

## GRC Mastery Case Study: 3LODs

### GRC Mastery Case Study: 3LODs



### Scenario

Attached is excerpt from the publicly available Annual Report and Financial Statements FY24 for [The Foresight Group Holdings Limited](#).

### Instructions

You are hired as a Cyber Security Consultant to help The Foresights Group Holding Limited with their Cyber Security Risk Management and Audit activities.

Your first task is to understand the report attached.

The following questions can be answered with information provided in the attached report.

### Download

## Quiz

1 / 13

Which line of defence is primarily responsible for managing inherent risks on a day-to-day basis?

First Line of Defence- Correct

Second Line of Defence

Third Line of Defence

Executive Committee

Who oversees the overall adequacy and effectiveness of the Group-wide Risk Framework?

First Line of Defence

Risk & Compliance function

incorrectExecutive Committee

Board of Directors- Correct

Which function provides independent assurance on the effectiveness of the risk management framework?

First Line of Defence

Risk Committee

Third Line of Defence- Correct

Compliance function

The Second Line of Defence is responsible for which of the following activities?

Directly managing day-to-day operational risks

Implementing risk reporting and escalation- Correct

External audit and independent verification

Setting business strategy and risk appetite

What is the role of the First Line of Defence within the 3LOD model?

Setting the overall risk appetite for the group

Day-to-day risk management and control adherence- Correct

Independent oversight and challenge of controls

Approving risk policies and procedures

Who provides input into risk identification and scoring managed by the Risk function?

External auditors

incorrectSecond Line of Defence

First Line of Defence (businesses and functions)- Correct

Executive Committee

Which line of defence is responsible for verifying the adequacy of the Group Risk Framework through external oversight?

© Anushka Sinha | [github.com/rikusmiles/](https://github.com/rikusmiles/)  
First Line of Defence

Second Line of Defence

Third Line of Defence- Correct

Compliance Team

What is a key focus of the Foresight Group's cyber risk management approach?

Reducing the company's physical footprint

Using advanced encryption and data protection mechanisms- Correct

Limiting the use of digital technology

Avoiding external audits altogether

How does Foresight Group test its cyber defences?

Hiring hackers to simulate attacks

Passive monitoring of external threats

Disabling non-essential systems

correct Simulated cyber-attacks (penetration testing)

What is the major risk associated with third-party service providers?

Compromised cyber security leading to breaches in Foresight's systems- Correct

Poor customer service quality

Reduced profitability in global markets

Lower compliance with internal HR policies

How does Foresight address the risk of cyber threats through third-party vendors?

Outsourcing all data management to external providers

Ignoring third-party risks since they are low probability

Allowing vendors unrestricted access to internal systems

Performing detailed IT security assessments as part of due diligence- Correct

Which recent technological development is highlighted as increasing cyber risk complexity for Foresight Group?

The rise of cloud computing

Simple AI tools that enhance phishing email quality- Correct

Introduction of 5G technology

Blockchain adoption

The Board delegates responsibility for risk management to which body?

Executive Committee- Correct

Risk Committee

Compliance Function

Sustainability Committee

Recommendations:

GRC Mastery by Abed Hamdan