GIBRALTAR FINANCIAL SERVICES COMMISSION

Insurance Industry Event

Friday 8 March 2024

GIBRALTAR FINANCIAL SERVICES COMMISSION

Conduct Risk Framework Thematic Review

Rowan Humphries, Insurance Conduct of Business Supervision Team

Friday 8 March 2024

Background & Rationale

- At the 2023 Insurance Industry Event, firms were informed that conduct risk was an area of focus.
- The aim was to determine quality of conduct risk framework in place.
- **Five** insurance companies and **three** insurance intermediaries were sampled.

Initial Findings

- Results indicated some poor industry practices in relation to management of conduct risk.
- Some firms have not done enough to embed conduct risk into their controls.
- Findings were used towards setting a standard of expected good practice.
- Lack of focus on following areas:

Desk Based Review

Defining & Capturing Conduct Risk

Two out of eight firms evidenced they had effectively captured conduct risk in their risk registers.

Examples of poor practice	
Generic approach	Some firms who outsourced the drafting and design of its conduct risk framework and conduct risk policy had adopted a generic approach to these risks and had not considered where conduct issues impacted the firm's specific business activities.
Defining conduct risk	Some firms failed to define conduct risk in its Risk Registers or logs and told us that it was captured under its operational risks as a secondary risk.
Accountability	Some firms could not confirm who was responsible for conduct risk nor articulate how conduct related issues would be remediated once discovered.
Transparency	In the absence of a conduct risk framework, specific risks were captured within an overall risk management framework & therefore unable to evidence conduct risk assessment or mitigation.

Conduct Risk Appetite

Two out of eight firms evidenced that they had an existing Conduct Risk Appetite Statement.

Examples of poor practice	
Ineffective measures	Some firms had not set a conduct risk appetite and did not know how to quantify its desired risk appetite and tolerances around conduct.
Misalignment	Firms had established a conduct risk appetite statement, but its content wasn't aligned with how it had defined conduct risk and the controls around these risks.
Lack of implementation	Some firms had defined a level of conduct risk exposure in its risk appetite statement, but this had not been implemented across the firm to help it prevent inappropriate behaviours, therefore, the firm was not measuring whether it was operating within its conduct risk tolerances.
Calibration	Firms had set a conduct risk appetite of 'low' or 'zero' but couldn't explain this in the context of its business activities.

Own Risk & Solvency Assessment

Two out of five firms evidenced that they had considered conduct risk in the ORSA.

Examples of poor practice	
Lack of focus	Some firms did not include conduct risk as a relevant risk in its ORSA.
Poor categorisation	Some firms included conduct risk as a high risk without providing any assessment as to why this was a key risk in the ORSAs.
Failure to embed	In some circumstances we were unable to determine the true position on conduct risk. For example, where it had been addressed in the ORSA but with no other reference to conduct risks in any of their policies or processes.

Management Information/Key Performance Indicators

Two out of eight firms evidenced that they had produced MI or KPI's specific to conduct risk

Examples of poor practice	
Inaccuracy	When reporting to different committees, some firms' complaints MI had disparities.
Poor processes	Lack of procedure for examining the MI obtained for conduct risk meant that vital information and essential corrective measures were missing from Board or Committee meetings.
Ineffective review period	MI should be produced, monitored and provided to the relevant committee, however, some firms only obtain and review MI on an ad-hoc or infrequent basis, or once an issue has arisen.
Ineffective dashboard management	Firms had included conduct dashboards in committee packs but failed to evidence review or escalation of out of tolerance KPIs.

Governance

Four out of eight firms could evidence that their Board & Senior Management had oversight of conduct risks

Examples of poor practice	
Lack of record keeping	Firms told us they were discussing conduct risks at Board level but were not able to evidence this in the meeting minutes they then sent.
Sole focus on commercial	Committee and Board meeting minutes demonstrated that customer interests and conduct risk issues were not a priority compared to the commercial interests of the firm.
Poor prioritisation	Tick-box approach to conduct risk, evidenced by a lack of prioritisation in any reporting. Therefore, a lack of opportunity to escalate to the Board or Senior management.

Key Take Aways

1. Claim of effective conduct risk management but little substance.

2. Commercial Committees in charge of conduct risk or Consumer Duty.

3. Conduct risk and consumer outcomes have been treated as a tick-box exercise, and very much an after-thought.

4. Stronger focus required on conduct – new opportunity through Consumer Duty.

GIBRALTAR FINANCIAL SERVICES COMMISSION

Consumer Duty - Suggested Areas of Focus

Amanda Eccleston, Director of Authorisations and Conduct of Business

Fair Value

- At launch/significant adaptations – consider S83a.
- Reliance on co-manufacturers for FV assessment.
- Agreements -clarification of specific information requirements and frequency for the purposes of enabling FVAs.
- Not looking along the whole distribution chain - your responsibility as an insurer.
- Show how distribution supports and not adversely affects FV.
- Correct metrics being used - using full and necessary data.
- Lack the detailed analysis – unevidenced statements.
- Foreseeable period/length of product and at renewal – insured risk, expected claims.
- Products under scrutiny.
- Governance/Committees - lack of evidence of discussions around consumers/focus on financial performance.

Key take aways – Fair Value

- Data without analysis achieves nothing.
- Detailed assessments – look back, compare – reporting since 2021.
- Why have you reached conclusion/satisfied.
- Comparison of overall price to customer and the benefits and services provided.
- Appropriate challenge.
- Any product adaptations, remediation or action taken to address harm.
- Evidence is key.

Customer support

- Filters through everything – overarching, considered through all interactions.
- Implementation plan – customer journey, touch points, but ongoing.
- Clear signposting of support available – GFSC receiving calls.
- Processing renewals and claims on same basis as sales.
- Measuring – on-going monitoring of quality of support, metrics used.
- Vulnerable customers – cost of living, financial vulnerability, adjustments made, channels.
- Incidents reported – vulnerable customers, consider in all comms, issues.
- S83a – assessments.
- Outsourced services.

Customer support - Complaints data companies 2023 return

Reason	No. complaints
Customer service (general)	
Claim (quality of repair or service)	
Customer service (delay)	
Other	
Claim (unsatisfactory settlement)	
Policy (pricing)	
Claim (declined due to lack of cover)	
Customer service (client account accessibility)	
Renewal (unwanted)	
Renewal (pricing)	
Claim (declined due to misrepresentation or non-disclosure)	
Policy (details incorrect)	
Policy (lack of understanding)	
Policy (misleading wording)	
Renewal (timing)	

Governance – Annual Board Report

- Not a one off - fully embedded on day-to-day basis.
- Honest assessment – all four outcomes.
- MI, assessments, monitoring used to support, three lines of defence.
- Remedial action taken, further plans for improvement.
- Future strategy is consistent with the outcomes, customer centric.

Governance – Annual Board Report

Analysis

Challenge

Evidence

GIBRALTAR FINANCIAL SERVICES COMMISSION

Conduct of Business Supervision – 2024 Focus

Amanda Eccleston, Director of Authorisations and Conduct of Business

2024 Focus

- Consumer Duty Gibraltar.
- Consumer Duty thematic review.
- Conduct return 2023 output.
- Risk assessments and actions (in line with Prudential team).
- Published feedback.

GIBRALTAR FINANCIAL SERVICES COMMISSION

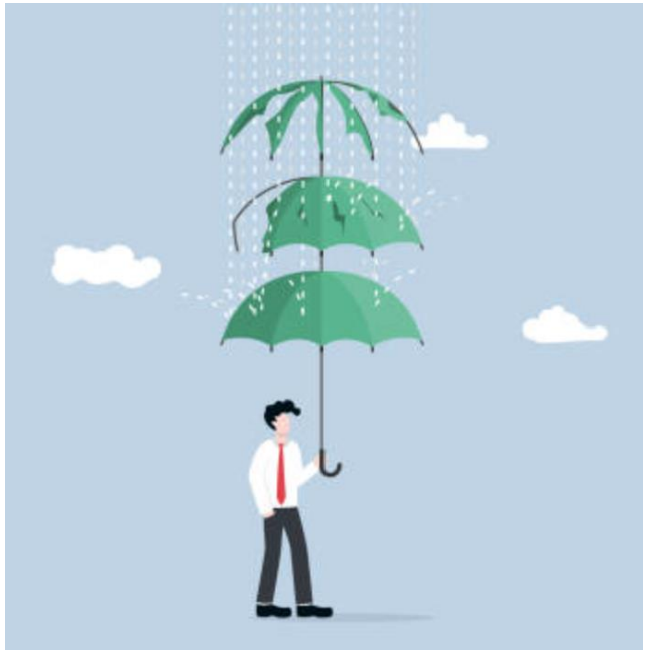
General Policy and Operational Resilience Regulatory update

Julian Sacarello, Head of Policy

08 March 2024

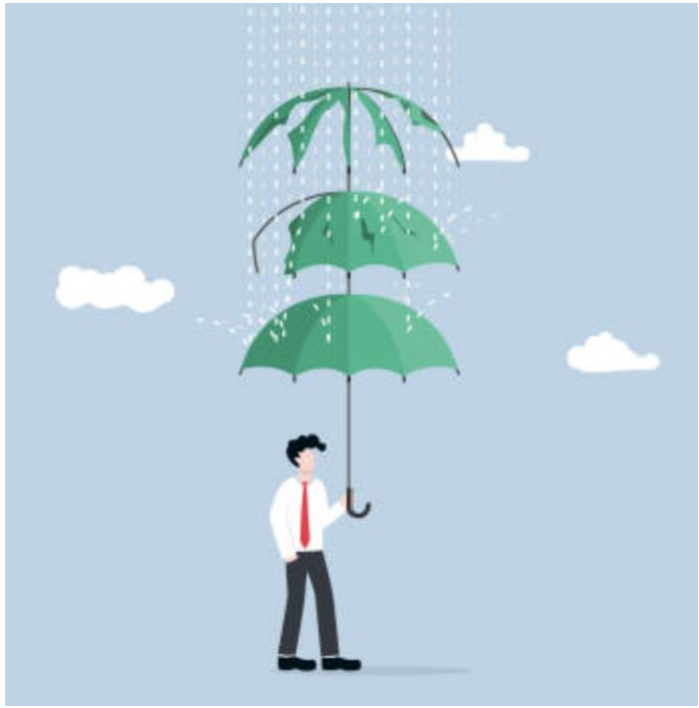
General Policy update

- GAR work continues to be our priority.
- Direct work to establish the regime working with GoG, HMT and the UK Regulators.
- Indirect work to ensure Gibraltar's framework (law/guidance) remains aligned with the UK in the interim period.



Recap

- Operational Resilience Regulations came into force in July 2023.
- We will soon be publishing a GFSC Operational Resilience Guidance note.
- By July 2024, firms must comply with the requirements.
- By July 2026, firms must demonstrate they can remain within IT for their Important Business Services.



Implementing Operational Resilience

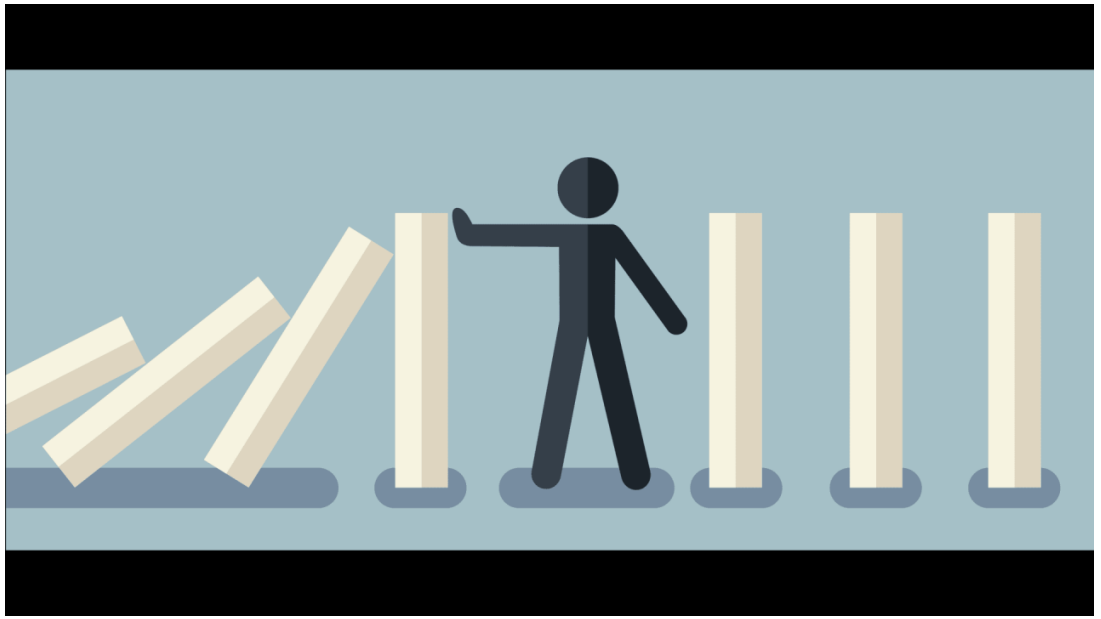
- Firms should have identified their important business services and set impact tolerances for each.
- Mapping and scenario testing programme should also have commenced.
- Firms' approaches need to acknowledge failures are inevitable.
- Mapping should include all critical resources and consider internal and external dependencies.
- Mapping and scenario testing should evolve.

Scenario Testing

- Scenario testing must assume disruption has occurred.
- Failures of backup arrangements and cases where multiple parts of organisation are disrupted should be included.
- Testing needs to be appropriate and robust – the higher the potential impact of disruption, the less likely that desktop testing will be sufficient.
- Senior Management and Boards need to be involved.

Building Resilience

- Resilience can be achieved in different ways – the regime is outcomes-focused.
- Firms should consider building in substitutability to services, reviewing and adapting outsourcing arrangements, and re-building or replacing legacy systems.
- Completing mapping and testing earlier will allow more time to address vulnerabilities and build resilience.



GIBRALTAR FINANCIAL SERVICES COMMISSION

Operational Resilience -Thematic Reviews

Kristian Menez, Director of Prudential Supervision

The aim of Thematic Reviews

- Thematic reviews aim to understand and assess the level of systems, processes and controls in a particular aspect of an entity.
- They are helpful in informing the regulator of how a cross-section of firms operate and discharge their regulatory obligations.
- Thematic reviews are useful as they allow for clear benchmarking performance.
- They can help provide meaningful feedback to firms on areas for improvement.
- They usually result in industry reporting on good and poor practices in particular areas, aiding improvements and understanding.

Operational Resilience Thematic Review

A Desk Based Thematic Review

Areas that will be covered by the thematic will include a review of:

- The important business services identified by the firm.
- The impact tolerances set and justification for these.
- The mapping of the IBS to people, processes, technology, data and facilities.
- The vulnerabilities identified.

Operational Resilience Thematic Review

A Desk Based Thematic Review (continued)

- The firm's plan for scenario testing.
- Any lessons learnt exercises or scenarios.
- How the plan was considered and approved by the Board.
- The interaction between the operational resilience and financial resilience assessment.
- The interaction between operational resilience and the BCP.

The thematic will commence post implementation date on 13/7/2024.

GIBRALTAR FINANCIAL SERVICES COMMISSION

Oversight of Pricing, Underwriting and Claims

Monika Sookhee, Head of Insurance Supervision

Thematic Areas to be Reviewed

- The GFSC is looking to conduct thematic reviews in the following areas this year:

  Outsourcing which will cover oversight of:

  - Delegated underwriting and pricing.
  - Oversight of claims outsourcing.
  - Oversight of IT, Data and Cyber security.

Pricing and Underwriting

This area has been selected for a thematic review due to the number of firms operating a delegated underwriting model

Areas that will be covered by the thematic review are:

- Board and Committee oversight.
- MI provided to the Board and other Committees.
- Governance of pricing models.
- Pricing controls.
- Underwriting controls.
- Use of internal audit or validation checks.
- Interaction with the actuarial function.
- Consideration of business strategy.

Pricing and Underwriting

Board and Committee oversight

Aims: To understand and assess

- The Governance and Underwriting Committee structure.
- Whether the documentation and oversight is appropriate.
- The quality of the information packs and minutes.

MI provided to the Board and committees

- Understanding the controls and validation performed on data in the packs provided to the Committees.

Pricing and Underwriting

Governance of pricing models and pricing controls

Aims: To understand and assess

- The governance and controls over pricing models.
- How pricing models are used in the business.
- The data available to support changes and how changes are made.
- How data integrity is managed.
- Delegation of pricing decisions.
- The limits and monitoring of discounts.

Pricing and Underwriting

Underwriting controls

Aims: To understand and assess

- The governance and controls over underwriting guidelines.
- The data available to support changes and how changes are made.
- How data integrity is managed.
- How oversight of underwriting is conducted.

How internal audit is used in underwriting and pricing

- Aims to understand how firms used internal audit in this area and the frequency of reviews.

Pricing and Underwriting

Interaction with the actuarial function

Aims: To understand and assess

- The role the actuarial function plays within the firm.
- How the actuarial function is used to assess pricing and underwriting.
- The analysis conducted over the preceding periods in arriving at the AFH opinion.

Consideration of business strategy

- Aims to understand and assess how the results of pricing and underwriting are considered in business strategy.

Oversight of Claims Outsourcing

Assessment of oversight of claims

Aims: To understand and assess

- The Board and Claims Committee structure.
- Whether the documentation and oversight is appropriate.
- The quality of the information packs and minutes.
- The type of KPI data considered.
- How internal audit is used and the frequency of reviews.

Next steps on Thematic Reviews

Timing

- We will be writing to firms in Q2 2024 to start the process of the information requests.
- Timing of visits and information requests will be agreed with firms in scope on a case-by-case basis.
- Aim to complete the reviews by December 2024, with feedback to follow in Q1 2025.

GIBRALTAR FINANCIAL SERVICES COMMISSION

Supervision of Technologies – The new norm

Alan Pereira, Chief Information Officer

The GFSC Supervisory Landscape

- Supervisory landscape constantly changing.
- Conventional supervision adapting to technological change and reliance.
- Firms become reliant on technology and regulators need to adapt to change.
- Old supervisory threats of Governance and financial prudence, etc.
- Technology governance and controls now an important part of landscape.

Rapid Growth

- Technology's rapid growth and impact on various financial industries.
- Need for effective regulation and supervision to ensure ethical and responsible use and implementation of technology for all financial industry firms.
- The need for the GFSC to monitor and supervise technology, resilience, security, cyber and governance and control for all regulated entities as part of its licencing regime.

Why Regulator Supervision

- Potential risks and negative consequences of unchecked technology.
- Protecting consumers, privacy and data security (GDPR overlap). Data Breach notification under PSD II (Payment Service Directive) is one of many examples.
- GFSC protects consumers and jurisdiction.

Areas of Regulation

Data Privacy and Security

Ensuring compliance with data protection regulations

- Safeguarding sensitive personal information.
- Implementing robust security measures.

Consumer Protection

- Monitoring for fraudulent practices and scams.
- Enforcing fair business practices and transparency.
- Addressing consumer complaints and disputes.

Areas of Regulation

Technological Advancement

- Keeping up with rapidly evolving technologies.
- Understanding complex technical aspects.

Global Nature of Technology

- Cross-border implications and jurisdictional challenges.
- Collaborating with international regulators.

Balancing Innovation and Regulation

- Encouraging innovation while mitigating risks.
- Avoiding stifling technological progress.

GFSC Approach

- 2015 we started implementing change introducing tech supervision in banking.
- 2016 saw further guidance and more supervision through the CIO role.
- 2018 DLT landscape introduced a principles-based approach (10 in total).
  - Principle 7 – Systems and Security
  - Principle 9 – Resilience
- Changed the landscape of supervision around Security, Cyber and Resilience.
- Guidance which is transferable across all sectors for Technology Supervision.
- 2020/21 Other sectors included in the approach.
- 2023 New Insurance applications in scope.

GFSC Principles Approach

Guidance 7 – Systems and Security

- Cybersecurity & IT Vulnerabilities
  - Management of risks.
  - Keeping systems safe.
  - MFA and security measures.
  - Disaster recovery.

GFSC Principles Approach

Guidance 7 – Systems and Security

- Board of Directors and / or Senior Management
  - ensuring ethical data and security governance is kept.
  - having good cyber risk management culture and practices.
  - aligning of business strategic objectives with information and communications technology (ICT) objectives.
  - having adequate cybersecurity budget and resourcing.
  - management of the firm's cybersecurity controls and frameworks through adequate periodic testing and reporting.
  - ensuring all cyber controls are disseminated throughout all areas servicing the firm's operational model.

GFSC Principles Approach

Guidance 7 – Systems and Security

- Information Security
  - Appointment of key technology individual.
  - Information Security and Cybersecurity Policies and control.
  - Security measures should meet industry standards (benchmark).
  - Segregation of authoritative controls and Privileged accounts.

<u>The nominated person should ensure that:</u>

- users are adequately kept informed about potential cyber risks and threats. Education of staff on security and cyber risk is important.
- the controls, processes and policies are understood and followed by all those involved in a firms day to day business.
- appropriate user and device credentials are maintained. Strong passwords and keys should be used when logging into hardware or software platforms. The use of all high privileged credentials should be kept to a minimum and adequately logged; and
- appropriate Cyber Training and Cyber accreditation is obtained/achieved.

GFSC Principles Approach

Guidance 7 – Systems and Security

- It is good practice to follow industry standards in cyber and security founded on the following:

  - ISO 27001 Security Policies.
  - the National Cyber Security Centre's website : www.ncsc.giv.uk/guidance/10-steps-cybersecurity.
  - National Cyber Security Centre (NCSC) approach and benchmarks.
  - Cyber Security Information Sharing Partnerships (CiSP): www.ncsc.gov.uk/cisp.

GFSC Principles Approach

Guidance 7 – Systems and Security

- ICT Governance

These should comply with ICT requirements, ensuring that the relevant cyber requirements are embedded in its security protocols, including:

  - strong IT governance allowing the management of IT risks with adequate process to adjust these
  - as and when required.
  - adequate procedures and policies to mitigate potential cyber or security attacks or leaks with these being updated regularly to accommodate the ever-changing landscape evolving around cyber security.
  - clearly defined roles and responsibilities around ICT infrastructures with clearly demarcated segregation and adequate levels of access around all areas of systems; and
  - integration of processes and procedures into the risk framework methodology.

GFSC Principles Approach

Guidance 7 – Systems and Security

- ICT Governance
  - Incident Handling.
  - Patch Management.
  - IT Governance Framework for IT and Business Strategies (International Standard for corporate governance of IT is ISO/IEC 38500:2015).
  - Standards are used as a benchmark and measure and accreditation is not required so long as the standards are followed and applied and properly documented and evidenced.

GFSC Principles Approach

Guidance 7 – Systems and Security

- Independent Assessments and Tests
  - Whitebox testing - Full information about the target is shared with the testers. This type of testing confirms the efficiency of internal vulnerability assessment and management controls by identifying the existence of known software vulnerabilities and common misconfigurations in an organisation's systems.

  - Blackbox testing - No information is shared with the testers about the internals of the target. This type of testing is performed from an external perspective and is aimed at identifying ways to access an organisation's internal IT assets. This more accurately models the risk faced from attackers that are unknown or unaffiliated to the target organisation. However, the lack of information can also result in vulnerabilities remaining undiscovered in the time allocated for testing.

- Cloud Computing and firms use and compliance of new technologies
- Generative AI and its uses

GFSC Principles Approach

Guidance 9 – Resilience

- Business Continuity Management
  - Risk Assessments.
  - A Business Impact Assessment (BIA) considering the risks and likelihood of potential disruptions to the continuity of operations.
  - The creation of a Crisis Management Team (CMT), Business Continuity Plan and Disaster Recovery Plan in accordance with industry standards (ISO 22301).
  - Adequate documentation on the strategic approach to be taken in order to maintain the continuity of its operations in the event of a failure, inclusive of recovery operations to achieve this.
  - Adequate internal and external Communications Strategies and Plans.
  - Regular testing of BCP and DR arrangements (at least bi-annually), including an adequate test run(at least annually). All tests need to be documented and logged with any findings.
- Disaster Recovery Planning also required (Pandemic Example)

GFSC Principles Approach

Guidance 9 – Resilience

- Change Management

Risks and potential security vulnerabilities can occur when changes are made to processes and procedures that might impact an organisation's operations. For this reason, we expect DLT Providers to have adequate change management processes in place taking into account the following:

  - an impact assessment of any proposed changes.
  - a migration or change plan.
  - rollback processes.
  - detailed plan on how the testing of any change is to be conducted; and
  - a backup plan.

GFSC Principles Approach

Guidance 9 – Resilience

- Testing
  - Comprehensive functional and security testing should be carried out before systems are made operational and subsequently performed at suitable intervals proportionate to the size and structure of a DLT Provider's operations. This should include physical security, IT security and cybersecurity.

- Systems recovery
  - Backups looked into including the use of immutable backups, offline storage and multiple backup solutions.
  - Regular testing and recovery plans.

Data Backup Strategies

Ensuring you are able to recover

- The need to ensure firm controls ”their” data.
- The need to ensure adequate systems and controls are in place and remove hold of data by Brokers.
- Approach is a proven methodology applied to other sectors for many years Interdependencies in systems will be looked into and firms expected to meet regulatory obligations.
- Staged approach to implementation – although new firms coming into jurisdiction already being put through the new approach.
- Giving 9 months for firms to adapt to the change.
- Trigger Events such as material changes to their business may instigate process sooner with CIO assessment.

GFSC is also evolving

The impact of technology on regulated entities is “now” and the GFSC is ensuring we adapt to the ever-changing landscape of firms so we can perform our regulatory responsibilities monitoring Systems, Data, its use and controls, Cyber and Technology footprints.

Ensuring the consumers and jurisdiction is protected !

GIBRALTAR FINANCIAL SERVICES COMMISSION

Supervisory Approach – Insurance BAU Team and Intensive & Systemic Firms Supervision

Monika Sookhee, Head of Insurance & Oliver Spicer, Head of Intensive & Systemic Supervision

Insurance BAU Supervisory Approach

- Risk based approach, underpinned by the GFSC risk framework.
- Firms are tiered based on their impact.
- We then consider likelihood of risks materialising to assign an overall residual score.
- All firms have a risk assessment at intervals that are based on their impact to the jurisdiction, or when a trigger event occurs.
- The risk assessment forms the basis of the supervisory tasks for those firms.
- We will aim to spend 25% of our time doing thematic work. This will consist of onsite review and desk-based supervision.
- Firms that are inherently very impactful are invited for annual meetings where we go through a defined agenda on the business plan, risks to the firm. We will review key documents such as Board packs from the firm and use our supervisory tools to review the ongoing reporting of the firm.

Systemic Firm Supervision

- Firms writing in excess of £650m Gross Written Premium.
- Allocated supervisors and additional oversight by GFSC panel.
- Supervisory plan aligned to UK for equivalent size and market share.
- Annual supervisory plan includes:
  - Meeting with all relevant regulated individuals on an annual basis.
  - Meeting with Executives and Non-Executive Directors quarterly.
  - Monthly and firm-specific reporting.
  - Board and committee pack reviews.
  - Review of business plans, ORSA.
  - Group supervision and peer analysis.

Intensive Supervision

- Firms operating outside of GFSC risk appetite.
- Overall objective to bring firm within GFSC risk appetite and to protect consumers.
- Firms transferred to IST following the formal agreement from the relevant industry panel and recommendations made by supervisory team.
- Oversight provided by allocated supervisors, subject matter experts and GFSC panel.
- Core strategy is to understand, plan and implement one of “3Rs”.
- These are Remediate, Replace (transfer) or Run-off (cessation).
- Supervisory plan tailored to the risks of the firm.

GIBRALTAR FINANCIAL SERVICES COMMISSION

Prior year areas of focus - Update

Oliver Spicer, Head of Intensive & Systemic Supervision

Areas of Focus

- Inflation.
- Group Supervision.
- Premium Debtors.
- Claims Reviews.
- Reinsurance & Sliding Scales.
- Regulated Individuals.

Questions

Comments