

CIVIL CONTINGENCIES POLICY BRANCH







RISK REGISTER 2019/20

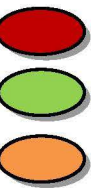
November – March

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	CCPB fails to support and strategically lead arrangements for CCG (NI) in the event of a serious civil contingency.	
2	Lack of sufficient resources (staffing and funding) to action lessons learned and respect best practice from the EU exit Preparedness Exercises and take forward strategic review of Civil Contingencies.	
3	TEO's suite of protocols and guidance documents are not up to date or user friendly	
4	Failure to operate within allocated budget: avoiding overspend and managing underspend within 1.5% target	
5	CCPB is at risk of being in breach of its information governance obligations	
6	Physical security of CCPB's physical assets is at risk of becoming compromised.	






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

RISK 1 – CCPB fails to support and strategically lead arrangements for CCG (NI) in the event of a serious civil contingency.			
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. Lack of availability of sufficient staff within CCPB with the relevant knowledge, skills and experience to deal with an emergency. 		<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. NI Hub – Centre of Excellence Operations Room and supporting infrastructure established and in place, the lessons learned report will ensure this learning is documented Testing of operational preparedness to ensure that TEO can put the necessary strategic response structures in place quickly have been successful for EU exit preparation. <p>Staffing:</p> <ul style="list-style-type: none"> Redesign of CCPB Project in preparation stage, business case under development to secure external experts Elective transfers to recruit an AO and a DP (within current complement) New Head of Branch has attended a 5 day Introduction to Civil Protection Course and will be receiving further training Training plan for all staff being developed, budget confirmed for this Funding – Business case for additional staff to be developed 	
Consequences			
<ul style="list-style-type: none"> The effectiveness of the strategic central government response to a civil emergency is compromised. Potentially significant damage to infrastructure, the economy and/or the environment. Reputational damage to TEO, NICS, Ministers and the NI Executive, poor reflection on NI to the rest of the UK Critical work cannot be taken forward due to a lack of resources both in terms of staff and money. 			
Risk Assessment (after current and planned actions)	Impact	Likelihood	Overall Risk Assessment
			
Business Plan Objective(s)	2.4 Provide the leadership and co-ordination needed to ensure Northern Ireland's preparedness to respond quickly and effectively to serious civil emergencies.		
Risk Owner	NR		
Responsible Officer(s)	NR		

RISK 2 – Lack of sufficient resources (staffing and funding) to action lessons learned from the EU exit Preparedness Exercises and take forward strategic review of Civil Contingencies.			
Primary Causes		Current and planned actions to manage the risk	
<ul style="list-style-type: none"> Sufficient staffing resources not available to carry out necessary work and put in place improvements Funding Resource not secured to implement lessons learned report and carry out review of CCPB 		Staffing: <ul style="list-style-type: none"> Business case for External consultants being drafted Additional staff resources also being sought from within NICS/public sector if possible. Business case to increase staff complement to previous level being drafted. JEGS will be required (6-9 months before new staff would be starting defendant on securing budget) Elective transfers for AO and DP (within existing complement in CCPB) have commenced. Senior staff from within CCPB and the Hub are meeting regularly to discuss and address ongoing issues, providing briefing to G3 as necessary. 	
Consequences			
<ul style="list-style-type: none"> Critical work cannot be taken forward due to a lack of resources both in terms of staff and money. The effort in time of money and resources spent on EU exit preparedness are wasted Contacts built up and training for Hub volunteers is not utilised going forward 			
Risk Assessment (after current and planned actions)	Impact	Likelihood	Overall Risk Assessment
			
Business Plan Objective(s)	2.4 Provide the leadership and co-ordination needed to ensure Northern Ireland's preparedness to respond quickly and effectively to serious civil emergencies.		
Risk Owner	NR		
Responsible Officer(s)			

RISK 3 – Failure to maintain TEO’s suite of protocols and guidance documents			
Primary Causes		Current and planned actions to manage the risk	
<ul style="list-style-type: none">Reduced staffing resources over several years as well as preparations for EU exit have resulted in no capacity to consider and take forward revisions		<ul style="list-style-type: none">The Strategic review of civil contingency arrangements in NI could potentially make changes to these documents therefore this will be taken forward once the review has concludedWork ongoing to get additional staff for CCPB should assist with this	
Consequences			
<ul style="list-style-type: none">Outdated documents (some publicly available online) are the only reference material available causing reputational damage to TEO, NICS, Ministers and the NI Executive, poor reflection on NI to the rest of the UKLocal government and other stakeholder guidance is not in line with TEO			
Risk Assessment (after current and planned actions)	Impact	Likelihood	Overall Risk Assessment
			
Business Plan Objective(s)	2.4 Provide the leadership and co-ordination needed to ensure Northern Ireland’s preparedness to respond quickly and effectively to serious civil emergencies.		
Risk Owner	NR		
Responsible Officer(s)			

RISK 4 – 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.An internal transfer of £18k has been made, this includes £15k for training which is required, ongoing work to determine training needs and ensure that they can be fulfilled within this financial year.		
<ul style="list-style-type: none">Unable to meet objectives regarding operational readiness to respond.Unable to resource adequate training needs for the BranchUnable 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)	1.5 We manage our resources effectively, focusing on the delivery of PfG outcomes (a) Ensure that the Department and ALBs operate within allocated budget, avoiding overspend and managing underspend within tolerance of 1.5% - by 31 March 2020.			
Risk Owner	NR			
Responsible Officer(s)				

RISK 5 – CCPB is at risk of being 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 management 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)

NO DIRECT LINK TO DEPARTMENTAL BUSINESS PLAN

To maintain information systems and processes including for third party contact lists.

Risk Owner

NR

Responsible Officer(s)

RISK 6 –**Physical security of CCPB's physical assets is at risk of becoming compromised.****Primary Causes**




- Non-compliance with departmental security policy on the security of assets.
- Staff unfamiliar with security requirements/regime.

Consequences

- Potential loss or compromise of classified information or assets.
- Reputational damage.
- Potential for operational readiness to be compromised.

Current and planned actions to manage the risk

- Ensure strict adherence to the clear desk policy
- Compliance with NICS policies and procedures issuing from the Departmental Security Officer.
- Regular change of access codes for CCPB office suite and restriction of the individuals being given the code
- Staff familiarisation and training as required.
- Maintenance of CCPB asset register.
- Relevant security clearance obtained for staff
- Staff familiarisation of and compliance with all Security policies in relation to the operation of the IT equipment.

Risk Assessment (after current and planned actions)	Impact	Likelihood	Overall Risk Assessment
			
Business Plan Objective(s)	NO DIRECT LINK TO DEPARTMENTAL BUSINESS PLAN To ensure safe custody of all assets for which CCPB has responsibility including the former RGHQ site and information assets including personal data. 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				