Risk Register

Project: Vendor_Name
Date: XXXXX

Risk No.	Date raised	Raised by	Description	Area / Division	Team impacted	Assigned to	Likelihood	Consequence	Flag Status	Risk Mitigation / Actions to resolve	Comments	Due Date	Status	Audience
001			Data integrity is an issue with almost all OSS/NMS, particularly with cross-domain information. - OSS Vendor expects CSP will be responsible for data discrepancies and resolution (i.e. data cleansing). - OSS Vendor states that it assumes data migration issues will be resolved by the CSP within 10 working days so turnaround expectations are quite tight				H	M	High	* Work with OSS vendor to develop data migration plan * The DM (Data Migration) Plan should ensure appropriate master-slave data-flow relationships are identified * In addition to vendor's reconciliation capabilities, CSP to develop processes to ensure master data is kept as accurate as possible (regular audits, audits as standard part of build activities, etc) * Set the expectation with operations groups (ie that we will be requesting their help to gather and perhaps cleanse data) * Allocate the resources to cleanse or create data			Open	External
002			Full requirements analysis and specification not done until after signing contract, which means we don't know for sure what all the real business requirements are and risks having to do re-work later. Lack of familiarity by CSP staff with the OSS application makes the analysis and definition phase difficult for them				H	H	High	* Identify the areas of specification needed by the vendor (eg what data objects are required, etc) * Preliminary requirements definition to be done as soon as possible * AGILE development methodology could be considered by vendor * Seek access to vendor sandpit as early as possible			Open	External
003			CNDB stores part of cross-domain information but full data sets would need to be created manually				H	M	High	* Significant data mapping exercise required * Develop process for data collection during routine maintenance * Ensure appropriate master-slave data-flow relationships and develop processes to ensure master data is kept as accurate as possible (regular audits?) * Set the expectation with operations groups (ie that we will be requesting their help to create / cleanse data)			Open	Internal
004			Reticence of key stakeholders to accommodate change caused by OSS rollouts				H	H	High	* Change management strategies to be developed. Involve and inform, particularly the potential blockers * Establish detailed workflow diagrams, responsibility charts and training packs to help with the change management process. This should be closely coordinated with the Business Analyst			Open	Internal
005			Northbound interfaces (NBI) on OSS software modules, NE's or existing NEMS may not support any or all of the full scope of FCAPS that we wish to achieve. Reduces overall capability or significantly increases mediation complexity				M	M	Medium	* Allocate resources to lock-down interface capabilities and determine a way forward * Identify any additional modules or packages required from equipment vendors to activate NBI			Open	Internal
006			CSP has a number of unique aspects of its data design that are necessitated by protection of assets. These diverge slightly from the "standard" architectures that vendors build their systems around. Some vendors may not be able to support the CSP's network designs without customisation				M	M	Medium	* CSP to create a service modelling document that describes all types of protection * Work with vendor to model these services in their applications to ensure capability to model CSP designs			Open	Internal
007			Vendor solutions may be fantastic products, but not necessarily have all the features relating to CSP business needs (particularly visualisation and presentation needs)				M	M	Medium	* Workarounds will need to be developed in conjunction with the vendor to overcome any gaps between requirements and product capability * Project Team to set this expectation with operational teams to acknowledge that some functionality may be lost in gaining a lot of new functionality * The period of post*production support by vendor is important			Open	Internal
008			High availability, protected platforms are required to overcome business continuity risk. The CSP's SOE doesn't fully align with OSS vendor preferred HA infrastructure				L	H	Medium	* OSS Vendor HA architecture looks solid but not per CSP SoE * Commence HA, diversity, backup, restore and general DR (Disaster Recovery) planning * Consider vendor recommendations as priority rather than SoE to avoid performance degradation			Open	External
009			Some NMS/EMS that will be feeding the CSP OSS are legacy / End-of-Life. This is a business continuity risk as it may be difficult to find the appropriate support/development skill-set to assist the vendor. One of OSS Vendor's assumptions is that the selected interface will be available at the end of design stage so if the interfaces aren't available then there could be significant delays in the project roll-out				M	M	Medium	* Identify third-party vendor contacts ASAP * Work with equipment vendor to perform up-front analysis of each of the NMS/EMS and NBI to determine the level of risk and to then ensure that interfaces are activated and documented * Establish mitigation strategies on a case-by-case basis			Open	Internal

Risk Rating

Likelihood	Consequence		
	Low	Medium	High
High	M	H	H
Medium	L	M	H
Low	L	L	M

LEGEND

H	**High Risk**	Immediate program-level attention needed
M	**Medium Risk**	Project-level planning required
L	**Low Risk**	Manage by normal procedures

Risk Rating matrix is derived from the following two tables

Consequence

Level	Descriptor	Description
Low	Insignificant	No time delays, low/no financial loss
Medium	Moderate	High time delays or effort required, high financial
High	Catastrophic	Massive time delays or effort required, huge financial

Likelihood

Level	Descriptor	Description
High	Almost certain	Is expected to occur in most circumstances
Medium	Possible	Might occur at some time
Low	Unlikely	Could occur at some time