






CIVIL CONTINGENCIES POLICY BRANCH

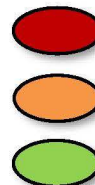
RISK REGISTER 2018/19

CIVIL CONTINGENCIES POLICY BRANCH AIM




'To encourage effective emergency preparedness; support emergency response through delivery of government's central crisis management arrangements; and work with key partners to strengthen NI resilience, primarily through the work of the Civil Contingencies Group (NI) led by HOCS.'

CIVIL CONTINGENCIES POLICY BRANCH SUMMARY OF RISKS




		Overall Risk Assessment
1	TEO's co-ordination arrangements fail to respond quickly and effectively to serious civil contingencies.	
2	Local civil contingencies arrangements are ineffective	
3	Failure to operate within allocated budget: avoiding overspend and managing underspend within 1.5% target	
4	CCPB is in breach of its information governance obligations	
5	Physical security of CCPB's physical assets is compromised.	






The CCPB Risk Register will be updated, reviewed and considered on a regular basis

RISK 1 – TEO's co-ordination arrangements fail to respond quickly and effectively to serious civil contingencies			
Primary Causes		Current and planned actions to manage the risk	
<ul style="list-style-type: none"> Lack of central co-ordination of the strategic preparedness agenda. Lack of engagement with and by multi-agency partners. Low level of operational preparedness. Availability of key personnel. 		<ul style="list-style-type: none"> Tri-annual meetings of the Civil Contingencies Group (NI) (CCG(NI)), the principal civil contingencies strategic preparedness body for NI chaired by HOCS. Ongoing maintenance by TEO of a central suite of emergency response protocols for use by all emergency planners/responders. Ongoing TEO engagement with multi-agency partners to identify gaps in preparedness and to prioritise resulting actions via CCG(NI). Regular tests of operational preparedness to ensure that TEO can put the necessary strategic response structures in place quickly and easily. 	
Consequences			
<ul style="list-style-type: none"> The effectiveness of the strategic central government response to a civil emergency is compromised. Potential loss of life. Potentially significant damage to infrastructure, the economy and/or the environment. Reputational damage to TEO, Ministers and the NI Executive. 			
Risk Assessment (after current and planned actions)	Impact	Likelihood	Overall Risk Assessment
			
Business Plan Objective(s)	R2.1 By March 2019 maintain operational readiness to respond to actual or anticipated strategic level emergencies. 2.3 Provide for and maintain the structures and arrangements necessary to provide an appropriate level of preparedness to respond quickly and effectively to serious civil emergencies.		
Risk Owner	NR		
Responsible Officer(s)	NR		

RISK 2 – Local civil contingencies arrangements are ineffective

RISK 2 – Local civil contingencies arrangements are ineffective			
Primary Causes	Current and planned actions to manage the risk		
<ul style="list-style-type: none"> Lack of a sustainable funding stream for local government to deliver local level co-ordination. Inadequate personnel resource allocated to this role by local government 	<ul style="list-style-type: none"> Ongoing TEO discussions with DfC (the funding department) and SOLACE to effect a resolution. TEO senior management discussion with DoF/DfC. TEO (CCPB) working with DfC officials on the business case from local government on the delivery of the sub-regional co-ordination role. Governance by CCG(NI) of the workstream associated with achieving the required outcomes. 		
Consequences			
<ul style="list-style-type: none"> No sub-regional planning will be carried out leading to significant vulnerability to a wide range of emergencies Reputational damage for departments and Ministers. Public outrage. Effectiveness of strategic level (central government) response will be very significantly compromised. 			
Risk Assessment (after current and planned actions)	Impact	Likelihood	Overall Risk Assessment
			
Business plan objective(s):	R1.3 By June 2017 to work with key stakeholders to establish robust, substantive sub-regional civil contingencies arrangements.		
Risk Owner			
Responsible Officer(s)	NR		

RISK 3 – Failure to operate within allocated budget: avoiding overspend and managing underspend within 1.5% target

Primary Causes		Current and planned actions to manage the risk		
<ul style="list-style-type: none"> Constrained public expenditure context and the likely decision to protect certain departments. There are no Ministers to put in place mitigating measures. The absence of key mechanisms in the NI public expenditure process (eg delay in setting budget; uncertainty of monitoring rounds). 		<ul style="list-style-type: none"> Ongoing budgetary management to ensure maximum VFM in discretionary spend. Liaison with Finance Division in re-profiling exercises and Monitoring Rounds. Robust financial management/governance in place to maximise VFM and to prioritise expenditure effectively. Regular expenditure reviews in branch. 		
Consequences				
<ul style="list-style-type: none"> Unable to meet objectives regarding operational readiness to respond. Unable to resource adequate training needs for the Branch Unable to meet statutory requirements regarding maintenance repair of the former RGHQ site. Reputational damage. 				
Risk Assessment (after current and planned actions)		Impact	Likelihood	Overall Risk Assessment
				
Business Plan Objective(s)		R3.1 To ensure effective branch financial management.		
Risk Owner				
Responsible Officer(s)				

RISK 4 – CCPB is in breach of its information governance obligations

Primary Causes

- Non-compliance with protective security requirements.
- Cyber risk.
- Inadequate management of corporate information (including personal and sensitive personal information under the Data Protection Act 1998 and GDPR).
- Non-compliance with the Freedom of Information Act 2000.
- Inadequate preparation for the implementation of General Data Protection Regulation (GDPR).

Current and planned actions to manage the risk

- Adherence to the departmental policies and guidance on data storage/security.
- Adherence to the requirements of the department's disposal schedule.
- Training for the introduction of GDPR.
- Attendance at seminars/information events on GDPR.
- Ensure strict adherence to the clear desk policy

Consequences

- Reputational damage – public and political criticism.
- Regulatory action taken by ICO (including decision and enforcement notices, performance monitoring and fines).
- Inability to retrieve information leading to poor evidential basis for policy development and accountability purposes.

Risk Assessment

(after current and planned actions)

Impact



Likelihood



Overall Risk Assessment



Business Plan Objective(s)




BP2 To ensure safe custody of all assets for which CCPB has responsibility including the former RGHQ site and information assets including personal data.
BP3.2. To maintain information systems and processes including for third party contact lists.

Risk Owner

Responsible Officer(s)

NR

RISK 5 – Physical security of CCPB's physical assets is compromised.

RISK 5 – Physical security of CCPB's physical assets is compromised.			
Primary Causes	Current and planned actions to manage the risk		
<ul style="list-style-type: none"> Non-compliance with departmental security policy on the security of assets. Staff unfamiliar with security requirements/regime. 	<ul style="list-style-type: none"> Ensure strict adherence to the clear desk policy Compliance with all other requirements issuing from the Departmental Security Officer Regular change of access codes for CCPB office suite. Staff familiarisation and training as required. Maintenance of CCPB asset register. 		
Consequences			
<ul style="list-style-type: none"> Potential loss or compromise of classified information or assets. Reputational damage. Potential for operational readiness to be compromised. 			
Risk Assessment (after current and planned actions)	Impact	Likelihood	Overall Risk Assessment
			
Business Plan Objective(s)	BP2 To ensure safe custody of all assets for which CCPB has responsibility including the former RGHQ site and information assets including personal data. BP2.2. Ensure that CCPB is fully compliant with departmental security policy.		
Risk Owner	NR		
Responsible Officer(s)			

1. RISK/IMPACT EVALUATION – IMPACT

DESCRIPTOR	FACTORS TO CONSIDER TO AID ASSESSMENT
Low	Little or no impact on achievement of key objective(s); or £10,000s lost; or minor non-compliance issues; or minor delay in timing.
Medium	Some impact on achievement of key objective(s); or £100,000s lost; or local media attention; or NIAO criticism.
High	The failure of key objective(s); or regional/national media attention; or £1,000,000s lost; or critical attention from Assembly/PAC; or death.

2. RISK/IMPACT EVALUATION – LIKELIHOOD

DESCRIPTOR	FACTORS TO CONSIDER TO AID ASSESSMENT
Low	May occur only in exceptional circumstances
Medium	Could occur at some time
High	Is expected to occur in most circumstances

3. OVERALL ASSESSMENT:

Impact	High			
	Medium			
	Low			
		Low	Medium	High
Likelihood				