

Guidance for setting out existing risk controls using the 3 Lines of Defence

For each strategic and directorate risk, the risk owner sets out the controls in place to address the risk and the arrangements in place to make sure that these controls are working effectively. The aim is to provide an easy to follow summary using the 3 Lines of Defence model:

- 1st line: management controls
- 2nd line: corporate oversight
- 3rd line: independent assurance

Clear and high quality input helps managers to ensure that the arrangements put in place to address the risk are sufficiently robust and are proportionate. It also provides assurance to ELT and the Audit & Standards Committee who monitor on behalf of the council. This guidance sets out what we expect to see (and things we want to avoid) under each Line of Defence.

1st Line of Defence: Management Controls	
Management activity. Requires input of those who know the business, culture and day to day challenges.	
What we want to see	What we want to avoid
<ul style="list-style-type: none"> • A structured and logical approach that sets out how managers address the whole of the risk • Simple descriptions • Controls that are in place • Controls that can be tested 	<ul style="list-style-type: none"> • Long lists of controls (no more than six?) • Lack of clarity as to whether the whole of the risk is being addressed • Controls that cannot be tested • Good intentions (eg planned improvements) • Wishful thinking

2nd Line of Defence: Corporate Oversight	
This involves those responsible for delivery, but not independent of the organisation’s management chain such as ELT, Boards and Committees. It includes overview of policy delivery and regulatory considerations.	
What we want to see	What we want to avoid
<ul style="list-style-type: none"> • 2nd line defences that provide assurance over the 1st line controls • 2nd line defences that are in place: <ul style="list-style-type: none"> ○ does the 2nd Line know that this is their role? ○ is this set out in in job descriptions, terms of reference, regular agenda items etc. 	<ul style="list-style-type: none"> • Lack of clarity as to whether assurance is provided over the whole of 1st line • 2nd lines of defence that are not in place. • 2nd lines that don’t contribute to better management of a risk

3rd Line of Defence: Corporate Oversight	
Includes internal audit, external audit and inspectorates such as OFSTED. Provide independent assurance for senior management and Members about the effectiveness of the 1 st and 2 nd lines of defence.	
What we want to see	What we want to avoid
<ul style="list-style-type: none"> • Only include audits and inspections which have reasonable link with the risk. • Include the titles, the dates and results/conclusions of the latest assessments linked to the risk. 	<ul style="list-style-type: none"> • Avoid audits and inspections which are not reasonably linked to providing assurance is provided over the whole of 1st and 2nd lines • 3rd lines of defence that do not exist. • Committees are not the 3rd Line of Defence.

