Current assessment rationale for grading the priority of recommendations in Internal Audit reports

Risk rating	Assessment rationale
🔴 Critical	Critical and urgent in that failure to address the risk could lead to one or more of the following occurring: ▪ Significant financial loss (through fraud, error, poor value for money) ▪ Serious safeguarding breach ▪ Life threatening or multiple serious injuries ▪ Catastrophic loss of service ▪ Failure of major projects ▪ Critical Information loss leading to Information Commissioner's Office (ICO) referral ▪ Reputational damage – Intense political and media scrutiny i.e. front-page headlines, television coverage. ▪ Possible criminal, or high profile, civil action against the Council, Members or officers. ▪ Intervention by external agencies *Remedial action must be taken immediately*
🟠 Major	Major in that failure to address the issue or progress the work would lead to one or more of the following occurring: ▪ High financial loss (through fraud, error, poor value for money) ▪ Safeguarding breach ▪ Serious injuries or stressful experience requiring medical treatment, many work days lost. ▪ Significant disruption to service (Key outcomes missed, some services compromised. Management action required to overcome medium term difficulties) ▪ Major Information loss leading to internal investigation ▪ Reputational damage – Unfavourable external media coverage. Noticeable impact on public opinion. ▪ Scrutiny required by external agencies *Remedial action must be taken urgently*
🟡 Moderate	Moderate in that failure to address the issue or progress the work would lead to one or more of the following occurring: ▪ Medium financial loss (through fraud, error or poor value for money) ▪ Significant short-term disruption of non-core activities ▪ Scrutiny required by internal committees. ▪ Injuries or stress level requiring some medical treatment, potentially some work days lost ▪ Reputational damage – Probable limited unfavourable media coverage. *Prompt specific action should be taken*
🟢 Low	Low in that failure to address the issue or progress the work would lead to one or more of the following occurring: ▪ Low financial loss (through error or poor value for money) ▪ Minor errors in systems/operations or processes requiring action or minor delay without impact on overall service delivery schedule. Handled within normal day to day routines. ▪ Reputational damage – Internal review, unlikely to have a wider impact. *Remedial action is required*

Assurance Level	Description
Good	*Good assurance* – there is a sound system of internal control designed to achieve the objectives of the system/process and manage the risks to achieving those objectives. Recommendations will normally only be of Low risk rating. Any Moderate recommendations would need to mitigated by significant strengths elsewhere.
Adequate/ Satisfactory	*Adequate/satisfactory assurance* – whilst there is basically a sound system of control, there are some areas of weakness, which may put the system/process objectives at risk. There are Moderate recommendations indicating weaknesses but these do not undermine the system's overall integrity. Any Critical recommendation will prevent this assessment, and any Major recommendations relating to part of the system would need to be mitigated by significant strengths elsewhere.
Limited	*Limited assurance* – there are significant weaknesses in key areas in the systems of control, which put the system/process objectives at risk. There are Major recommendations or a number of moderate recommendations indicating significant failings. Any Critical recommendations relating to part of the system would need to be mitigated by significant strengths elsewhere.
No	*No assurance* – internal controls are generally weak leaving the system/process open to significant error or abuse or reputational damage. There are Critical recommendations indicating major failings

Overdue Critical and Major Internal Audit Recommendations as at 31 October 2020

Audit Review Title	Function	Recommendation	Latest Target Date	Last Status Update	Owner	Rating
GDPR Compliance (1920 CC16)	Corporate and Customer	Training Completion	14/09/20	**Update as at 4 August 2020:** eLearning modules have now been revised and our previous three modules have now been reduced to one slightly longer course. This course is designed to give the basic Information Governance training for all. This is also supported by further IG 'playlists' that can be accessed through My Learning. Anything more detailed will be communicated to targeted audiences. The eLearning modules have now been updated on the My Learning site, however we are now waiting for confirmation from Learning and Development when communication will be sent to staff regarding recertification. There have been delays with this action due to Covid-19, as much resource from IG and Learning and development had to be pulled.	Information Security Business Officer	Major
Major Incident Management Follow Up (1920 CD3)	Finance and Technology	Improving the governance over major incidents through reporting	30/09/20	Update as at 27 August 2020: Work ongoing, expected shortly.	Chief Operations Officer Technology Services	Major
Accounts Receivable (1920 CC1 AR)	Finance and Technology	Management Information does not help compliance with the Collection Strategy and prioritise activity	31 July 2020	None provided; audit finalised in July 2020. The Service Manager came to AGS Committee in September 2020 to discuss this audit review as it received Limited Assurance overall.	Service Manager, Income	Major