BARCUD
SHARED SERVICES

Cost of Failure – Can you afford to miss the opportunities that great risk management provides?

February 2025

Nigel Ireland, Chief Executive

BARCUD
SHARED SERVICES

Corporate failure causes

[Case Study 1: The £10 Billion IT Disaster at the NHS - Henrico Dolfing]

Corporate failure causes

- Austerity / insufficient resource allocation?
- Personal gain?
- Optimism bias?
- Poor decision making?
- Lack of effective scrutiny?
  - Internal Audit
  - Board Members
- Lack of accountability?
- Underestimating complexity?
- Lack of clear objectives & performance metrics?
- Ignoring cultural change?

Max:

- Governance
- Leadership
- Honesty

Corporate failure causes

Max:

- Governance
- Leadership
- Honesty

- Structures / Purpose
- Training / Understanding
- Robustness
- Focus

- Behaviours

- 👆
- Transparency
- Accepting scrutiny

Where was risk management?

- Structures
- Training / Understanding
- Robustness
- Focus

- Behaviours

- 👆
- Transparency
- Accepting scrutiny

Barriers to good risk management

- Over-complexity
- Lack of understanding
- Lack of purpose
- Poor articulation of objectives
- Risk management not linked to objectives
- Poor articulation of risks
- Lack of cause and effect / threat & consequence

BARCUD
SHARED SERVICES

What is risk?

The threat that an event or action will impact on our ability to achieve our strategic and operational objectives

Note: risk can operate in both directions, it is not always “adverse”. The effect could be:

- negative (threat / downside); or
- positive (opportunity / upside)

What is risk?

The threat that an event or action will impact on our ability to achieve our strategic and operational objectives

"Business objectives" include some fundamentals that may not be explicitly documented, e.g. compliance with the law and continuing the existence of the organisation

BARCUD
SHARED SERVICES

Risk Cause & Effect

- If you don't understand the cause, you don't know what to do to reduce the risk
- If you don't know the effect (impact) on the objective, then you don't know how much effort to invest to manage it

Impact = the impact ON THE OBJECTIVE

Likelihood = probability of the event impacting ON THE OBJECTIVE

Bow Tie – Root Cause

OBJECTIVE: Deliver our new Finance system by 31 March 2026

Some examples:

City Centre Security & Safety

Risk Overview	Minimise the risks and disruption to people and businesses due major incidents or deliberate acts that pose hazards to people and business and can result in structural damage; damage/disruption to infrastructure and utilities; impacts on business continuity, reputation, and the economy, in both the city centre and affected surrounding areas.
Parent Service(s)	Infrastructure
Lead Cabinet Member(s)	Cabinet Member for Assets and Infrastructure

12

Inherent Risk Score

9

Target Risk Score

BARCUD
SHARED SERVICES

Some examples:

Risk Name/Owner/Responsible CLO	
R009: Information Management - Security	[redacted]

Current Score	Target for Risk
16	12

Description	Failure to ensure that we have effective Information Management compliance in place will increase the risk and damage from any governance or data breaches. Weakness in compliance will also affect our ability to respond to FOIs and Subject Access requests. This may lead to increased risk of fines, loss of data or access to one or more systems and cause reputational damage.
Evidence of Risk	• Strained capacity to move projects forward. • Lack of details Information Processing Register • Lack of active retention on electronic files • Poor electronic record keeping practices. • Difficulty maintaining required standards. • Current EDRMS end of life
Potential Consequences	Failure to fully suitable governance of data processing could lead to – • Inappropriate processing • Security Risks • Failures in supplier assurance • Poor Decision making • Reputational damage • Damage to service users

What could we do differently?

Why do we have risk registers?

1. A tool for management to help them achieve the organisation's objectives
2. To provide assurance to management and the 'governing body' that risks are being managed / objectives will be achieved.

OBJECTIVE	Risks & Controls								ASSURANCE THAT WE ARE ACHIEVING OBJECTIVE		Risk Appetite	ADDITIONAL CONTROLS (C) OR ASSURANCES (A)
		Inherent Risk				Residual Risk						
	Risk Description	Impact	Prob.	Inherent Risk Score	Key Controls in Place	Impact	Prob.	Residual Risk Score	Internal Assurance (*Second Line*)	Independent Assurance (*Third Line*)		
2. Increase the efficiency of our service delivery and reduce ongoing costs through improved efficiency in our IT systems and processes.	**2.01 - Proficiency / Capability** A lack of technical expertise within the organisation or resources in place deliver change initiatives effectively may lead to reduced likelihood of change success, financial loss through over-spends and a loss of future efficiency savings.	5	4	20	1. Dedicated project management office tasked with leading on all significant change projects. 2. Programme Board in place, including Board representation, to oversee projects. 3. Risk registers mandatory for all projects and reported to Programme Board. 4. Technical expertise commissioned for each project to ensure technical proficiency.	3	3	9	1. PMO report to Board Aug24 showed all projects on track. 2 & 3. Board Member update to Nov24 Board provided reasonable assurance over project management and risk register maintenance. 4. Technical exertise involved in all 3 current major organisational projects.	All - Internal Audit of Project & Programme Management (November 2024) provided Reasonable assurance.	6	(C) Further work being undertaken to free up staffing resources to be seconded to key projects.

Why do we have risk registers?

OBJECTIVE	Risks & Controls								ASSURANCE THAT WE ARE ACHIEVING OBJECTIVE			ADDITIONAL CONTROLS (C) OR ASSURANCES (A)
		Inherent Risk				Residual Risk						
	Risk Description	Impact	Prob.	Inherent Risk Score	Key Controls in Place	Impact	Prob.	Residual Risk Score	Internal Assurance (*Second Line*)	Independent Assurance (*Third Line*)	Risk Appetite	
2. Increase the efficiency of our service delivery and reduce ongoing costs through improved efficiency in our IT systems and processes.	**2.01 - Proficiency / Capability** A lack of technical expertise within the organisation or resources in place deliver change initiatives effectively may lead to reduced likelihood of change success, financial loss through over-spends and a loss of future efficiency savings.	5	4	20	1. Dedicated project management office tasked with leading on all significant change projects. 2. Programme Board in place, including Board representation, to oversee projects. 3. Risk registers mandatory for all projects and reported to Programme Board. 4. Technical expertise commissioned for each project to ensure technical proficiency.	3	3	9	1. PMO report to Board Aug24 showed all projects on track. 2 & 3. Board Member update to Nov24 Board provided reasonable assurance over project management and risk register maintenance. 4. Technical exertise involved in all 3 current major organisational projects.	All - Internal Audit of Project & Programme Management (November 2024) provided Reasonable assurance.	6	(C) Further work being undertaken to free up staffing resources to be seconded to key projects.

How worried are we?

How worried are we now?

What may stop us achieving our objective / what is keeping us awake at night?

(Cause & Effect)

What **key things** are we doing that are reducing the likelihood and/or the impact?

How do we know that:

- Our controls are effective
- Our risk is being sufficiently managed; or
- Our objective will be achieved?

Must think “outcomes”

BARCUD
SHARED SERVICES

But… we do that don't we?

- Risks rarely linked clearly to objectives (problem with clarity of objectives?)
- Risk descriptions too narrative and don't clearly identify the causes that can be acted upon
- Controls tend to be a description of everything someone or a team is doing in that area; lack of specific focus on "key" controls
- Lack of focus on 'outcomes' rather than outputs
- As a result, risk assessment is highly subjective / qualitative

Assurance

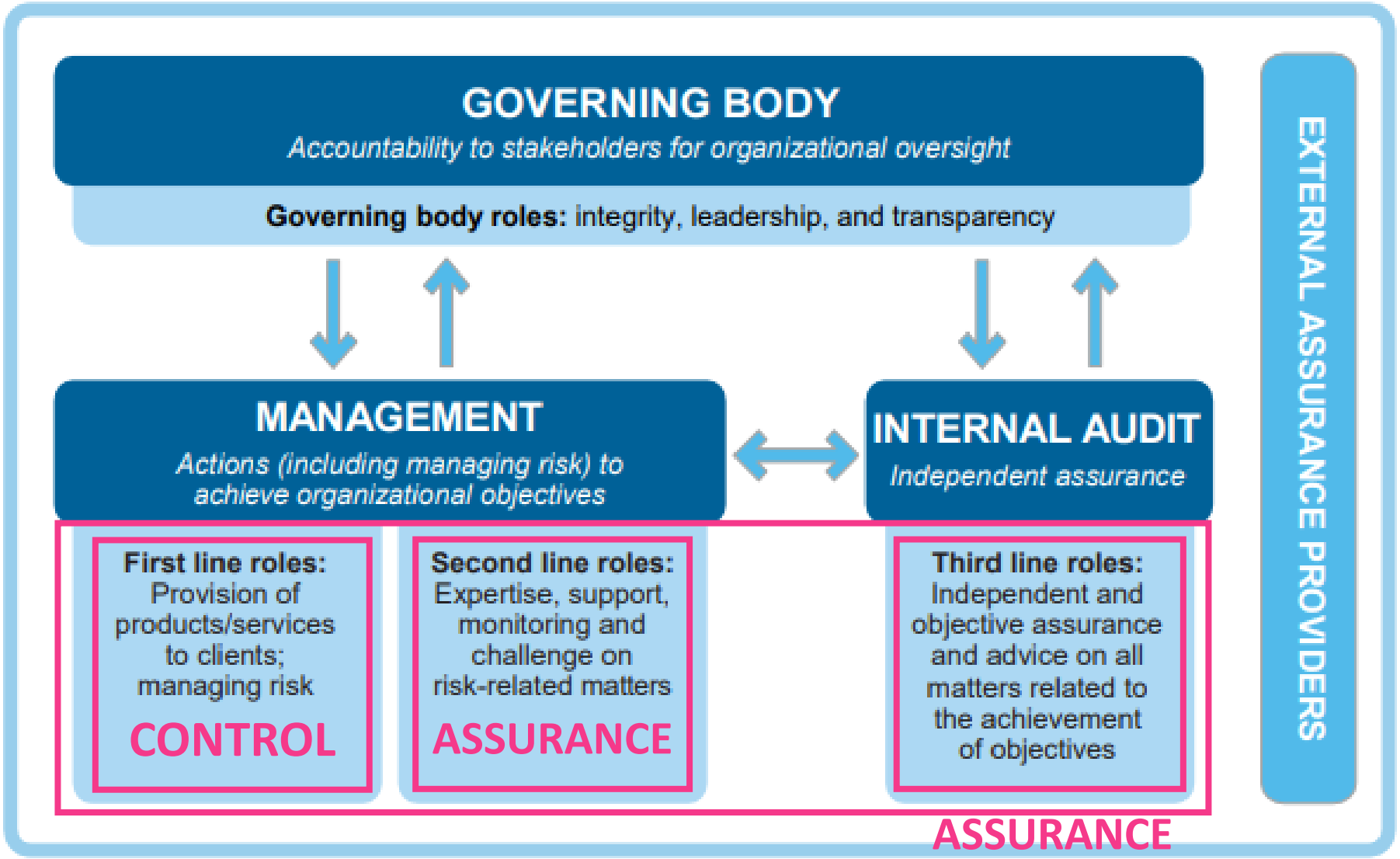
- “Confidence, based on sufficient evidence, that internal controls are in place, operating effectively and objectives are being achieved” (*various – Public Sector*)

- Assurance is what gives you comfort that a control is working (and therefore informs whether a risk is being managed as you had envisaged)

BARCUD
SHARED SERVICES

Three Lines Model

https://www.astari.org.uk/blog/new-three-lines-model



Sources of Assurance

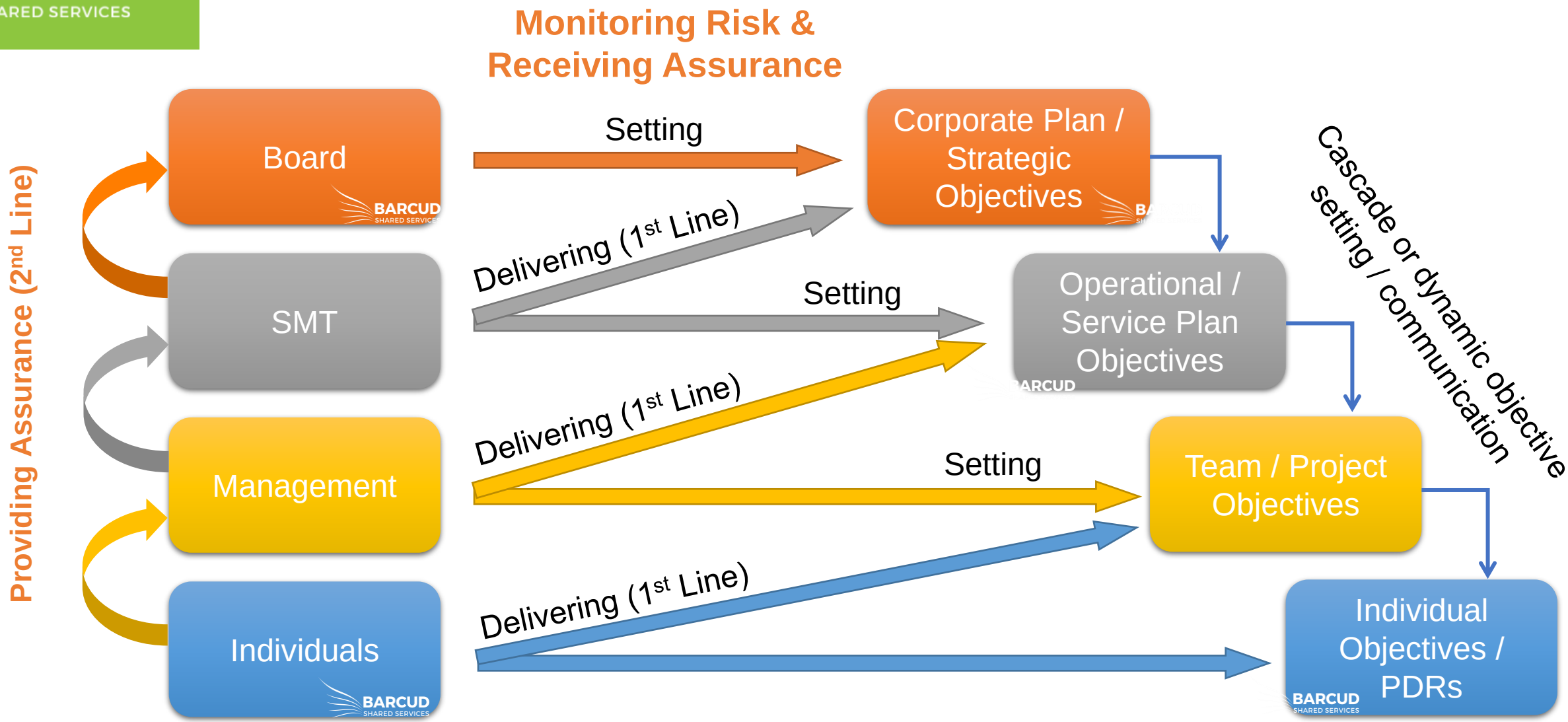
1. Many different sources of assurance
2. Internal (2nd Line) Assurance & Independent (3rd Line) Assurance

3. Assurance must be evidence-based
4. Efficiency = a combination of all assurance sources, both Internal (2nd Line) and Independent (3rd Line).

Risk & Internal Audit

- Internal Audit Strategy & Annual Plan should be based around the organisation's risks (as far as possible)
- Testing should focus on the controls that have the greatest impact on the risk
- The priority of findings should be based on their impact **on the risk**
- Overall assurance level should be based on the organisation's performance in managing its risk
- New Standards (January '25) – Internal Audit must focus on protecting the 'public interest'

Monitoring Risk (Receiving) & Giving Assurance



BARCUD
SHARED SERVICES

How does this protect you from failure?

- Clarity of objectives (strategically, operationally and in projects) makes the expectations clear
- Clarity of risks – means the understanding of the potential success of achieving objectives is clear, honest and transparent
- Risk assessment can be more quantitative and objective
- “Key” controls reduce the ‘noise’ and enable focus and clearer scrutiny & challenge
- Focused assurance – adds value and reduces tick-boxing
- Effective scrutiny & challenge, once enabled, brings different perspectives and ideas

So what else do we need to do?

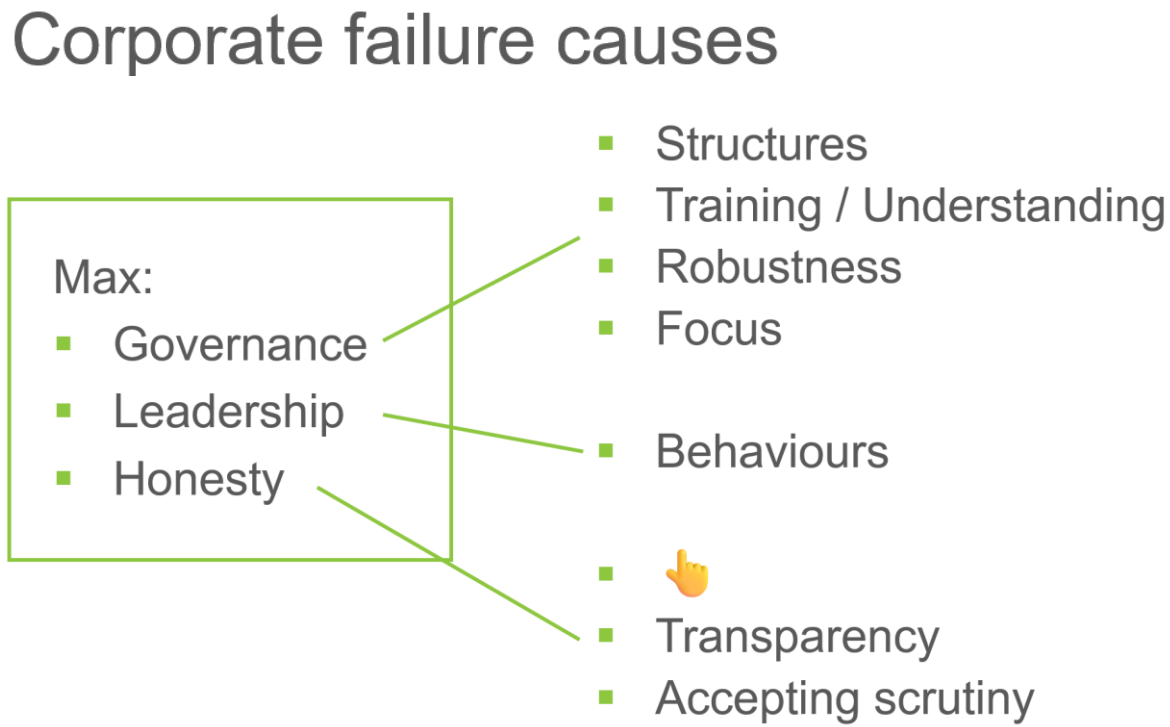
- Review your risk register structure – is it concise, are the links clear, does the structure lead to simplicity rather than complexity?
- Consider the layers of risk – don't combine too many risks together – lack of transparency of the key risk factors

- Focus on "key" risks and "key" controls – don't just describe everything that is being done in the area. Usually, 3 - 4 controls are doing c.70% of the risk management!
- Ensure your governing body / audit committee are trained in your processes
- Focus on outcomes and welcome scrutiny and challenge. Admitting you need help / support is not a weakness!

BARCUD
SHARED SERVICES

In summary…

- Risk Management isn't about ticking boxes; it should be a tool to help you achieve
- Risk management provides structure



- Remember – it is not just a reporting tool to the Board, it is also a tool for management – keeps focus, enables prioritisation
- Effective risk management at all levels encourages positive behaviours, both when things are going right, but most importantly when things may be starting to go wrong
- Most effective when it is transparent & effectively challenged

BARCUD
SHARED SERVICES

Nigel Ireland

Chief Executive

nigel@barcudsharedservices.org.uk