Risk management checklist

ERMF: Enterprise Risk Management Framework; ERMP: Enterprise Risk Management Process	Yes	No*	If no …
Mandate and commitment			
• Are staff aware of the elements and processes of DETE ERMF and ERMP?			Make sure that staff know how to access the ERMF and ERMP
• Are staff equipped with the knowledge, skills and capabilities to effectively manage risks?			Contact GSP to discuss training requirements
• Do staff understand their accountabilities, roles and responsibilities for management of risks?			
• Are staff fully trained in their risk management responsibilities?			
• Has a person in the division been identified to be responsible for supporting risk management?			Appoint a risk champion
Establish the Context			
• Do you understand the internal and external context within which your area operates, including your stakeholders?			Spend more time doing operational planning. Contact GSP for help if necessary
• Do you have clear objective/s (or strategies) that link to the DETE strategic plan?			
• Do you have business rules/mechanisms for managing (identifying, recording, monitoring, escalating, reporting, communicating/consulting) operational risks?			Review the ERMP and apply to local practices
• Have you communicated those business rules to staff?			
• Do staff understand the DETE risk assessment criteria and acceptable risk levels?			Contact GSP to discuss training requirements
Risk Identification			
• Has a comprehensive process been used for identifying risks?			Spend more time identifying your risks. Consider a risk identification workshop involving key staff and customers. GSP can help if necessary
• Were appropriate management, staff and stakeholders involved in identifying risks?			
• Has enough information been collected about the risk to make decisions? (e.g. source, effect on objectives, causes, areas affected, control review)			
• Have risks been identified in relation to your objectives?			
• Are all of the risks 'risks', or have some actually happened, and are therefore issues?			Remove issues from the risk management process and manage them through an issues management process
For each risk:			
• Can the following elements be clearly identified in the risk statement (1) uncertain event? (2) cause? (3) effect on objectives?			Re-define your risk to identify these elements
• Has the risk category been allocated according to the cause of the risk?			Assign an appropriate risk category

ERMF: Enterprise Risk Management Framework; ERMP: Enterprise Risk Management Process	Yes	No[*]	If no …
• Has a risk owner been allocated to the risk?			Assign an appropriate risk owner
• Does the risk owner have the appropriate levels of authority, skills and knowledge to manage the risk?			
• Is the risk owner aware of their role and responsibility for managing the risk?			Ensure the risk owner is aware of their responsibilities
Risk Analysis			
• Has the risk level been assessed without controls in place and with controls in place, using tables 1 – 3 in the ERMP?			Use the tables to assess the inherent and controlled risk
• Is the assessment based on reliable information (past data, industry data)?			Seek additional data
• Were appropriate management, staff and stakeholders involved in assessing risks?			Seek input and advice from appropriate parties
• Have you identified the critical controls for the risk?			Spend time considering the controls you have in place and whether they are cost effective
• Do all of the controls that you've listed already exist?			Controls that are not already in place are treatment strategies
• Has someone who understands the risks and the controls assessed the effectiveness of controls using robust information?			Assess the control effectiveness
• Do the controls address the cause of the risk? Are they working as intended?			Consider introducing additional risk treatments
• Are there any control gaps?			
Risk evaluation			
• Is the controlled risk level below the department's tolerance?			You will need to design a risk treatment plan
• Have you prioritised the controlled risks so that you know which risks to treat first?			Prioritise risks
Treat Risks			
• Do high and extreme controlled risks have treatment plans?			You will need to design risk treatment plans
• Have stakeholders been consulted and involved in developing and evaluating treatment plans?			Consider your stakeholders
• Have you considered different treatment options for modifying the risk to an acceptable level? Have you evaluated the options, including cost/ benefit analysis and stakeholder implications?			'Think outside the box' when designing treatment plans
• If you thought controls were ineffective or that there are control gaps, does the treatment plan include ways to strengthen the controls?			Use this process to strengthen your controls
• For complex treatments: does the treatment plan contain actions, resources, responsibilities, timing, monitoring and reporting requirements? Have these resources been included in relevant budgets?			Make sure your treatment plan is comprehensive and resourced
• Has someone with the appropriate authority approved the treatment plan?			
• Do all parties understand their responsibilities for risk treatments?			Clearly assign responsibilities

ERMF: Enterprise Risk Management Framework; ERMP: Enterprise Risk Management Process	Yes	No*	If no …
• Has the treated risk been reassessed?			Reassess the risk
• If the risk is above the department's tolerance, but no further treatment options are available (e.g. if the risk is externally driven), has this been documented and escalated? Are contingency arrangements in place?			Record acceptance of risk and contingency arrangements. Escalate as required.
• Have high/extreme risks been escalated?			Escalate as required.
• Have you prioritised the residual risks so that you know where your highest exposures are?			Prioritise risks
• Are your risks recorded in ERA or in an offline risk register?			
Monitoring and review			
For each risk:			
• Have you worked through the checklist?			Review the checklist to make sure that your answers still apply
• Has the risk level changed?			Use this information to inform your re-assessment of control/ treatment effectiveness
• If so, what caused the change (i.e. external/internal environment, control/ treatment effectiveness)?			Use this information to inform your re-assessment of control/ treatment effectiveness
• Are there any new or emerging risks?			Analyse, evaluate and, if necessary, treat these as per the steps above
• Are identified risks still relevant?			Remove any risks that are now obsolete
• Did the risk eventuate (i.e. turn into an issue)? How effective were your treatments in addressing the consequences? What can you learn from that?			Remove any risks that are now obsolete
• Are risks being 'over controlled'?			Reduce or stop any controls that are excessive to reduce red tape and eliminate waste
• Are treatments still required? Have any treatments become ongoing controls?			Reduce or stop treatments that are no longer required to reduce red tape and eliminate waste. Update the risk register where treatments have become controls
• Have lessons learnt from the reassessment been identified and used to guide future risk management decisions?			Record and share lessons
Overall process:			
• Has the risk register been updated?			For risks recorded in ERA: forward changes to GSP For risks recorded in an off-line risk register: record any changes
• Is risk monitoring and review integrated with planning, performance management, budgeting, and other management processes?			Integrate processes
• Have your local business rules been reviewed in consultation with staff and stakeholders?			Make sure that you keep your documented business processes and rules up to date and accessible
• Are the business rules explicit, cohesive, and accessible?			Make sure that you keep your documented business processes and rules up to date and accessible