Beyond the Risk Register
An Overview of Risk Management

Risk management is often seen as a document - the risk register.
In practice, it is how an organisation is run.
It is understanding what could help or hinder objectives, deciding how to respond, and reviewing the landscape regularly.

What "good" looks like in practice:

- Clear objectives: If objectives aren't clear, risks can't be meaningfully defined.
- Risk appetite and tolerance: Agreement on how much risk is acceptable while pursuing those objectives.
- Identification and assessment: Not just listing risks, but understanding *likelihood*, *impact*, and key drivers.
- Responses and controls: Deciding whether to avoid, reduce, share/transfer, or accept risk, embedding proportionate controls for what matters.
- Ownership and accountability: Being clear who is accountable and responsible for managing risks and implementing agreed responses.
- Monitoring and reporting: Regular reviews of existing risks and identifying new ones as strategy, operations, suppliers, regulations and technologies change.

The different roles – the "three lines":

- First line identify and manage risks day-to-day.
- Second line (e.g., risk, compliance, security) provide expertise, support, and challenge on risk-related matters.
- Internal audit provide independent assurance and advice on the effectiveness of governance, risk management, and controls.

A simple checklist:

For your key organisational objectives, can you answer and evidence:

1. What could stop us achieving them?
2. Who owns the related risks?
3. What are we doing about the risks?
4. How do we know risk management is working?

And remember, risk isn't only about downside, it includes upside opportunities too.

tickbox

rebecca.dyson@tickboxsolutions.co.uk
07989 865452