Corporate Risk 876 – TfN Cyber Security

March 2024

Risk Manager: Daniella Della-Cerra-Smith

IT and Information Manager: Danny Chapman

The Audit and Governance Committee are encouraged to review the following risks prior to the meeting to allow for feedback during the corporate risk review/deep dive.

Purpose of Deep Dives:

- Allow the Audit and Governance Committee to undertake a comprehensive review of selected risks
- Provide the opportunity to check and challenge selected risks in more detail to ensure completeness, integrity and accuracy of data
- Demonstrate that the Audit and Governance Committee provide due diligence in the assurance of risk management
- Recommend areas for consideration, if required.

Sample Deep Dive Questions:

1. Is the risk description, cause and impacts articulated clearly?
2. Is the risk scored against TfN's Risk Management Criteria?
3. Are there controls, actions and fallbacks in place?
4. Are the controls, actions and fallbacks effective enough to achieve the target score?
5. Any additional comments/ areas for consideration?

5 x 5 Threat Impact Scoring Criteria

Likelihood Criteria	Very Low	Low	Medium	High	Very High
	≤5%	6-25%	26-50%	51-74%	>75%
Impact Criteria	**Very Low**	**Low**	**Medium**	**High**	**Very High**
Cost (Tier 1 - £0-£2m Budget)	£0 - £10k	£10k - £20k	£20k - £50k	£50k - £80k	£80k - £100k
Reputation	Minimal negative local media coverage quickly remedied /loss of trust and credibility	Minor negative local media coverage quickly remedied /loss of trust and credibility	Moderate negative regional media coverage/loss of trust and credibility	National short – term negative media coverage/considerable loss of trust and credibility	National long – term negative media coverage, significant loss of trust and credibility
External Relationship	Minimal strained relationship with partners/third parties	Minor strained relationship with partners/third parties	Moderate strained relationship with partners/third parties	Evidence of relationship issues with partners/third parties	Severe relationship issues with partners/third parties
Quality	Work is fit for purpose but may require minimal changes	Work is fit for purpose but may require minor changes	Moderate changes or specialist resource required to provide high quality outputs	Scope changes required to provide high quality outputs	Project outputs are not credible/robust, with no assurance and partners do not endorse reports
Time	0 – 1 month	1 – 3 months	3 – 9 months	9 – 12 months	12 – 18 months

5 x 5 Opportunity Scoring Criteria

Likelihood Criteria	Very Low	Low	Medium	High	Very High
	≤5%	6-25%	26-50%	51-74%	>75%
Impact Criteria	**Very Low**	**Low**	**Medium**	**High**	**Very High**
Cost (Tier 1 - £0-£2m Budget)	£0 - -£10k	-£10k - -£20k	-£20k – -£50k	-£50k - -£80k	-£80k - -£100k
Reputation	Minimal positive local media coverage/ increase of trust and credibility	Minor positive local media coverage/increase of trust and credibility	Moderate positive regional media coverage/increase of trust and credibility	National short – term positive media coverage/considerable increase of trust and credibility	National long – term positive media coverage, significant increase of trust and credibility.
External Relationship	Minimal increase in TfN's relationships with partners/third parties	Minor increase in TfN's relationships with partners/third parties	Moderate increase in TfN's relationships with partners/third parties	There is considerable evidence that TfN's relationships with partners/third parties is increasing	Relationships with partners/third parties significantly increased, benefitting TfN's credibility
Quality	Work is high quality with minimal changes	Work is high quality with minor changes	Moderate changes and no additional specialist resource to provide very high-quality outputs	Scope changes not required to exceed high quality outputs	Exceeds credible/robust project output expectations, with assurance & partners endorse reports
Time	0 – -1 month	-1 – -3 months	-3 – -9 months	-9 – -12 months	-12 – -18 months

Corporate Risk 876

Description	Actions	Owner	Due Date
Cyber disruption/attacks to the available information and technical infrastructure. Inappropriate user access to confidential information. Access may be limited for an unknown period.	1. IT and Data Policies are in place, reviewed, and updated in line with known cyber threats. 2. Training to all TfN staff on new policies. 3. Communications Plan in place for regular updates to employees when required. 4. Monitoring and compliance checks performed (e.g. phishing attacks). 5. On-going/monitoring security updates performed to user devices and software services. 6. Business Continuity Plan checks, system reviews and restoration timescales regularly assessed. 7. Insurance cover in place for ransoms where required. 8. Ensure multifactor authentication in place for all TfN accounts.	1. DC 2. DC 3. DC 4. DC 5. DC 6. DC 7. DC 8. DC	1. Ongoing 2. Ongoing 3. Ongoing 4. Ongoing 5. Ongoing 6. Ongoing 7. Ongoing 8. Ongoing
Cause			
Hacking, denial of services, phishing, fraudulent activities and inappropriate security access granted.			
Impact			
Site outages, loss of resource time, which could impact on programme timescales, impact on cost for restoration of resources and information. Ransomware, compromise of information, potential legal implications due leakage of data/GDPR fines which leads to reputational challenges.			

Current Score	Target Score
10	10

Current Assessment						Target Assessment					
Probability Rating	External Relationship	Reputation	Financial Rating	Quality	Time Rating	Probability Rating	External Relationship	Reputation	Financial Rating	Quality	Time Rating
Medium	Medium	Medium	Medium	n/a	Very Low	Medium	Medium	Medium	Medium	n/a	Very Low