

Annex B Detailed appetite matrix by risk categories.

The following table provides a sample of risk appetites developed against a selection of the risk categories recommended in Annex 4 of the [Orange Book](#).

Risk appetite level definition					
	Averse	Minimal	Cautious	Open	Eager
Strategy	Guiding principles or rules in place that limit risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 5+ year intervals	Guiding principles or rules in place that minimise risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 4-5 year intervals	Guiding principles or rules in place that allow considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 3-4 year intervals	Guiding principles or rules in place that are receptive to considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 2-3 year intervals	Guiding principles or rules in place that welcome considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 1-2 year intervals
Governance	Avoid actions with associated risk. No decisions are taken outside of processes and oversight / monitoring arrangements. Organisational controls minimise risk of fraud, with significant levels of resource focused on detection and prevention.	Willing to consider low risk actions which support delivery of priorities and objectives. Processes, and oversight / monitoring arrangements enable limited risk taking. Organisational controls maximise fraud prevention, detection and deterrence through robust controls and sanctions.	Willing to consider actions where benefits outweigh risks. Processes, and oversight / monitoring arrangements enable cautious risk taking. Controls enable fraud prevention, detection and deterrence by maintaining appropriate controls and sanctions.	Receptive to taking difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements enable considered risk taking. Levels of fraud controls are varied to reflect scale of risks with costs.	Ready to take difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements support informed risk taking. Levels of fraud controls are varied to reflect scale of risk with costs.
Operations	Defensive approach to operational delivery - aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority.	Innovations largely avoided unless essential. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.	Innovation supported, with clear demonstration of benefit / improvement in management control. Responsibility for non-critical decisions may be devolved.	Innovation pursued – desire to ‘break the mould’ and challenge current working practices. High levels of devolved authority – management by trust / lagging indicators rather than close control.

Legal	Play safe and avoid anything which could be challenged, even unsuccessfully.	Want to be very sure we would win any challenge.	Want to be reasonably sure we would win any challenge.	Challenge will be problematic; we are likely to win, and the gain will outweigh the adverse impact.	Chances of losing are high but exceptional benefits could be realised.
Property	Obligation to comply with strict policies for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Recommendation to follow strict policies for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Requirement to adopt arrange of agreed solutions for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Consider benefits of agreed solutions for purchase, rental, disposal, construction, and refurbishment that meeting organisational requirements.	Application of dynamic solutions for purchase, rental, disposal, construction, and refurbishment that ensures meeting organisational requirements.
Financial	Avoidance of any financial impact or loss, is a key objective.	Only prepared to accept the possibility of very limited financial impact if essential to delivery.	Seek safe delivery options with little residual financial loss only if it could yield upside opportunities.	Prepared to invest for benefit and to minimise the possibility of financial loss by managing the risks to tolerable levels.	Prepared to invest for best possible benefit and accept possibility of financial loss (controls must be in place).
Commercial	Zero appetite for untested commercial agreements. Priority for close management controls and oversight with limited devolved authority.	Appetite for risk taking limited to low scale procurement activity. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.	Innovation supported, with demonstration of benefit / improvement in service delivery. Responsibility for non-critical decisions may be devolved.	Innovation pursued – desire to ‘break the mould’ and challenge current working practices. High levels of devolved authority – management by trust / lagging indicators rather than close control.
People	Priority to maintain close management control & oversight. Limited devolved authority. Limited flexibility in relation to working practices. Development investment in standard practices only	Decision making authority held by senior management. Development investment generally in standard practices.	Seek safe and standard people policy. Decision making authority generally held by senior management.	Prepared to invest in our people to create innovative mix of skills environment. Responsibility for noncritical decisions may be devolved.	Innovation pursued – desire to ‘break the mould’ and challenge current working practices. High levels of devolved authority – management by trust rather than close control.

Risk appetite level definitions					
	Averse	Minimal	Cautious	Open	Eager
Technology	General avoidance of systems / technology developments.	Only essential systems / technology developments to protect current operations.	Consideration given to adoption of established / mature systems and technology improvements. Agile principles are considered.	Systems / technology developments considered to enable improved delivery. Agile principles may be followed.	New technologies viewed as a key enabler of operational delivery. Agile principles are embraced.
Data & Info Management	Lock down data & information. Access tightly controlled, high levels of monitoring.	Minimise level of risk due to potential damage from disclosure.	Accept need for operational effectiveness with risk mitigated through careful management limiting distribution.	Accept need for operational effectiveness in distribution and information sharing.	Level of controls minimised with data and information openly shared.
Security	<p>No tolerance for security risks causing loss or damage to HMG property, assets, information or people. Stringent measures in place, including:</p> <ul style="list-style-type: none"> • Adherence to FCDO travel restrictions • Staff vetting maintained at highest appropriate level. • Controls limiting staff and visitor access to information, assets and estate. • Access to staff personal devices restricted in official sites 	<p>Risk of loss or damage to HMG property, assets, information or people minimised through stringent security measures, including:</p> <ul style="list-style-type: none"> • Adherence to FCDO travel restrictions • All staff vetted levels defined by role requirements. • Controls limiting staff and visitor access to information, assets and estate. • Staff personal devices permitted, but may not be used for official tasks. 	<p>Limited security risks accepted to support business need, with appropriate checks and balances in place:</p> <ul style="list-style-type: none"> • Adherence to FCDO travel restrictions • Vetting levels may flex within teams, as required • Controls managing staff and limiting visitor access to information, assets and estate. • Staff personal devices may be used for limited official tasks with appropriate permissions. 	<p>Considered security risk accepted to support business need, with appropriate checks and balances in place:</p> <ul style="list-style-type: none"> • New starters may commence employment at risk, following partial completion of vetting processes • Permission may be sought for travel within FCDO restricted areas. • Controls limiting visitor access to information, assets and estate. • Staff personal devices may be used for official tasks with appropriate permissions. 	<p>Organisational willing to accept security risk to support business need, with appropriate checks and balances in place:</p> <ul style="list-style-type: none"> • New starters may commence employment at risk, following partial completion of vetting processes • Travel permitted within FCDO restricted areas. • Controls limiting visitor access to information, assets and estate. • Staff personal devices permitted for official tasks

Project/Programme	<p>Defensive approach to transformational activity - aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority. Benefits led plans fully aligned with strategic priorities, functional standards.</p>	<p>Innovations avoided unless essential. Decision making authority held by senior management. Benefits led plans aligned with strategic priorities, functional standards.</p>	<p>Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Plans aligned with strategic priorities, functional standards.</p>	<p>Innovation supported, with demonstration of commensurate improvements in management control. Responsibility for noncritical decisions may be devolved. Plans aligned with functional standards and organisational governance.</p>	<p>Innovation pursued – desire to ‘break the mould’ and challenge current working practices. High levels of devolved authority – management by trust rather than close control. Plans aligned with organisational governance.</p>
Reputational	<p>Zero appetite for any decisions with high chance of repercussion for organisations’ reputation.</p>	<p>Appetite for risk taking limited to those events where there is no chance of any significant repercussion for the organisation.</p>	<p>Appetite for risk taking limited to those events where there is little chance of any significant repercussion for the organisation.</p>	<p>Appetite to take decisions with potential to expose organisation to additional scrutiny, but only where appropriate steps are taken to minimise exposure.</p>	<p>Appetite to take decisions which are likely to bring additional Governmental / organisational scrutiny only where potential benefits outweigh risks.</p>