

Generic Risk Register on which CENTR members may build their own specific ones

Impact Types

Trigger	Likelihood	Impact	Financial	Reputational	Service	Countermeasures	Check
1. Financial							
1.1 Legal suit by another party	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i> Provide good service Take legal advice act in good faith operate in a transparent and consistent manner provide proper notice Be honest <i>Minimize impact</i> If liable: negotiate or offer compromise/compensation <i>Transfer risk</i> Get government immunity if possible indemnity clauses <i>Insure</i> Purchase insurance cover - Errors and omissions <i>Reaction plan</i> If liable, deal with quickly if not, fight strongly (weighing the costs of litigation) settlement can include confidentiality provisions	N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A
1.2 Legal action against an infringer	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i> Avoid leaving yourself open monitor & issue early warnings <i>Minimize impact</i> Keep good evidence (I.e. complete and accurate records) get interim injunctions ex parte if necessary <i>Transfer risk</i> depending on situation, get other affected parties to sue instead bring criminal charges <i>Insure</i> litigation reserve funds <i>Reaction plan</i> Take as strong and quick action as possible get interim injunctions	N/A N/A N/A N/A N/A N/A N/A N/A
1.3 Minor errors in operating registry (e.g. low usage registration dropped for a short time)	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i> Establish good procedures and audit. Implement quality assurance standards such as ISO9002. <i>Minimize impact</i> Establish good customer support and general PR <i>Transfer risk</i> Suitably worded Terms & Conditions <i>Insure</i> Self-insure by maintaining a reserve fund <i>Reaction plan</i> Act quickly to recover negotiate and offer compensation	N/A N/A N/A N/A N/A N/A
1.4 Major errors in operating registry (e.g. very high usage registration dropped for a short time)	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i> Establish good procedures and audit. Implement quality assurance standards such as ISO9002. <i>Minimize impact</i> Establish good customer support and general PR <i>Transfer risk</i> Suitably worded Terms & Conditions <i>Insure</i> Errors and Omissions <i>Reaction plan</i> Act quickly to recover negotiate and offer compensation	N/A N/A N/A N/A N/A N/A
1.5 Fraud from outside organization	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i> Establish good procedures and audit. Implement quality assurance standards such as ISO9002. authenticate persons with whom you deal <i>Minimize impact</i> <i>Transfer risk</i> <i>Insure</i> Purchase insurance cover self-insure <i>Reaction plan</i> Sue for recovery write-off	N/A N/A N/A N/A N/A N/A N/A
1.6 Fraud from within organization	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i> Establish good procedures and audit. Implement quality assurance standards such as ISO9002 internal checks and balances <i>Minimize impact</i> Limit powers of individual staff	N/A N/A N/A N/A

						<i>Transfer risk</i>	Establish appropriate staff contracts	N/A
						<i>Insure</i>	Purchase insurance cover self-insure	N/A
						<i>Reaction plan</i>	Sue for recovery write-off	N/A
1.7 Fined by competition or regulatory authorities	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Get good legal advice Political lobbying	N/A
						<i>Minimize impact</i>	Establish good rapport political lobbying	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Purchase insurance cover self-insure	N/A
						<i>Reaction plan</i>	Fight in courts pay up cooperate	N/A
1.8 Unexpected sudden jump in costs (e.g. external supplier of bandwidth or hosting)	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Market analysis maintain good supplier relations	N/A
						<i>Minimize impact</i>	Do not depend on only a few suppliers avoid signing the contract in a foreign currency.	N/A
						<i>Transfer risk</i>	Write possibility for price increases into customer contracts	N/A
						<i>Insure</i>	Establish contingency fund	N/A
						<i>Reaction plan</i>	Re-negotiate find alternatives increase prices	N/A
1.9 Unexpected drop in revenues (1-6 months)	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Market analysis and monitor trends carefully	N/A
						<i>Minimize impact</i>	Minimize fixed overheads, especially ability to hire/fire staff	N/A
						<i>Transfer risk</i>	Diversify into other lines of business	N/A
						<i>Insure</i>	Fund to pay staff over market dips and pay redundancy	N/A
						<i>Reaction plan</i>	Shed fixed costs and unneeded staff. Borrow sell assets	N/A
1.10 Unexpected increase Insurance premiums	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Market analysis employ a good broker sign long term contracts	N/A
						<i>Minimize impact</i>	different policies with locked in premiums	N/A
						<i>Transfer risk</i>	pass costs on to consumers	N/A
						<i>Insure</i>	Establish good working reserves	N/A
						<i>Reaction plan</i>	Reduce cover Pay up Increase prices Borrow sell assets	N/A
1.11 Unexpected increase in taxation or social security costs	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Maintain political intelligence	N/A
						<i>Minimize impact</i>		N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Establish good working reserves	N/A
						<i>Reaction plan</i>	increase prices sell assets Borrow	N/A
1.12 Customers do not pay bills	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Don't give credit Limit credit Employ credit controllers Require money on account Vet customers - bank references	N/A

<i>Minimize impact</i>	Do not be reliant on only a few customers	N/A
<i>Transfer risk</i>	Factor the invoices	N/A
<i>Insure</i>		N/A
<i>Reaction plan</i>	Chase aggressively	N/A
	Take legal action to recover debt	N/A

2. Regulatory

2.1 Onerous political intervention or regulation	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Political lobbying understand political agenda	N/A
						<i>Minimize impact</i>	Ensure business model not too dependent on one view	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Adapt to it fight it in court move out of country	N/A
2.2 ICANN enforces unacceptable changes or threatens removal from root	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Engage with ICANN form strategic alliances internationally	N/A
						<i>Minimize impact</i>	Ensure business model not too dependent on one view	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Engage government sue in courts	N/A

3. Distractonal

3.1 Responding to investigations or enquiries by regulator or authorities	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Educate in advance Positive PR Train staff to deal with	N/A
						<i>Minimize impact</i>	Cost into operating budget and prices ensure that Registry is immune from any liabilities involved in complying	N/A
						<i>Transfer risk</i>	Become part of government	N/A
						<i>Insure</i>	Budget for costs	N/A
						<i>Reaction plan</i>	Change operation to accommodate requests	N/A
3.2 Responding to customer complaints	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Good web site and FAQs train customer support staff	N/A
						<i>Minimize impact</i>	Prepare "standard" responses cost into budget and prices	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Budget for costs	N/A
						<i>Reaction plan</i>	Deal with quickly and politely empower staff to resolve problems quickly	N/A
3.3 Responding to user complaints directly to MPs, government officials or regulator	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Educate in advance Positive PR Train staff to deal with	N/A
						<i>Minimize impact</i>	Prepare "standard" responses cost into budget and prices	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Budget for costs	N/A
						<i>Reaction plan</i>	Deal with quickly and politely	N/A
3.4 Dealing with potentially disruptive proposals by ICANN	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Engage	N/A
						<i>Minimize impact</i>		N/A
						<i>Transfer risk</i>	maintain independence Become part of government	N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Stay informed and collaborate	N/A
3.5 Dealing with cowboys or crooks	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Educate public	N/A

						<i>Minimize impact</i>	develop code of practice	N/A
						<i>Transfer risk</i>	Engineer procedures to remove their opportunities	N/A
						<i>Insure</i>	Budget for costs	N/A
						<i>Reaction plan</i>	Swift press campaign undo damage quickly	N/A
3.6 Working on diversification or new lines of business	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Do not consider it and stay "within your box"	N/A
						<i>Minimize impact</i>	Build into long-term strategic planning	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Allocate staff and ringfence budget	N/A
4. Reputational								
4.1 Being authoritarian and monopolistic	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Consider all stakeholders provide excellent service do the minimum	N/A
						<i>Minimize impact</i>	Good PR political lobbying promote competition	N/A
						<i>Transfer risk</i>	Become part of government	N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Review strategic structure and choices; PR	N/A
4.2 Being unresponsive to customer concerns	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Provide excellent service fund people for customer support	N/A
						<i>Minimize impact</i>	Deal with issues quickly phone rather than e-mail	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Develop better customer skills offer better service charge more	N/A
4.3 Being unresponsive to concerns from government, regulators etc	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Talk to them in advance don't abuse position provide excellent service	N/A
						<i>Minimize impact</i>	Deal with issues quickly phone rather than e-mail	N/A
						<i>Transfer risk</i>	Become part of government	N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Put money into forging political contacts at high level	N/A
4.4 Being financially imprudent	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Know the figures monitor the budget control who can spend audit	N/A
						<i>Minimize impact</i>	Build up good working capital and reserves	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Thoroughly review finances, costs and prices remove errant staff	N/A
4.5 Lacking in transparency with setting policies	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Enforce consultation engage with all relevant stakeholders	N/A
						<i>Minimize impact</i>	Be more open minimize role of registry	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Publish more openly	N/A

							PR review policy-making mechanisms	N/A
4.6 Scandal or reputational failure of senior executives	Not selected	Not	Not	Not	Not	Minimize likelihood Minimize impact	Establish appropriate recruitment procedures Build bank of goodwill with media	N/A
						Transfer risk Insure Reaction plan		N/A
4.7 Employment tribunal brought by staff	Not selected	Not	Not	Not	Not	Minimize likelihood Minimize impact	Invoke PR crisis plan Be fair to staff communicate and listen Good HR policies management/supervisor training Employ only subcontractors	N/A
						Transfer risk Insure Reaction plan		N/A
4.8 Being linked with another organization whose reputation becomes tarnished	Not selected	Not	Not	Not	Not	Minimize likelihood Minimize impact Transfer risk Insure Reaction plan	Investigate partners in advance and monitor regularly Build bank of goodwill with media	N/A
						Reaction plan	Invoke PR crisis plan	N/A
4.9 Someone else passing themselves off as you or otherwise misrepresenting you	Not selected	Not	Not	Not	Not	Minimize likelihood Minimize impact Transfer risk Insure Reaction plan	Register, enforce and publicize brands and IP Monitor external view of yourself and act quickly	N/A
						Reaction plan	Vigorously pursue and defend in courts maximize PR	N/A
5. Procedural								
5.1 Exploitable loophole in procedures	Not selected	Not	Not	Not	Not	Minimize likelihood Minimize impact	Good design, test and audit staff training Tripwire monitoring fallback procedures	N/A
						Transfer risk Insure Reaction plan		N/A
5.2 Procedure declared unlawful	Not selected	Not	Not	Not	Not	Minimize likelihood Minimize impact Transfer risk Insure Reaction plan	Legal advice in advance Arrange for legislation to be passed in support of procedure	N/A
						Reaction plan	Fight in court; suspend and re-engineer procedure	N/A
5.3 Procedures too complex or too impractical to follow	Not selected	Not	Not	Not	Not	Minimize likelihood Minimize impact	Anticipate in design trial runs Monitor performance engage with staff who operate	N/A
						Transfer risk Insure Reaction plan	Outsource	N/A
5.4 Sabotage from internal source	Not selected	Not	Not	Not	Not	Minimize likelihood Minimize impact	Re-engineer in simpler form Establish good procedures and audit peer review internal checks and balances proper back up procedures on-site security and monitoring Limit powers of individual staff	N/A

						<i>Transfer risk</i>	Establish appropriate staff contracts	N/A
						<i>Insure</i>	Purchase cover	N/A
							Self insure	N/A
						<i>Reaction plan</i>	Lockdown	N/A
							investigate	N/A
							prosecute	N/A
5.5 Volumes too high to follow procedures	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Anticipate in design	N/A
							extreme load test	N/A
							design data centre to handle peak loads	N/A
							hire additional staff	N/A
							automate	N/A
						<i>Minimize impact</i>	Monitor load and resources needed	N/A
							train staff	N/A
						<i>Transfer risk</i>	Outsource	N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Engage temporary staff	N/A
							upgrade hardware	N/A
							Outsource	N/A
6. Premises including external data centres (see also 11.6)								
6.1 Short term evacuation for external reasons (petrol tanker on fire outside; riot or demonstration in street)	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Choose "good" neighbourhood	N/A
							enforce boundary restrictions	N/A
						<i>Minimize impact</i>	Business backup site	N/A
							homeworking	N/A
							key information offsite	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Purchase cover	N/A
						<i>Reaction plan</i>	Invoke emergency plan	N/A
							telephone cascade procedure	N/A
6.2 Short term problem with the buildings (Legionnaires disease; dead body found; major break-in)	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Good building maintenance & hygiene	N/A
						<i>Minimize impact</i>	Business backup site	N/A
							homeworking	N/A
							key information offsite	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Purchase cover	N/A
						<i>Reaction plan</i>	Invoke emergency plan	N/A
							telephone cascade procedure	N/A
6.3 Serious damage to the buildings some material/resources recoverable (Fire, hurricane; earthquake, flood, bomb)	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Good building design	N/A
							compartmentalize key areas	N/A
						<i>Minimize impact</i>	Business backup site	N/A
							homeworking	N/A
							key information offsite	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Purchase cover	N/A
						<i>Reaction plan</i>	Invoke emergency plan	N/A
							recover material	N/A
							inform staff	N/A
6.4 Total destruction of buildings - nothing recoverable (Airliner crash, earthquake; bomb)	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Sensible location of building	N/A
							perimeter security	N/A
						<i>Minimize impact</i>	Business backup site; homeworking	N/A
							key information offsite	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Purchase cover	N/A
						<i>Reaction plan</i>	Invoke emergency plan	N/A
							inform staff	N/A

							recover material	N/A
7. People								
7.1 Mass resignation (disaffection; group lottery win)	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Good HR, communication & management small syndicates	N/A
						<i>Minimize impact</i>	Keep in touch with former staff develop contingency plan	N/A
						<i>Transfer risk</i>	Outsource	N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Invoke contingency plan hire emergency staff	N/A
7.2 Loss of key staff	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Career progression plan succession planning group travel policy	N/A
						<i>Minimize impact</i>	knowledge in >1 head document procedures understudies	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Key man: cover	N/A
						<i>Reaction plan</i>	Interim management	N/A
8. Corporate Governance								
8.1 Hostile takeover attempt	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Legal structure voting rights share restrictions legislation	N/A
						<i>Minimize impact</i>	Provide excellent service good PR political lobbying	N/A
						<i>Transfer risk</i>	Become part of government	N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Fight legally lobby public, government, shareholders	N/A
8.2 Conflict between stakeholder groups	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Provide equitable service balance rights	N/A
						<i>Minimize impact</i>	Provide excellent service good PR political lobbying	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Mediate review governance structure	N/A
8.3 Shareholder revolt	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	No shareholders or members spread over large number	N/A
						<i>Minimize impact</i>	Provide excellent service good PR political lobbying	N/A
						<i>Transfer risk</i>	Become part of government	N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Communicate improve service better dividends	N/A
9. Obsolescence								
9.1 Replacement (i.e. Alternative Roots) for DNS gains rapid acceptance	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Detect in advance by participate in IETF & forums	N/A
						<i>Minimize impact</i>	Develop run-down plan embrace alternative	N/A

								diversify into new business	N/A
								<i>Transfer risk</i>	N/A
								<i>Insure</i>	N/A
								<i>Reaction plan</i>	N/A
								Establish run-down fund	N/A
								Downsize & run-down operation	N/A
								wind up organisation	N/A
9.2 Massive switch to .eu from your own cc	Not selected	Not	Not	Not	Not			<i>Minimize likelihood</i>	N/A
								Provide excellent service	N/A
								promote your own cc	N/A
								<i>Minimize impact</i>	N/A
								Monitor to detect in advance	N/A
								diversify into new business	N/A
								<i>Transfer risk</i>	N/A
								<i>Insure</i>	N/A
								<i>Reaction plan</i>	N/A
								Lower price	N/A
								improve service	N/A
								promote your own cc	N/A
								downsize	N/A
10. Health and Safety									
10.1 Epidemic among staff	Not selected	Not	Not	Not	Not			<i>Minimize likelihood</i>	N/A
								Promote health awareness; private healthcare and screening	N/A
								private healthcare and screening	N/A
								build strong and valuable brand	N/A
								<i>Minimize impact</i>	N/A
								Plan for backup site, phone redirection & remote working	N/A
								cooperative marketing strategies with .eu and RARs	N/A
								<i>Transfer risk</i>	N/A
								Outsource	N/A
								<i>Insure</i>	N/A
								<i>Reaction plan</i>	N/A
								Key man: cover:	N/A
								Inform staff	N/A
								provide treatment	N/A
								invoke contingency plan	N/A
10.2 Death, major accident, violence or murder at site resulting in building quarantine	Not selected	Not	Not	Not	Not			<i>Minimize likelihood</i>	N/A
								Review building safety	N/A
								monitor staff emotions	N/A
								vet visitors	N/A
								<i>Minimize impact</i>	N/A
								Plan for backup site, phone redirection & remote working	N/A
								<i>Transfer risk</i>	N/A
								Outsource	N/A
								<i>Insure</i>	N/A
								<i>Reaction plan</i>	N/A
								Inform staff	N/A
								invoke contingency plan	N/A
								use remote access	N/A
11. Technical									
<i>11.1 Core name servers</i>									
11.1.1 Serious hardware failure on critical systems	Not selected	Not	Not	Not	Not			<i>Minimize likelihood</i>	N/A
								Pre-purchase assessment	N/A
								good environment and power	N/A
								safe buildings	N/A
								deploy multiple systems	N/A
								<i>Minimize impact</i>	N/A
								Diversify hard- & software	N/A
								good remote and physical access	N/A
								train staff	N/A
								<i>Transfer risk</i>	N/A
								Outsource, manufacturer's support contracts	N/A
								<i>Insure</i>	N/A
								Invest capital in spares	N/A
								<i>Reaction plan</i>	N/A
								Hot swap parts and/or standby systems	N/A
								on-csll staff	N/A
								invoke plan	N/A
11.1.2 Successful denial of service attack	Not selected	Not	Not	Not	Not			<i>Minimize likelihood</i>	N/A
								Evaluate architecture	N/A
								multiple systems	N/A
								don't give hackers a reason to target you	N/A
								anycast	N/A
								increase maximum throughput	N/A

						<i>Minimize impact</i>	Intrusion detection monitoring	N/A
							collaboration with carriers/hosts	N/A
						<i>Transfer risk</i>	Outsource some servers	N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Re-configure block IP ranges	N/A
11.1.3 Zone file corruption	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Build on protected system verify then & after transfer incremental updates use well tested industry software	N/A
						<i>Minimize impact</i>	Phase updates over multiple servers over time	N/A
						<i>Transfer risk</i>	Limit liability with registrant contract	N/A
						<i>Insure</i>	Errors & Omissions: cover:	N/A
						<i>Reaction plan</i>	Version rollback investigate the cause immediately and thoroughly	N/A
11.1.4 Intermittent and non-obvious software bug.	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Evaluate systems diversify software platforms extreme stress testing	N/A
						<i>Minimize impact</i>	New features rollable back with no business embarrassment (beta test)	N/A
						<i>Transfer risk</i>	Contract with software supplier	N/A
						<i>Insure</i>	Invest in duplicate of live system for testing purposes	N/A
						<i>Reaction plan</i>	Rollback version and/or new features	N/A
11.1.5 Key staff needed to fix outage unavailable for prolonged period.	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Key skills with >1 person on-call staff with multiple communications	N/A
						<i>Minimize impact</i>	Good remote & homeworking tools to operational staff documentation	N/A
						<i>Transfer risk</i>	Outsource	N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Invoke planned escalation procedures	N/A
11.2 Registration systems								
11.2.1 Serious hardware failure.	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Pre-purchase assessment good environment and power safe buildings	N/A
						<i>Minimize impact</i>	Hot standby systems	N/A
						<i>Transfer risk</i>	Outsource, manufacturer's support contracts	N/A
						<i>Insure</i>	Invest capital in spares	N/A
						<i>Reaction plan</i>	Hot swap parts switch to standby systems invoke contingency plan	N/A
11.2.2 Intermittent and non-obvious software bug.	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Full test environment before deployment software quality standards	N/A
						<i>Minimize impact</i>	New features rollable back with no business embarrassment (beta test)	N/A
						<i>Transfer risk</i>	Outsource contract with software supplier	N/A
						<i>Insure</i>	Invest in duplicate of live system for testing purposes	N/A
						<i>Reaction plan</i>	Rollback version and/or new features	N/A
11.2.3 Excessive registration , lookup or modification requests (including WHOIS abuse)	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Abuse policy for users automatic monitoring of limits and blocking	N/A
						<i>Minimize impact</i>	Realtime reporting of breaches to operations long-term trend analysis	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Manual intervention and blocking	N/A

							upgrade line and/or hardware speeds	N/A
11.2.4 Internet connectivity unavailable for prolonged period.	Not selected	Not	Not	Not	Not	Minimize likelihood	Diversify line supplier and particularly physical cable/fibre paths	N/A
						Minimize impact	Minimize business dependency on large data transfers	N/A
						Transfer risk	Contract with provider	N/A
						Insure		N/A
						Reaction plan	Switch to dialled; xDSL; or ISDN	N/A
							find new providers with spare capacity	N/A
11.3 Other key business systems								
11.3.1 Key staff needed to fix problems unavailable for prolonged period.	Not selected	Not	Not	Not	Not	Minimize likelihood	Key skills with >1 person	N/A
							phase holiday/absences across staff	N/A
						Minimize impact	Good documentation	N/A
							minimise criticality of all systems	N/A
						Transfer risk	Outsource	N/A
						Insure	Key Man cover	N/A
						Reaction plan	Re-deploy others	N/A
							engage temporary/contract staff	N/A
11.3.2 Serious hardware failure	Not selected	Not	Not	Not	Not	Minimize likelihood	Pre-purchase assessment	N/A
						Minimize impact	Hot standby system	N/A
						Transfer risk	Manufacturer's support contracts	N/A
						Insure	Invest capital in spares	N/A
						Reaction plan	Hot swap parts	N/A
							switch to standby system	N/A
11.3.3 Intermittent and non-obvious software bug.	Not selected	Not	Not	Not	Not	Minimize likelihood	Full test environment before deployment	N/A
							software quality standards	N/A
						Minimize impact	New features rollable back with no business embarrassment (beta test)	N/A
						Transfer risk	Outsource	N/A
							contract with software supplier	N/A
						Insure	Invest in duplicate of live system for testing purposes	N/A
						Reaction plan	Rollback version and/or new features	N/A
11.4 System security								
11.4.1 External hacker penetrates systems	Not selected	Not	Not	Not	Not	Minimize likelihood	High, certified security policy	N/A
							firewall	N/A
							tripwire	N/A
							staff training and awareness	N/A
						Minimize impact	Real-time monitoring & alarms	N/A
							develop plan for countermeasures	N/A
						Transfer risk		N/A
						Insure	Provide internal access mechanisms to counteract lockout by hacker	N/A
						Reaction plan	Provide honey pots	N/A
							monitor	N/A
							gather evidence	N/A
							prosecute	N/A
							publicise	N/A
11.4.2 Internal hacker penetrates systems	Not selected	Not	Not	Not	Not	Minimize likelihood	As 11.4.1 plus staff IT policy and limited superuser access	N/A
						Minimize impact	Real-time monitoring & alarms	N/A
							develop plan for countermeasures	N/A
						Transfer risk		N/A
						Insure	Provide internal access mechanisms to counteract lockout by hacker	N/A
						Reaction plan	Provide honey pots	N/A
							monitor	N/A
							gather evidence	N/A
							publicise	N/A
11.4.3 Rogue, incompetent or "having a bad day" technical staff member	Not selected	Not	Not	Not	Not	Minimize likelihood	Enforce peer review of all critical operations	N/A
							employ change control	N/A

leaves backdoor open.						<i>Minimize impact</i>	Real-time monitoring & alarms; develop plan for countermeasures	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Provide internal access mechanisms to counteract lockout by hacker	N/A
						<i>Reaction plan</i>	Provide honey pots	N/A
							monitor	N/A
							gather evidence	N/A
							publicise	N/A
11.5 Databases								
11.5.1 Catastrophic storage failure	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Evaluate systems pre-purchase multiple systems or components	N/A
						<i>Minimize impact</i>	Comprehensive and tested backup system	N/A
							hot standby	N/A
							transaction log	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Business continuity	N/A
						<i>Reaction plan</i>	Recover on standby from backup	N/A
							replay transactions	N/A
11.5.2 Subtle and progressive data corruption.	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Extreme load testing	N/A
							software quality standards	N/A
							change control	N/A
						<i>Minimize impact</i>	Comprehensive and tested backup system also storing transaction logs	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Rollback software version	N/A
							recover from backups	N/A
							replay transactions	N/A
11.6 Data centre (within or distinct from office)								
11.6.1 Fire	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Fire retardant walls & doors	N/A
							high temperature alarms	N/A
							staff policies	N/A
						<i>Minimize impact</i>	Fire suppressant system	N/A
							duplicate facility elsewhere	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Fire: cover	N/A
						<i>Reaction plan</i>	Switch to backup site	N/A
11.6.2 Building intact but inaccessible (e.g. fire in next door building)	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Choose building site carefully	N/A
						<i>Minimize impact</i>	Design for and test full remote operations, including reboot and console	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Fire cover	N/A
						<i>Reaction plan</i>	Switch to remote operation	N/A
11.6.3 Power supply failure	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Choose good quality power supply company	N/A
						<i>Minimize impact</i>	Battery backup and diesel generator	N/A
							duplicate facility elsewhere	N/A
						<i>Transfer risk</i>	Contract with utility supplier	N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Monitor generator performance	N/A
							shed load	N/A
							Switch to duplicate facility	N/A
11.6.4 Physical damage - flood, hurricane etc	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Choose site carefully	N/A
							good building maintenance	N/A
						<i>Minimize impact</i>	Duplicate facility elsewhere	N/A
							highly protect data centre within building	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Other hazard: cover:	N/A

						<i>Reaction plan</i>	Switch to duplicate facility	N/A
11.6.5 Physical damage - theft or vandalism	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Treat data centre as very restricted area keep it secret CCTV monitoring	N/A N/A N/A
						<i>Minimize impact</i>	Duplicate facility elsewhere	N/A
						<i>Transfer risk</i>		N/A
						<i>Insure</i>	Theft, damage, vandalism: cover	N/A
						<i>Reaction plan</i>	Identify from CCTV secure site avoid disturbing evidence prosecute	N/A N/A N/A N/A
<i>11.7 Nameserver hosting</i>								
11.7.1 Loss of a nameserver hosting site	Not selected	Not	Not	Not	Not	<i>Minimize likelihood</i>	Choose hostings site and/or subcontractors carefully	N/A
						<i>Minimize impact</i>	Maximize number of independent secondaries	N/A
						<i>Transfer risk</i>	Subcontract diversification	N/A
						<i>Insure</i>		N/A
						<i>Reaction plan</i>	Determine if recoverable and seek replacement if not	N/A

Likelihood Mapping

High	10
Low	20
Medium	30

Impact Mapping

High	1
Low	2
Medium	3

Risk Profile

Likelihood	Impact		
	High	Medium	Low
High	0	0	0
Medium	0	70	0
Low	0	0	0

