ISLE OF MAN FINANCIAL SERVICES AUTHORITY

The Role of the Head of Compliance /Compliance Officer

22 October 2024

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Corporate Governance Objectives

- Compliance with statutory objectives
- Management of Risk
- Aligning of the interests of Stakeholders
- Management and control systems
- Balancing of power and responsibility within the board

Join the discussion on Slido – #FSACOL2024

Role of the Board

- Approve the business strategy
- Approve and oversee an adequate and effective internal control framework
- Approve and oversee risk appetite strategy
- Corporate governance principles and values/standards of conduct (“tone at the top”)

Join the discussion on Slido – #FSACOL2024

Role of the Senior Management

- Manage the daily operations, soundly (and prudently)
- Implement appropriate systems
- Individuals should have necessary skills and experience

Join the discussion on Slido – #FSACOL2024

Role of Risk Management

- Identifying, measuring, monitoring, controlling or mitigating, and reporting on risk exposures.
- Establish and maintain comprehensive policies
- Larger organisations have different splits of responsibilities.

Join the discussion on Slido – #FSACOL2024

Role of Compliance

- Identify and understand the legal and regulatory obligations
- Compliance strategies, policies, procedures and training
- Foster a sound compliance culture
- Proactive engagement with the Board

Join the discussion on Slido – #FSACOL2024

Compliance Roles within an organisation

- The Board of Directors - overall responsibility & tone setting
- Management - maintaining compliance day to day
- All employees - obligation to follow the policies and procedures and act with integrity.
- Compliance is a governance function

Join the discussion on Slido – #FSACOL2024

Authority of Compliance

- Board of Directors establish the authority and responsibility
- The Head of Compliance - develop more detailed processes/responsibilities as appropriate.
- The Compliance function:
  - ✓ review all areas and to have full, free and unrestricted access
  - ✓ initiate and manage investigations on potential compliance breaches.
  - ✓ direct and timely access to all management and the Board of Directors.

Join the discussion on Slido – #FSACOL2024

Fitness & Propriety ("F&P")

- Comparable with similar jurisdictions
- Protect consumers
- Prevent controllers engaged in criminal activity
- Protect the reputation of the Isle of Man
- Flexible - where appropriate
- Review each application on its own merits
- Review multiple factors top build an overall picture

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Head of Compliance – "HoC"

5 Key components:

- Identification
- Prevention
- Monitoring and detection
- Resolution
- Advisory

Covers core elements such as:

- Developing and Implementing Policies and Procedures
- Monitoring Compliance
- Identifying Potential Risks
- Acting as a Liaison
- Educating and Training Employees – all levels

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Head of Compliance – Key Skills

- Regulatory & Technical Knowledge
- Communication
- Critical thinking
- Problem-Solving
- Leadership
- Integrity
- Analytical Skills
- Adaptability
- Collaborative
- Proactive

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Reporting – HoC

- Compliance Monitoring
- Breaches
- Mapping
- Regulatory inspection findings
- Key risks / business focus
- Horizon Scanning
- Material correspondence with the regulator(s)
- Complaints
- Risk trends & data
- Periodic review statistics
- Legal and Regulatory issues
- Capacity

Join the discussion on Slido – #FSACOL2024

HoC – Common Problems

- Lack of authority
- Intimidation by more senior members of an organisation
- Lack of adequate resources
- Inadequate level of awareness and training among staff of internal policies and obligations
- Lack of attention to reporting at senior and board level
- Commercial objectives v Compliance
- Poor record keeping
- Challenging poor senior management.

Join the discussion on Slido – #FSACOL2024

MLRO/DMLRO

5 Key components:

- Identification
- Prevention
- Monitoring and detection
- Resolution
- Advisory

Covers core elements such as:

- Developing and implementing the AML/CFT framework
- Monitoring and reviewing compliance with AML/CFT legislation
- Identifying Potential risks
- Reporting
- Acting as a Liaison
- Educating and Training Employees - all levels

Join the discussion on Slido – #FSACOL2024

MLRO – Key Skills

- Regulatory & technical knowledge
- Product and service knowledge
- Typical customer profile
- Ability to recognise potential suspicious activity
- Integrity
- Analytical skills
- Research skills
- Communication skills
- Approachability
- Confidence
- Decisiveness

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

MLRO – Main responsibilities:

- Have sufficient seniority and authority within the business
- Have sufficient time and resource for the role
- Have direct access to the officers of the firm
- Receive and evaluate internal SARs
- Document SAR cases e.g. a file note of actions taken
- Maintenance of a SAR Register
- Maintenance of a Register of Enquiries (or equivalent)
- Access available information from internal and external sources
- Make external reports to the FIU as necessary
- Act as a main point of contact with Competent Authorities
- **Act autonomously**

Join the discussion on Slido – #FSACOL2024

Reporting – MLRO

At least annual, direct to the Board:

- SAR figures and analysis
- PEPs – figures and analysis
- Sanctions – breaches, blocked/frozen accounts or assets
- AML/CFT material breaches
- AML/CFT regulatory update

Join the discussion on Slido – #FSACOL2024

MLRO - Common Problems

- Lack of authority
- Intimidation by more senior members of an organisation
- Lack of adequate resources
- Inadequate level of awareness and training among staff of AML/CFT/CPF
- Internal staff VS. customers in SAR cases
- Poor recordkeeping
- Challenging senior management.

HoC & MLRO – Responsibilities

- Compiling MI
- Provide regular reporting on matters arising
- Raising awareness money laundering typologies
- Horizon Scanning
- Monitoring the internal effectiveness of the procedures
- Awareness of sanctions
- Training for staff – regulatory and AML/CFT/CPF
- Being accessible
- Regulatory meetings and inspections
- Communication with the Regulator & Competent Authorities

Join the discussion on Slido – #FSACOL2024

HoC & MLRO – Independence

1. Independence and Autonomy
2. Confidentiality
3. Focus and Specialisation
4. Conflict of Interest
5. Regulatory Expectations

Join the discussion on Slido – #FSACOL2024

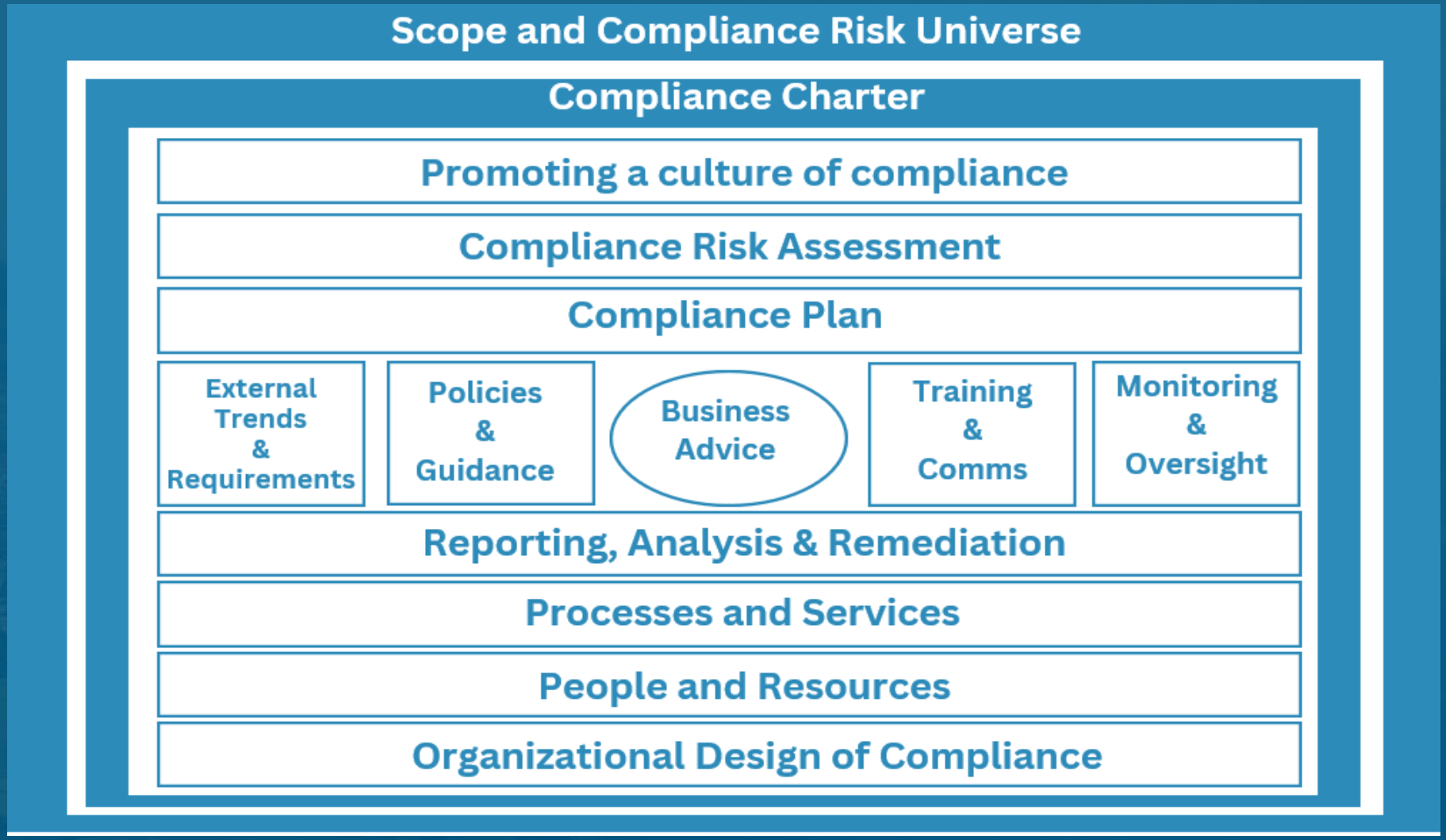
ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Operating Principles of Compliance

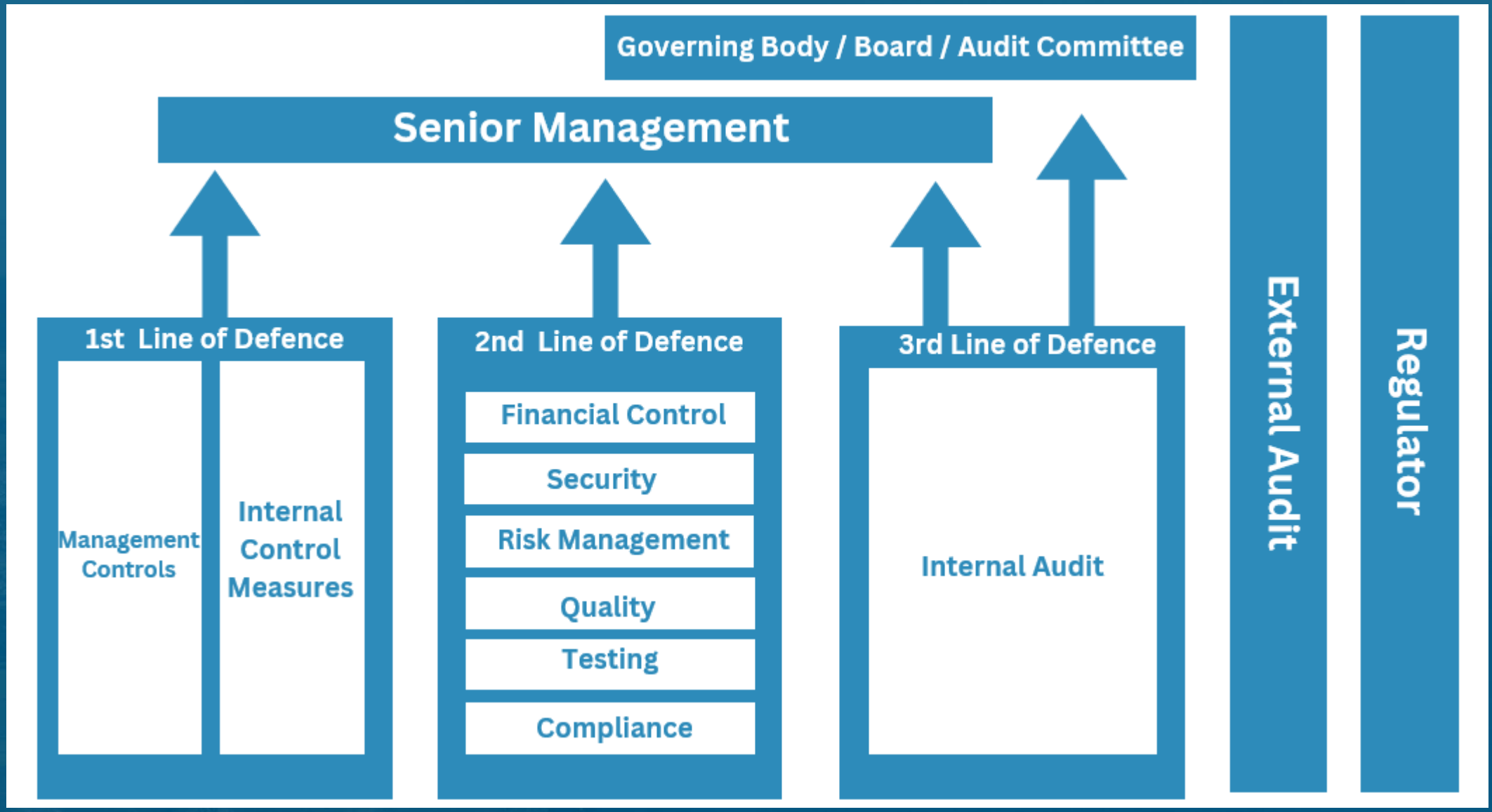
- Remain objective
- Clearly distinguished
- Risk-based approach
- People & Resources
- Organisational Design of Compliance
- Policy Approval

Join the discussion on Slido – #FSACOL2024

Compliance Framework



3 lines of Defence



ISLE OF MAN FINANCIAL SERVICES AUTHORITY

First Line of Defence: Operational Management

- **Role**: Owns and manages risks.

- **Responsibilities**:
  - ✓ Implementing and maintaining effective internal controls
  - ✓ Control procedures
  - ✓ Identifying and managing risks directly

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Second Line of Defence: Risk Management and Compliance

Role: Oversees risk management and compliance.

Responsibilities:

- Risk management frameworks and policies
- Monitoring compliance
- Providing guidance and support to the first line
- Risk assessments and testing
- Identifying and managing risks directly

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Third Line of Defence: Internal / External Audit

Role: Provides independent assurance.

Responsibilities:

- Evaluating
- Reporting findings
- Effective functioning of 1st and 2nd lines

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Compliance Monitoring Plan

- HoC develops a Compliance Monitoring Plan (“CMP”)

- Core areas to include in the plan are:
- Perceived regulatory or reputational focus and or risk
- Areas or issues of high risk
- Financial Crime risk

- Demonstrates active and continuous compliance

- Findings evidenced by good record keeping

- Breach identification, recording and reporting

- Remediation of findings by 1st Line.

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Compliance Monitoring

- Must have:
  - ✓ An effective and sound methodology
  - ✓ Clear objectives
  - ✓ Clear evidence that it is rigorous
  - ✓ A clear timescale for remediation of issues
  - ✓ An escalation process to senior management
- Built into the process that it is designed to control.
- Embedded element of a technology-based process
- Physical checking of documentation and transactions
- Self-assessment reports or internal control questionnaires

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Compliance Monitoring

- Must be “preventative” and “detective”
- ‘Detection’ - any management activity which can identify
- Potential breaches of the rules, but which in itself can do nothing to drive behaviour that is inherently compliant; it identifies weaknesses that have already occurred and is therefore related to the past.
- ‘Prevention’ actively influences the outcome, or the organisation’s adherence to regulatory requirements; it is related to the present.

Join the discussion on Slido – #FSACOL2024

Examples of Preventative v Detective

Prevention

- F&P
- Inductions
- Training
- Feedback
- HR
- Audit
- Rules Mapping
- Policies & procedures

Detection

- CMP
- 4 eyes
- Reporting
- Objectives
- Rules mapping
- Breach risk indicators
- Policies & Procedures

Remediation

- Remedial training
- Complaints handling
- Remediation plans
- CMP testing remediation
- Breach remediation

Where things go wrong

- Procedures on how to carry out compliance monitoring activities provided insufficient or no detail on the testing to be undertaken. ›
- Compliance monitoring procedures reference incorrect obligations, e.g. Group/UK rather than IOM.
- Testing activities were not completed to schedule or were not performed, which could lead to risks crystallising or breaches not being addressed in a timely manner.
- Findings of CMP tests were not escalated, resulting in a failure to remediate.
- CMP reports did not accurately reflect the testing that had been carried out during the reporting period, hampering the Board's decision-making.

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Where things go wrong

- Procedures on how to carry out compliance monitoring activities AML/CFT/ policies were either not updated at the appropriate frequencies or were not in place at all, suggesting the HOC may not be fulfilling their statutory requirements to monitor compliance with the regulatory framework.
- Procedures referred to out-of-date legislation or former role-holders.
- Board minutes did not evidence scrutiny, discussion, and challenge in respect of HOC/MLRO reports to the Board.
- Training was not delivered to the organisation was not tailored to IOM's specific legal and regulatory obligations

Join the discussion on Slido – #FSACOL2024

Where things go wrong

- The HOC could not demonstrate they had the appropriate independence or authority within their organisation.
- The HOC could not demonstrate they had sufficient access to the Board.

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Red Flags for HoCs and MLROs

- Being asked to change your (board) reports
- Not presenting your reports in person
- Reports not being read
- Never any questions
- Not being involved in key business projects
- Culture
- Not being supported with resource
- Not having unfettered access to the Board
- Key meetings being cancelled on a regular basis
- Being bypassed / going over your head
- Pressure to make commercially favourable decisions
- Conflicts with other roles

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Future-proofing your firm

- Developing policies and updating existing policies to support sustainability
- Remaining alert to emerging threats and opportunities – AI, ESG, innovation
- Members of Board and Executive focused on risk horizon scanning
- Training and Competency Framework and the Regulatory Guidance for Fitness and Propriety
- Succession planning

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Supporting compliance professionals

- Working collaboratively to build knowledge and capacity
- Partnering with UCM to deliver training and education in compliance and AML
- Pragmatic approach to appointment of controlled function roles
- Talk to us and work together to find appropriate solutions

Join the discussion on Slido – #FSACOL2024

ISLE OF MAN FINANCIAL SERVICES AUTHORITY

Questions, Further Discussion

Join the discussion on Slido – #FSACOL2024

slido

Please download and install the Slido app on all computers you use

Audience Q&A

ⓘ Start presenting to display the audience questions on this slide.