve) completed by insurance managers only. The Authority notes that insurance managers complete the cyber risk filing return for LPIs and some of the small commercial insurers.

2.1 Board Oversight of Cyber Risk



In 2022, 100% of insurance managers confirmed that they have board approval of their cyber risk policy and that regular status updates are communicated to the board.

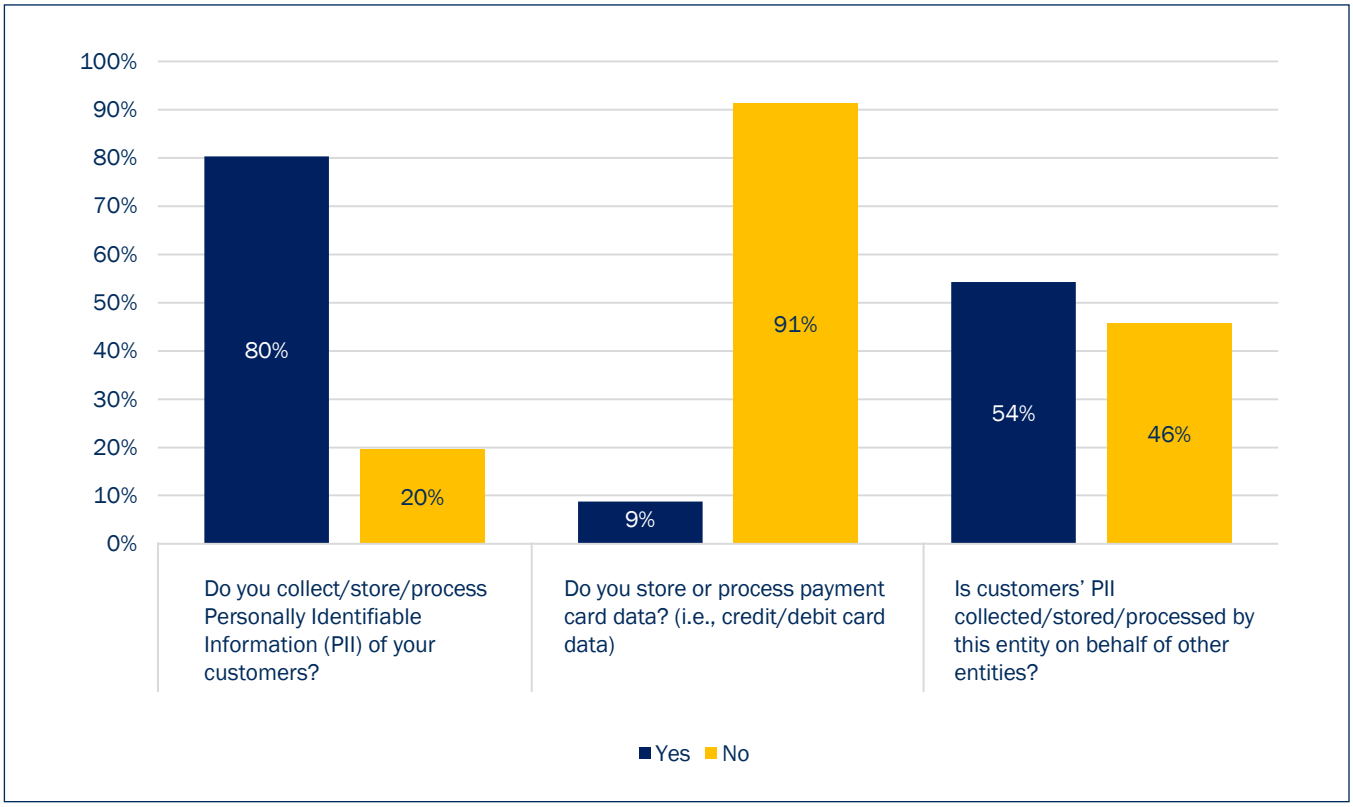
2.2 Three Lines of Defence



Only 82% of insurance managers have an annual IT audit plan in place. An annual IT audit plan is a requirement of the Code, which is noted as an area requiring improvement.

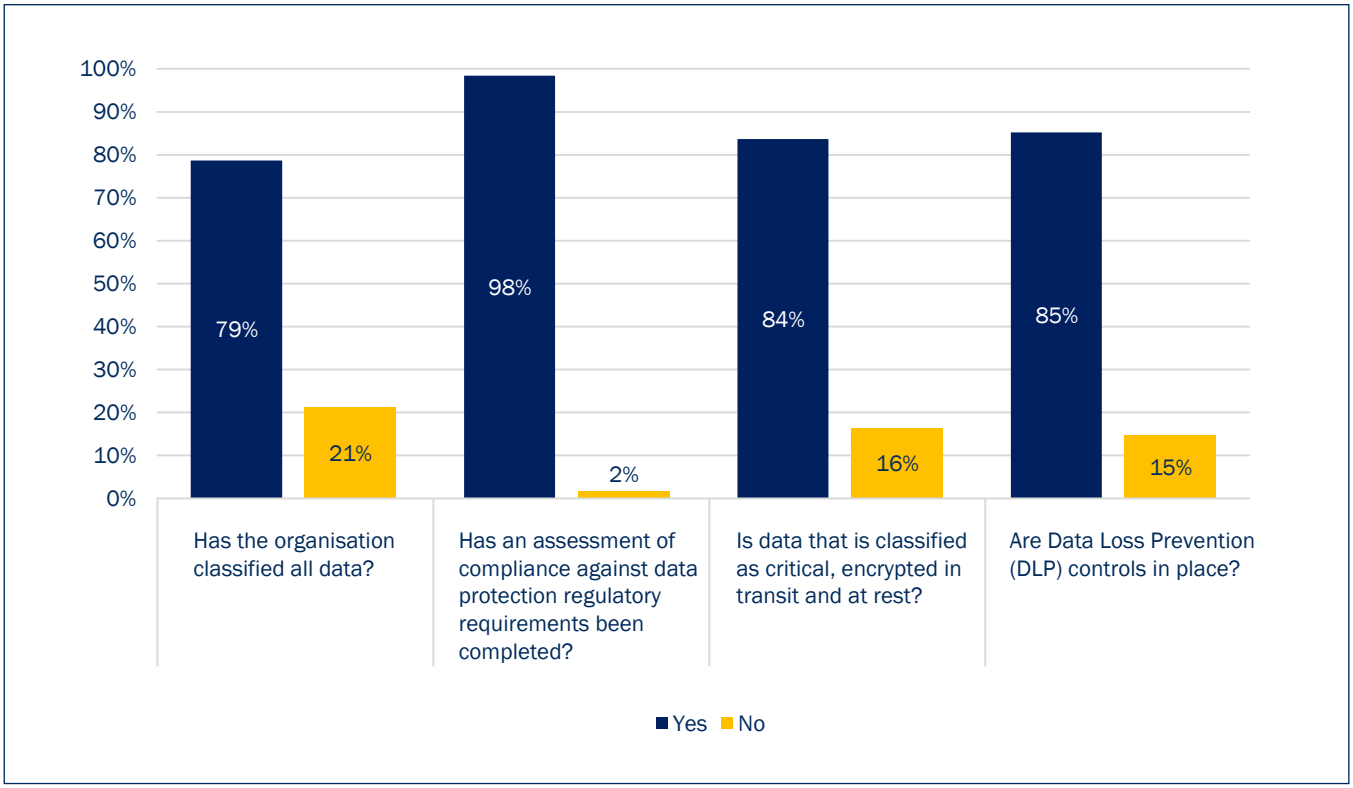
However, 98% of insurance managers reported that they have clearly defined roles and responsibilities for each of the three lines of defence.

2.3 PII collected, stored and processed



Furthermore, 80% of insurance managers collect, store or process PII, while just 9% reported they store or process payment card data. However, 54% of insurance managers reported collecting, storing, or processing PII on behalf of other entities.

2.4 Data Security Controls



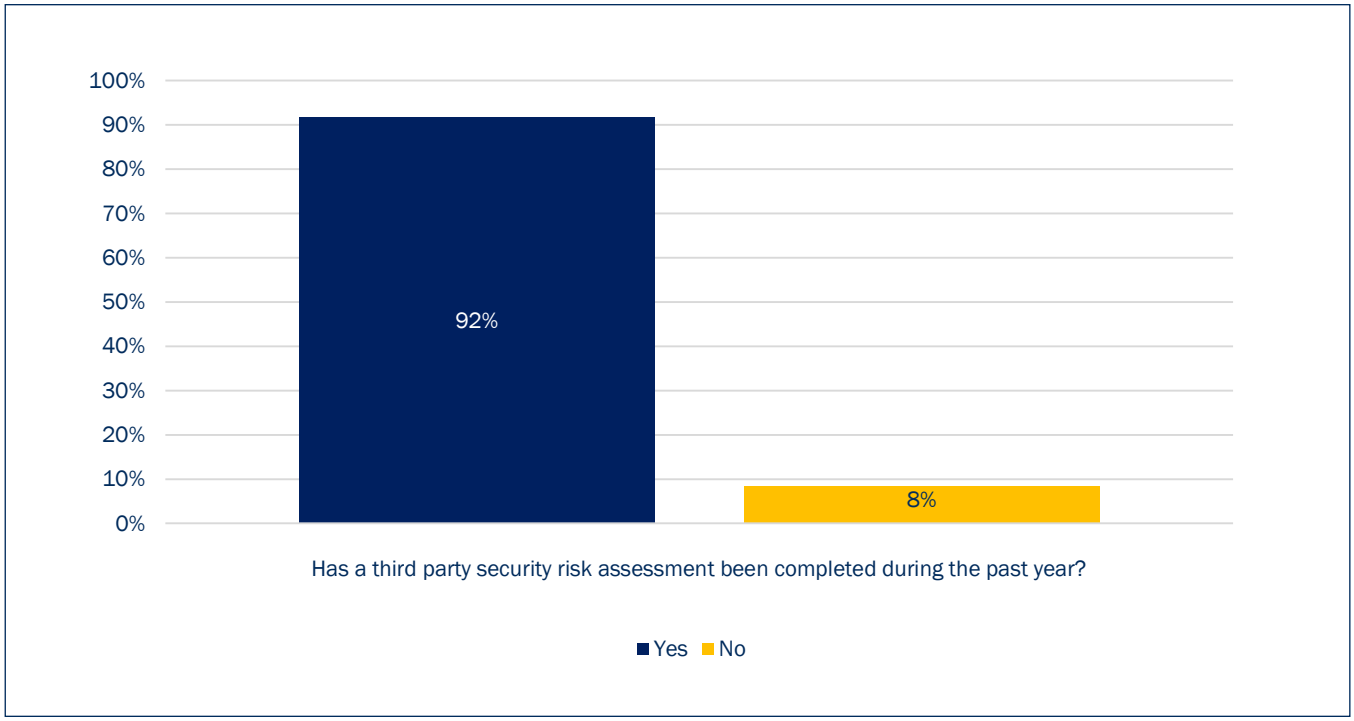
Only 79% of insurance managers reported that their data has been classified, which is lower than anticipated and is noted as an area for improvement.

In 2022, 98% of insurance managers have undertaken an assessment against data protection regulatory requirements; however, this has not translated to DLP controls being in place.

However, just 84% of insurance managers encrypt critical data in transit and at rest. The Cyber Code requires that non-public data is encrypted in transit and at rest. These entities should review their compliance with this requirement.

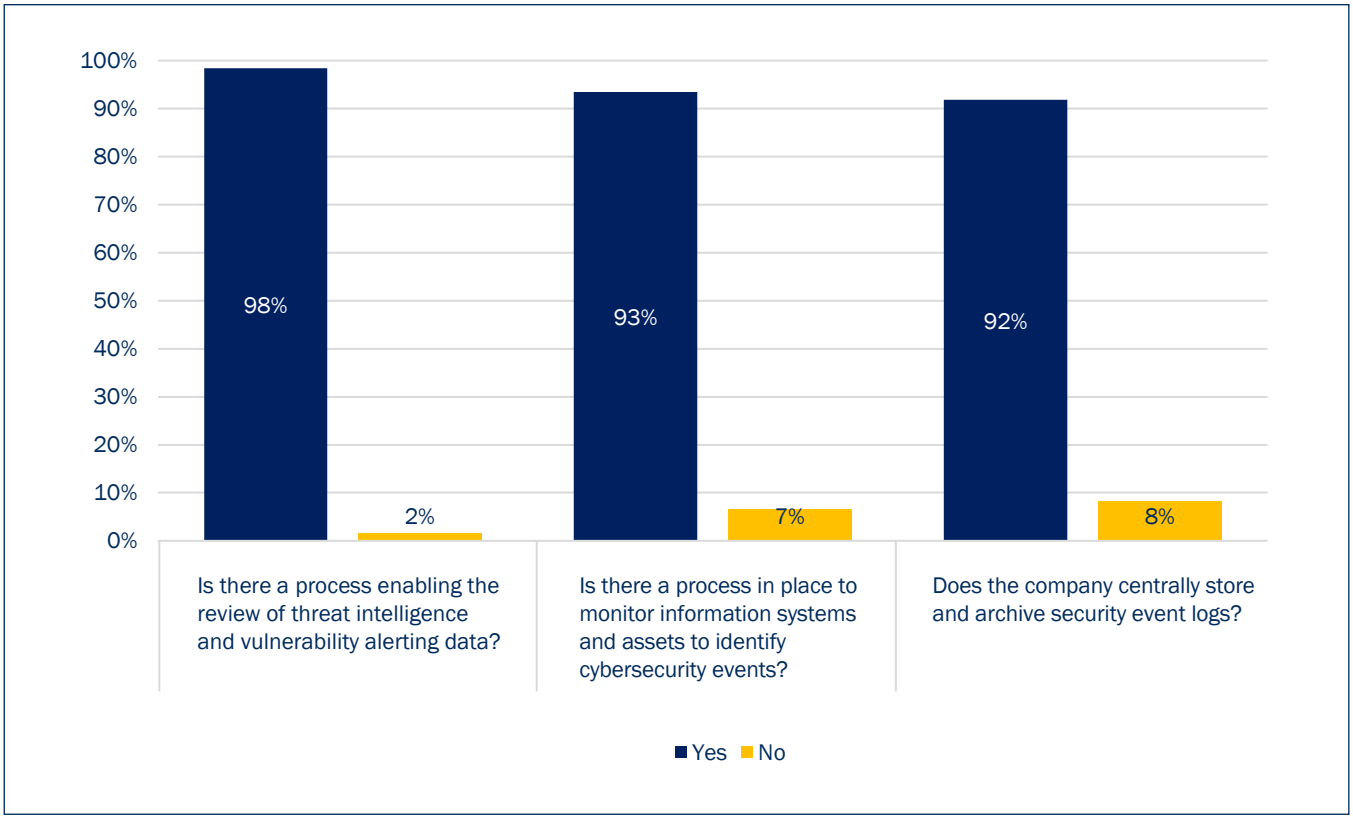
Only 85% of insurance managers reported having DLP controls in place. This is considered low and insurance managers should review their risk exposure.

2.5 Third Party Risk Assessment



In the past year, 8% of insurance managers have not undertaken third-party security risk assessments. Third-party risk has been identified as a key area of risk and entities should review the effectiveness of the controls they have in place.

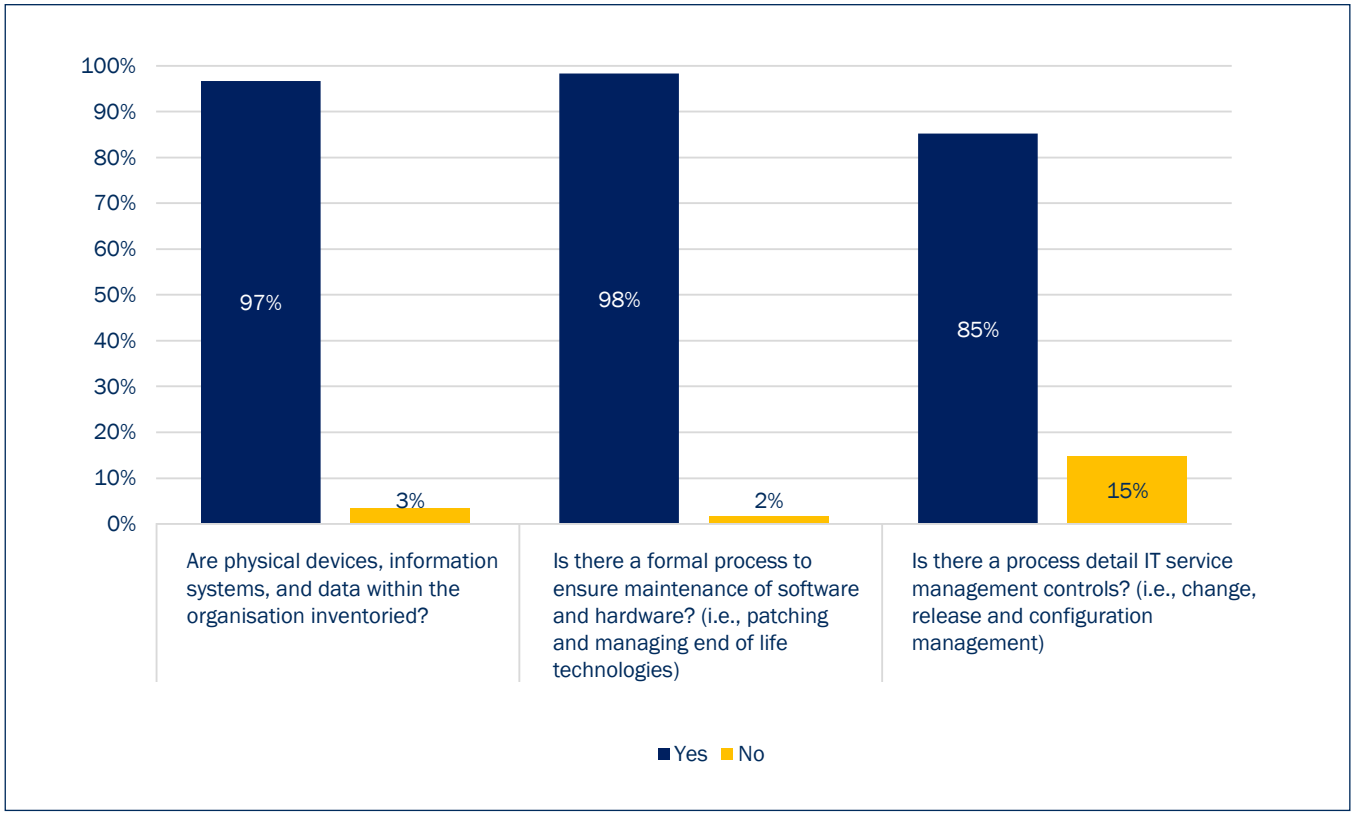
2.6 Detect and Protect Controls — threat intelligence and event monitoring



Additionally, 98% of insurance managers reported reviewing threat intelligence and vulnerability alerts, whereas just 7% of insurance managers have reported that they do not monitor security events. Instead, 8% reported that they do not have a central archive of event logs.

Security event logs must be available to be monitored, which is a proactive detective control. If an incident occurs, the inspection of event logs may assist in determining the root cause. Entities should ensure they have the ability to monitor, centrally store and archive security event logs.

2.7 IT Service Management Controls

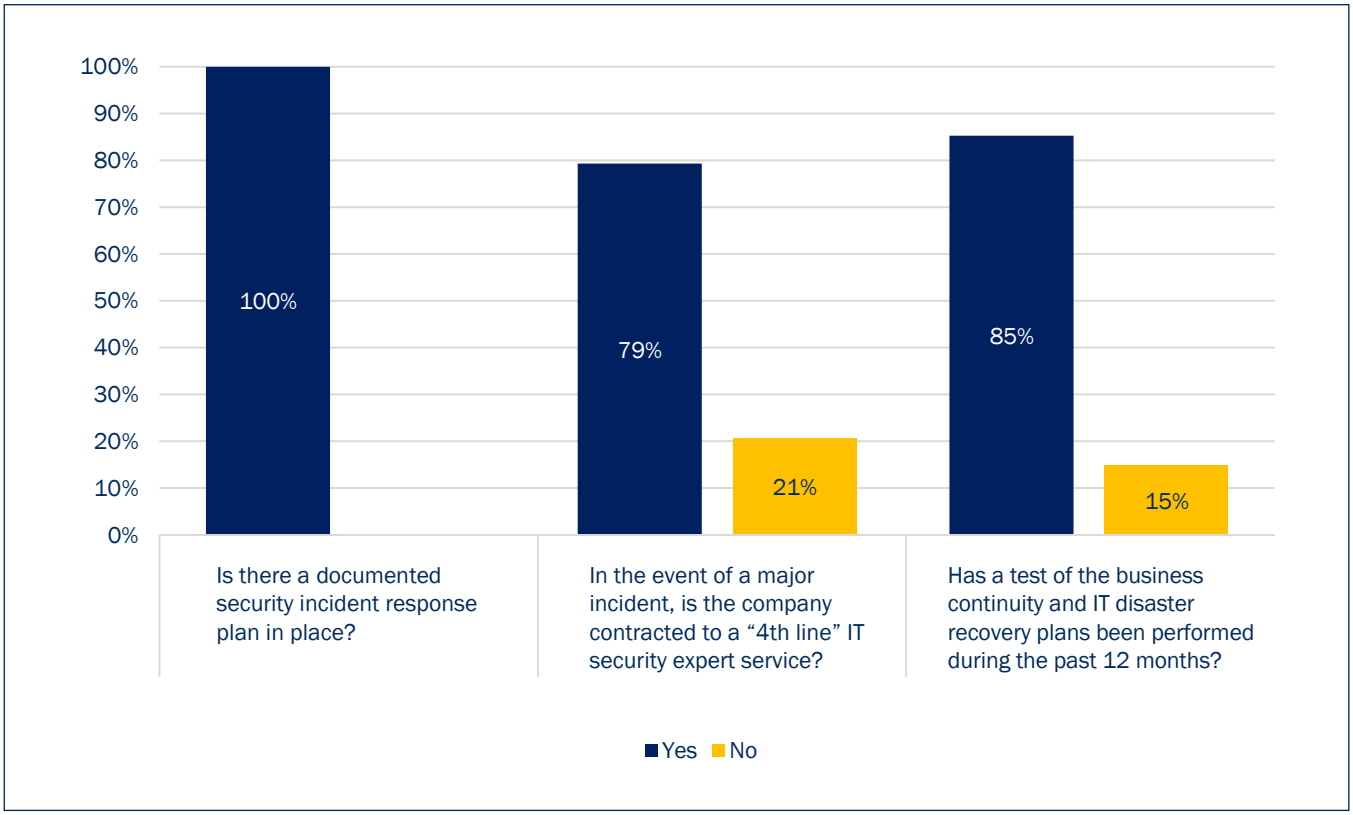


IT service management processes should be in place to ensure that IT systems are stable and secure.

In 2022, 97% of insurance managers reported having an asset inventory in place. Overall, 98% of insurance managers reported having a formal software and hardware maintenance process in place.

Additionally, 15% of insurance managers reported that they do not have a change management process in place. This is considered to be low and is noted as an area for improvement.

2.8 Respond and Recover Controls



Meanwhile, 100% of insurance managers reported that a documented security incident response plan was in place.

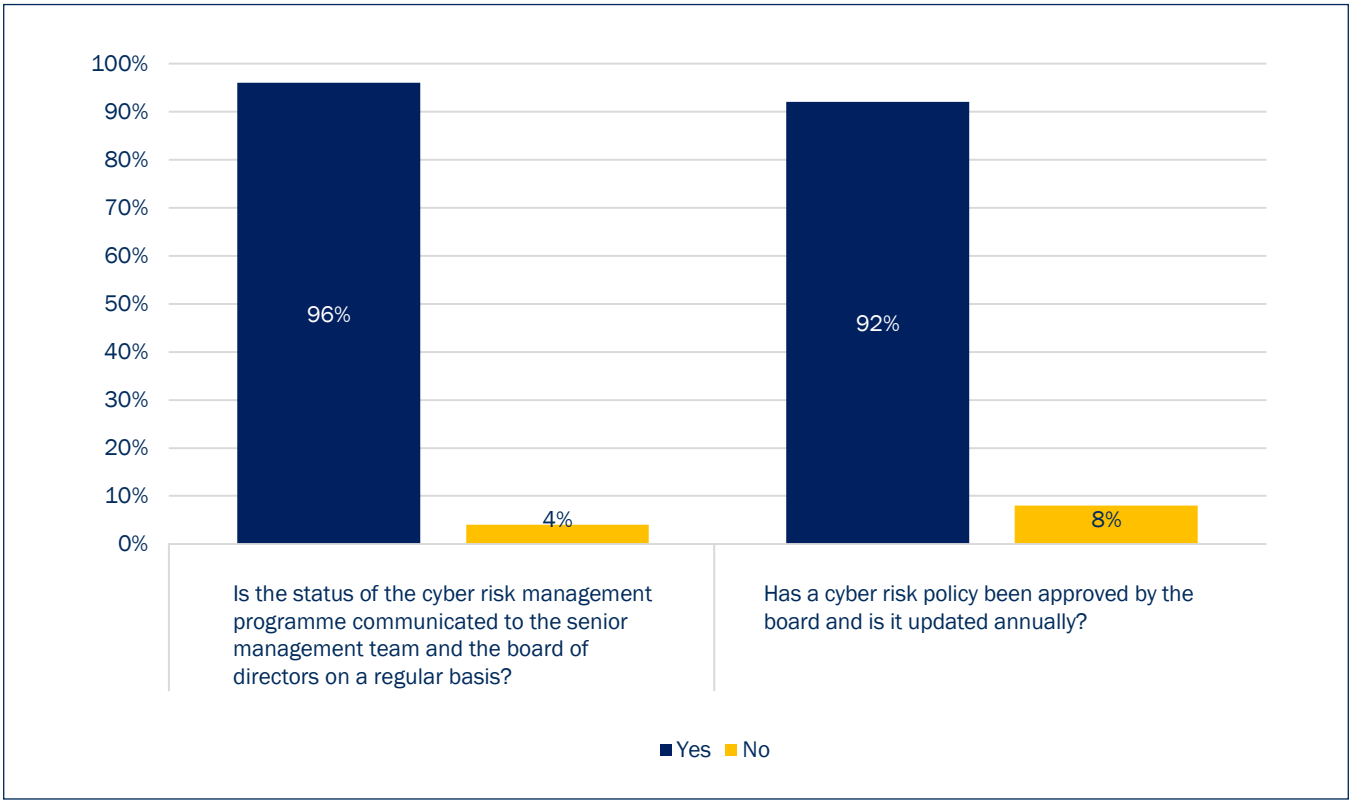
In the event of a major cyber incident, a contracted SME IT security service may be able to assist with incident response and recovery of IT services. In 2022, 79% of insurance managers reported having such a contract in place.

However, 15% of insurance managers have not tested their BCP and DR plans over the last 12 months. The Cyber Code requires annual BCP and DR testing, and entities should ensure they take the necessary steps in order to comply with this requirement.

3 Analysis of Filing Return Data 2022 — Agents and Brokers

This section assesses data from the 2022 BSCR cyber risk filing returns (Schedule Ve) completed by agents and brokers only.

3.1 Board Oversight of Cyber Risk

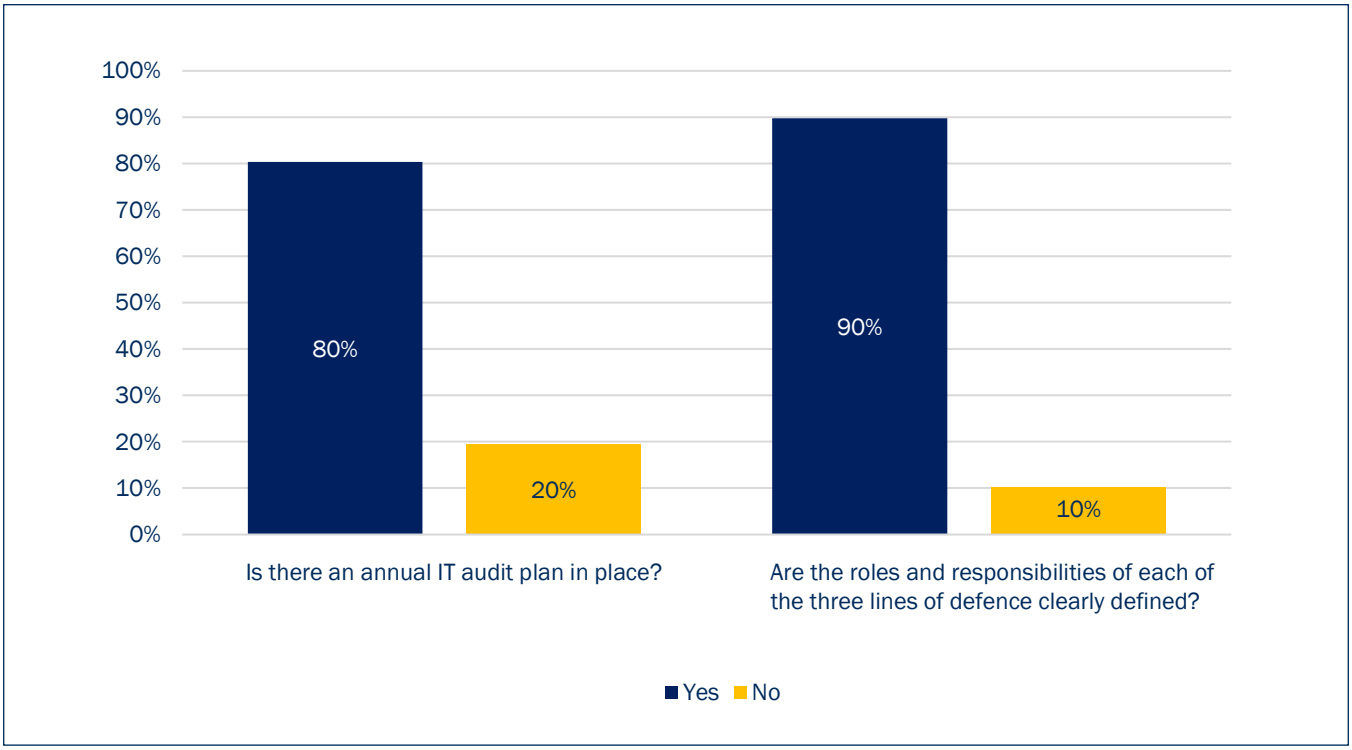


With reference to agents and brokers, 96% confirmed they have regular status updates for the board on their cyber risk management programme and annual review and approval of the cyber risk policy.

The board of directors and senior management team must oversee the cyber risk strategy. In this regard, 92% of agents and brokers reported having board approval for their cyber risk strategy.

The Code mandates that the board of directors and senior management team have oversight and accountability for cyber risk.

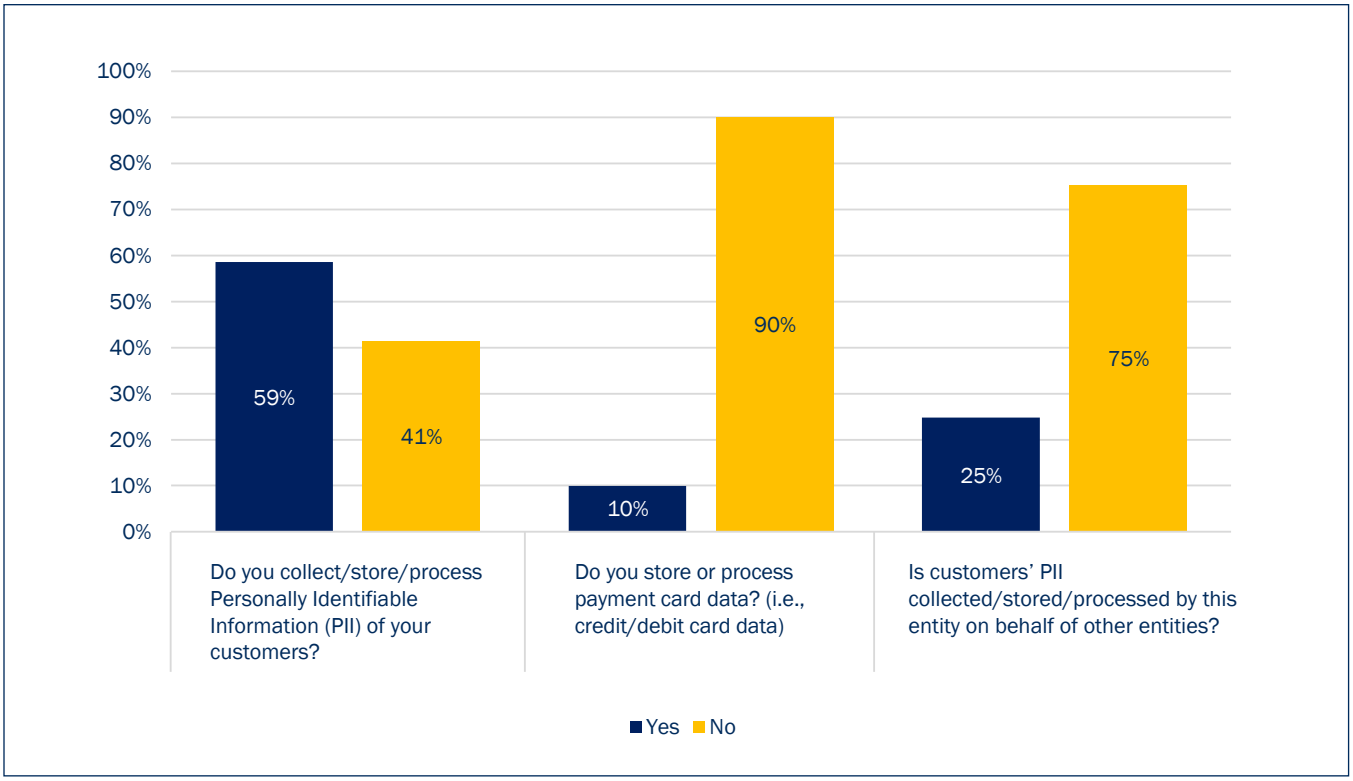
3.2 Three Lines of Defence



Only 80% of agents and brokers have an annual IT audit plan in place. The third line of defence, IT audit, should provide the audit committee of the board (or equivalent) an independent and objective assessment of the effectiveness of controls. An annual IT audit plan is a requirement of the Code. This is noted as an area for improvement.

Consequently, 90% of agents and brokers reported that they have clearly defined roles and responsibilities for each of the three lines of defence.

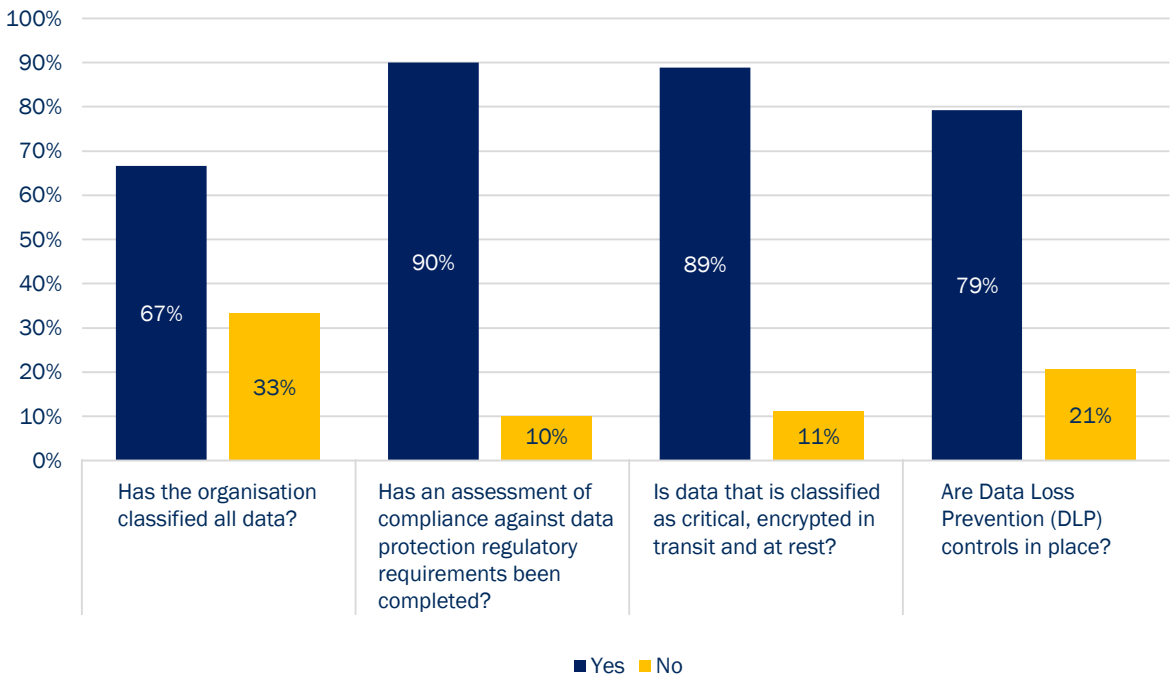
3.3 PII collected, stored and processed



An average of 59% of agents and brokers reported that they collect, store or process PII. It was noted that 10% reported they store or process payment card data.

As per graph 3.3, 25% of agents and brokers reported that they collect, store or process PII on behalf of other entities.

3.4 Data Security Controls



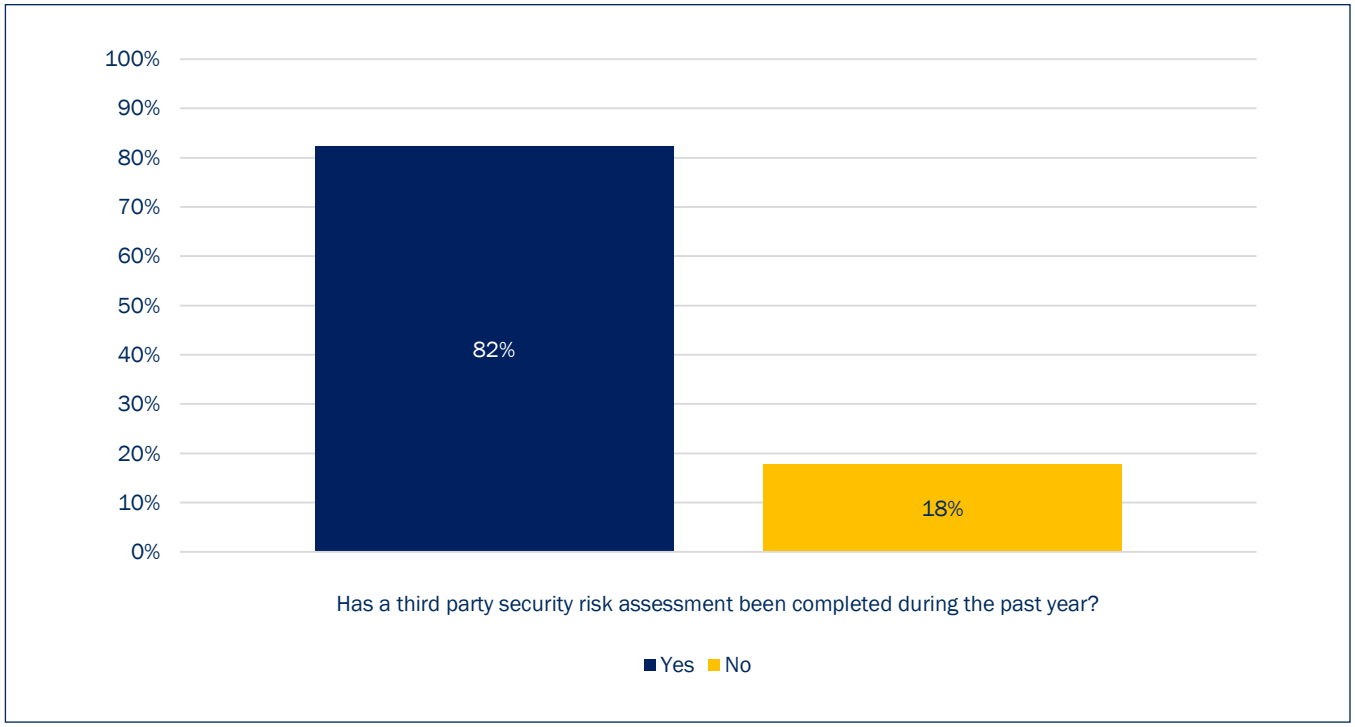
Only 67% of agents and brokers reported that their data had been classified. This is lower than anticipated and is noted as an area for improvement.

In contrast, 90% of agents and brokers have undertaken an assessment against data protection regulatory requirements; however, this has not translated to DLP controls being in place.

In 2022, 89% of agents and brokers encrypt critical data in transit and at rest, while 11% do not. The Cyber Code requires that non-public data is encrypted in transit and at rest. Entities should review their compliance with this requirement.

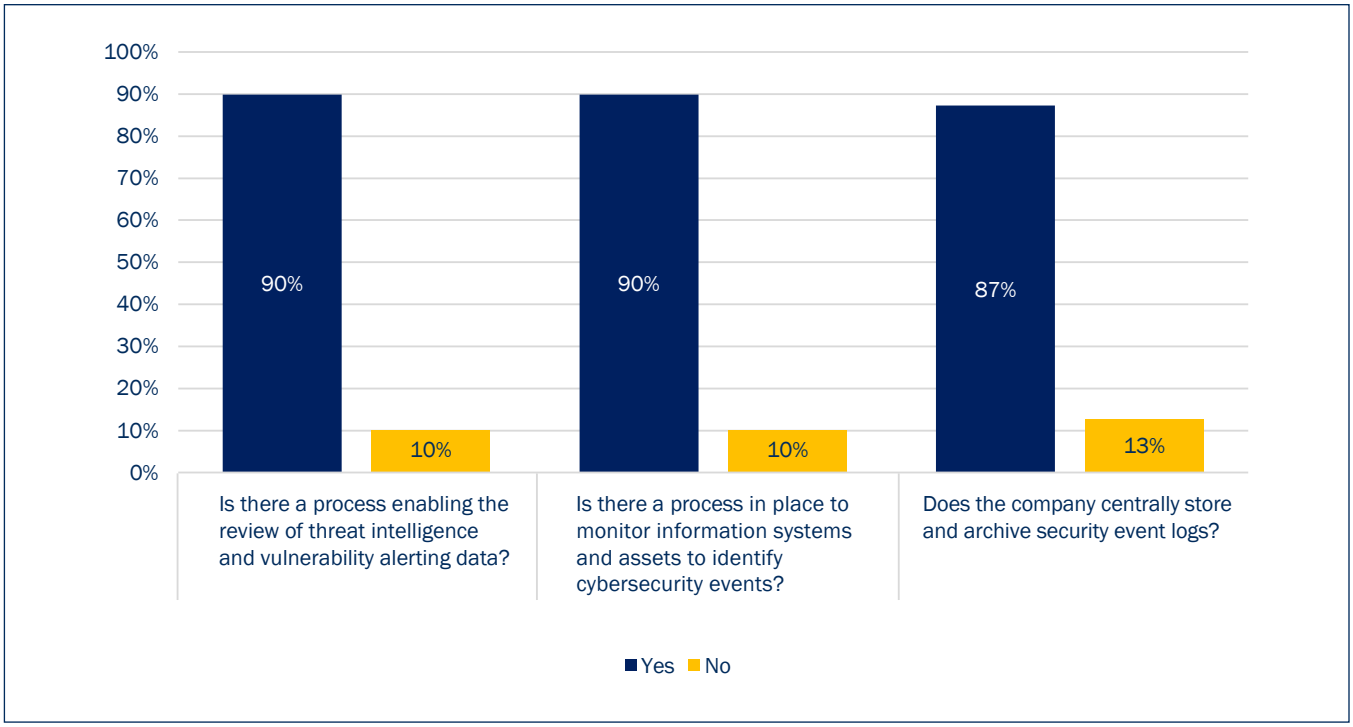
Only 79% of agents and brokers reported having DLP controls in place. This is considered low and agents and brokers should review their risk exposure.

3.5 Third Party Risk Assessment



In 2022, 18% of agents and brokers had not undertaken third-party security risk assessments. Although this service can be outsourced, the risks cannot. The registrant must ensure that there is oversight and clear accountability for all outsourced functions as if these functions were performed internally and subject to the registrant's own standards of governance and internal controls. Third-party risk has been identified as a key area of concern and entities should review the effectiveness of the controls they have in place.

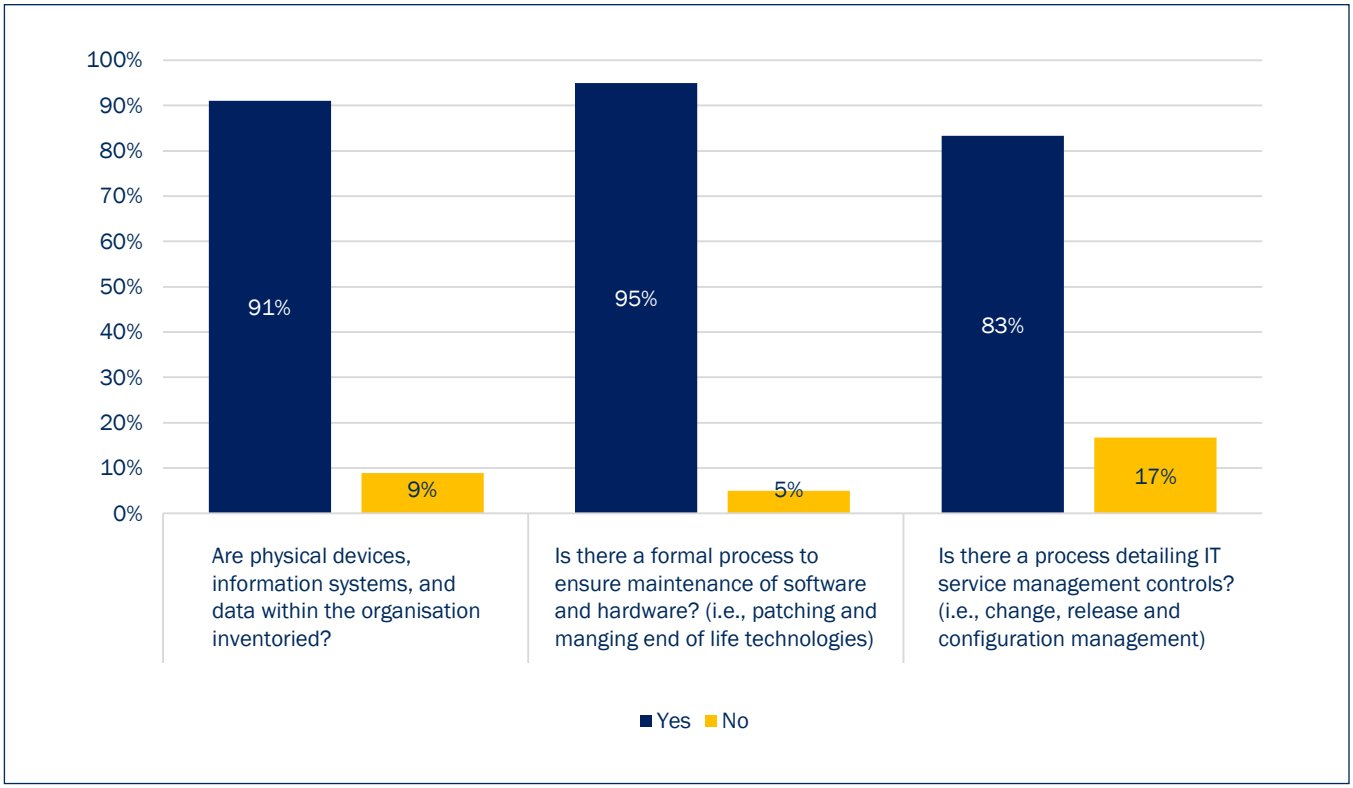
3.6 Detect and Protect Controls — threat intelligence and event monitoring



Although 90% of agents and brokers reported reviewing threat intelligence and vulnerability alerts, 10% of agents and brokers reported that they do not monitor security events. On average, 13% reported they do not have a central archive of event logs.

Security event logs must be available so that they can be monitored as a proactive control measure. If an incident occurs, then an inspection of the event logs may assist in the determination of the route cause. Entities should then ensure they have the ability to monitor, centrally store and archive security event logs.

3.7 IT Service Management Controls

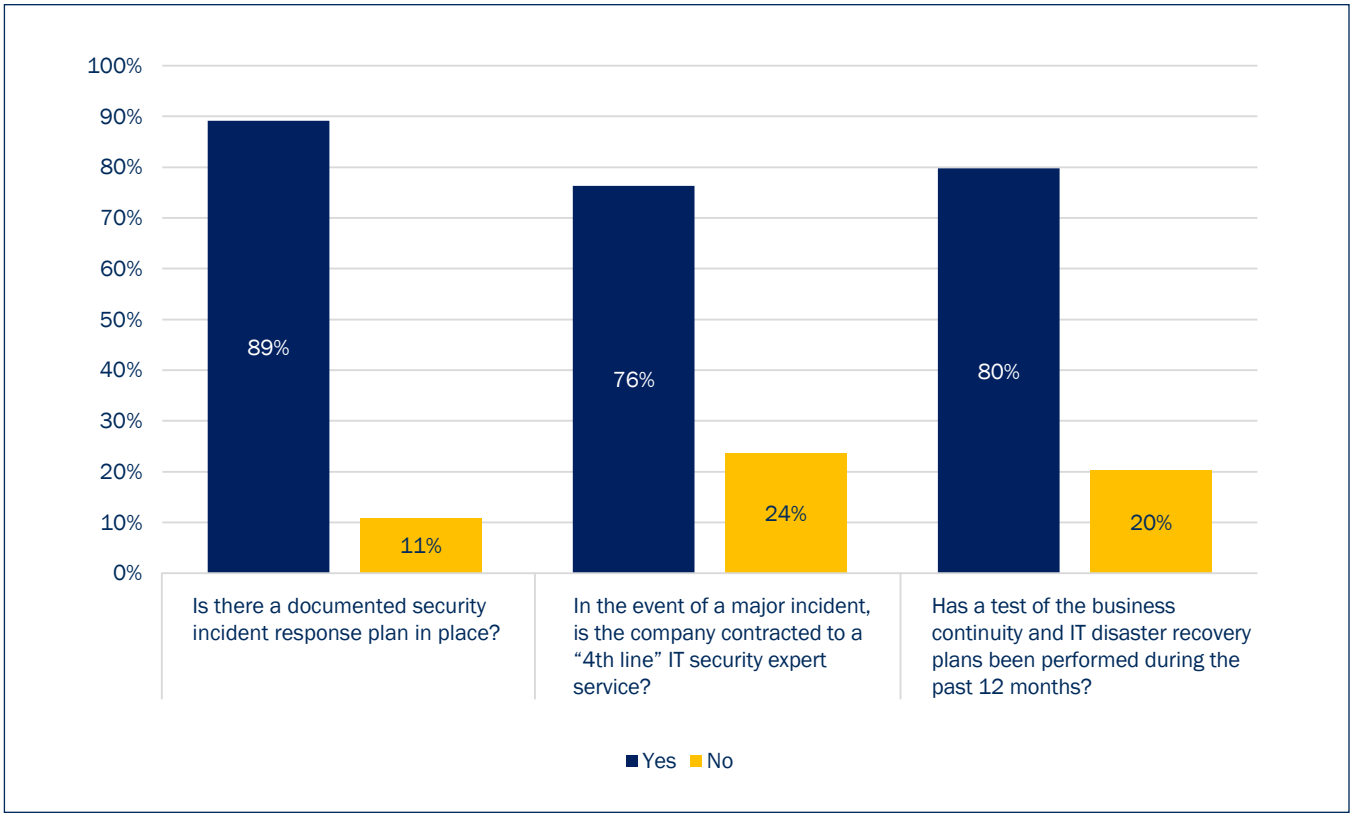


IT service management processes should be in place to assist in managing stable and secure IT systems.

In 2022, 91% of agents & brokers reported having an asset inventory in place, while 95% of agents and brokers reported that they had a formal software and hardware maintenance process in place.

Change, release and configuration management appear to be weak areas for agents and brokers, with 17% reporting that they do not have these controls in place.

3.8 Respond and Recover Controls



The response and recovery control percentages display an area of weakness for agents and brokers. On average, 11% have no incident response plan and 24% are not contracted to an IT security SME to assist with potential major incidents. Furthermore, 20% have not tested BCP and DR over the last 12 months and this is below regulatory expectations.

Conclusion

The Authority continues to engage closely with the insurance sector and the focus on cyber risk will continue in 2024. The key findings in the executive summary list the main control categories that require improvement according to the Authority.

Taking into consideration that the business models and inherent risks differ between commercial insurers, insurance managers and brokers and agents, the report has specific sections breaking down this industry data. Additionally, it provides an analysis of the adequacy of controls per insurer type.

Overall, this report demonstrates that cyber risk management practices across the sector are steadily improving, thereby reducing the probability of incidents that could potentially cause financial and reputational damage to insurers licensed to operate in Bermuda.

Glossary

BCP — Business Continuity Plan

BMA — Bermuda Monetary Authority

BSCR — Bermuda Solvency Capital Requirement

DiD — Defence in Depth

DLP — Data Loss Prevention

DR — Disaster Recovery

Large — LT Large Long Term

Large P&C — Large Property and Casualty

PII — Personally Identifiable Information

SaaS — Software as a Service

Small P&C/LT — Small Property and Casualty and Long Term

SME — Subject Matter Expert

BMA House

43 Victoria Street, Hamilton HM12, Bermuda
P.O. Box 2447, Hamilton HMJX, Bermuda

Tel: 441.295.5278 Fax: 441.292.7471

E-mail: enquiries@bma.bm

www.bma.bm