NSW RURAL FIRE SERVICE

POLICY P5.1.7
ICT DISASTER RECOVERY

ITEM	DESCRIPTION
Version Number	1.2
SOPs	› SOP P5.1.7-1 ICT Disaster Recovery Exemption
Owner	Executive Director, Infrastructure Services
Contact	Director, ICT
Approved Date	9 April 2018
Effective Date	10 April 2018
Next Review Date	9 April 2021
Document Control	Electronic - Printed Copies are Uncontrolled

1 Purpose

1.1 The NSW Rural Fire Service (NSW RFS) has implemented a Business Continuity Management (BCM) framework that includes the provision of a mirrored dual data centre arrangement with Disaster Recovery (DR) capabilities. This is because Information, Communication and Technology (ICT) services not covered by a DR capability pose a significant business continuity risk to the Service and its customers.

1.2 A DR capability gives the NSW RFS the capacity to provide key ICT services in the event of a catastrophic loss of IT assets or infrastructure. This may include, for example the loss of a data centre, i.e. either one of the Government Data Centres (Gov DC) at Silverwater or Unanderra.

1.3 An ICT DR policy allows the ICT Disaster Recovery (DR) Plan to be activated by the authorised officers, as nominated in the ICT DR plan.

1.4 The ICT DR plan should only be activated if both conditions of the following ICT Disaster definition are met:

a. an unexpected loss of ICT facility, infrastructure, service or personnel that degrades NSW RFS operational capabilities; and

b. the estimated time to restore that facility, infrastructure, service, person or capability to normal operations exceeds the agreed business outage tolerance.

2 Definitions

2.1 For the purpose of this policy document the following definitions apply:

a. **BCM:** Business Continuity Management;

b. **Business Owner:** the authorised position that represents the overall ownership (including short, medium and long term strategy) of an application or a system within the NSW RFS. For example:

i. Manager Aviation is the business owner for the Aircraft application;

ii. Manager Bushfire Information Line is the business owner for the applications BFIL, and BFIL FAQ.

c. **CIO:** NSW RFS Chief Information Officer;

d. **Disaster Recovery (DR):** To plan for continuity in the event of an unexpected loss of an ICT facility, infrastructure, business resource (including equipment and data), or personnel. This loss impacts on the NSW RFS ability to deliver core business functions or the loss of our ICT high availability capability;

The goal of disaster recovery is to resume normal computing capabilities in as little time as possible.;

e. **High Availability (HA):** Those ICT systems that contribute towards a high level of continuous service, without interruption. HA is delivered by implementing redundant components and fault tolerance;

f. **ICT:** the NSW RFS Information Communication and Technology section;

g. **NSW RFS:** the New South Wales Rural Fire Service;

h. **Risk Assessment:** the process outlined in Policy P7.1.10 Organisational Risk Management;

i. **The ICT Governance Group:** the group, comprising the NSW RFS Executive that considers and approves ICT initiatives;

3 Policy

3.1 NSW RFS Enterprise Architecture requires that all existing, new and upgraded production systems, data, and applications are DR compliant.

3.2 Most production systems, data and applications will also require HA.

3.3 Exemptions to DR shall be made to, and approved by, the ICT Governance Group and the CIO. If an exemption request is denied, it is the business owner's responsibility to ensure DR compliance.

3.4 It is the responsibility of the business owner to consult with all relevant parties before fully determining a solution's DR requirements and justification.

3.5 All aspects of the BCM framework and DR capability including analysis, design, implementation, costs and risk management should be determined before a business owner develops and submits a request for exemption.

3.6 All approved exemptions are to be reviewed annually by the CIO in consultation with the relevant business owner(s). This will ensure exemptions remain current and any new or potential dependencies are identified and assessed. Recommendations for continuation or removal of exemption will be presented to the ICT Governance Group for approval, by the CIO.

4 Related documents

- SS 1.1.26 Volunteer and Visitor Access to Network Services and Data
- P5.1.1 ICT Equipment Standards and Security
- P5.1.2 Acceptable Use of ICT
- P7.1.1 Project Management
- P7.1.9 Business Continuity Management
- P7.1.10 Organisational Risk Management
- ICT DR Exemption Request Form
- ICT DR Exemption Request process
- Information and Communications Technology (ICT) Disaster Recovery Planning Parts 1-3 (may be obtained on application to CIO)

5 Amendments

AMENDMENT DATE	VERSION NO	DESCRIPTION
14 December 2009	1.0	Initial release
1 July 2014	1.1	› Repealed and updated v1.0 › Reviewed to reflect Disaster Recovery and Exemption requirements
9 April 2018	1.2	› Repeals v1.1 › Administrative update › Clause 1.2

SOP P5.1.7-1
ICT DISASTER RECOVERY EXEMPTION

1 Purpose

1.1 This Standard Operating Procedure (SOP) details the procedures the NSW RFS will follow to review and manage Disaster Recovery (DR) Exemptions that is applications which have been approved not to have a Disaster Recovery Solution.

2 Procedures

Process flow chart

2.1 The ICT exemption process is shown at Appendix 1 below, and can be found on the ICT Community page of the intranet.

Exemption template

2.2 All exemptions should be submitted using the DR/HA Exemption template available on the ICT community page of the intranet.

2.3 The business owner shall submit the completed ICT DR Exemption Request form to the Manager, ICT Business and Major Projects for consideration by the ICT Governance Group and the CIO.

Production ICT solutions

2.4 NSW RFS Enterprise Architecture requires all production ICT solutions to have a DR capability. Most production systems will also require HA capability.

Business owner responsibilities

2.5 Business owners are responsible for conducting a risk assessment in accordance with P7.1.9 Business Continuity Management and P7.1.10 Organisational Risk Management.

2.6 All exemptions must be approved by the business owner's Director for submission to the Manager ICT Business and Projects.

2.7 Before submitting an exemption request, it is the responsibility of the business owner to consult fully with the Corporate Program Office, ICT and all other relevant parties.

ICT responsibilities

2.8 Where appropriate, ICT will assist business owners in completing the DR exemption request form by providing the ICT impact information including costs, resources and services affected by the exemption.

2.9 Upon implementation, ICT will support, maintain, monitor and upgrade all related ICT infrastructure and assets, subject to budgetary constraints.

2.10 The Manager ICT Business and Projects is the ICT contact point for all matters relating to ICT exemptions.

2.11 The CIO will liaise with the relevant Director(s) where required, including the ICT Governance Group.

ICT Governance Group responsibilities

2.12 The ICT Governance Group provides final approval on all exemptions and takes ownership of the associated risks.

2.13 Where approval of an exemption is made by the ICT Governance Group they are accepting the risk of the ICT solution being lost for an indeterminate period of time and the impact this loss might have on the NSW RFS and its customers.

Exemption register

2.14 ICT shall keep a register listing all approved exemptions. The register shall capture the application name and its purpose, business owner, ICT impacts, exemption approval and review dates.

Annual review

2.15 ICT will set up an automatic annual review reminder for all DR exemptions. All annual reviews should be accompanied by an audit trail of discussion, decisions and actions which shall be circulated to all relevant parties and the CIO.

2.16 The CIO shall submit recommendations for continuation or removal of DR exemptions to the ICT Governance Group for approval.

2.17 ICT DR annual review records may be subject to audit.

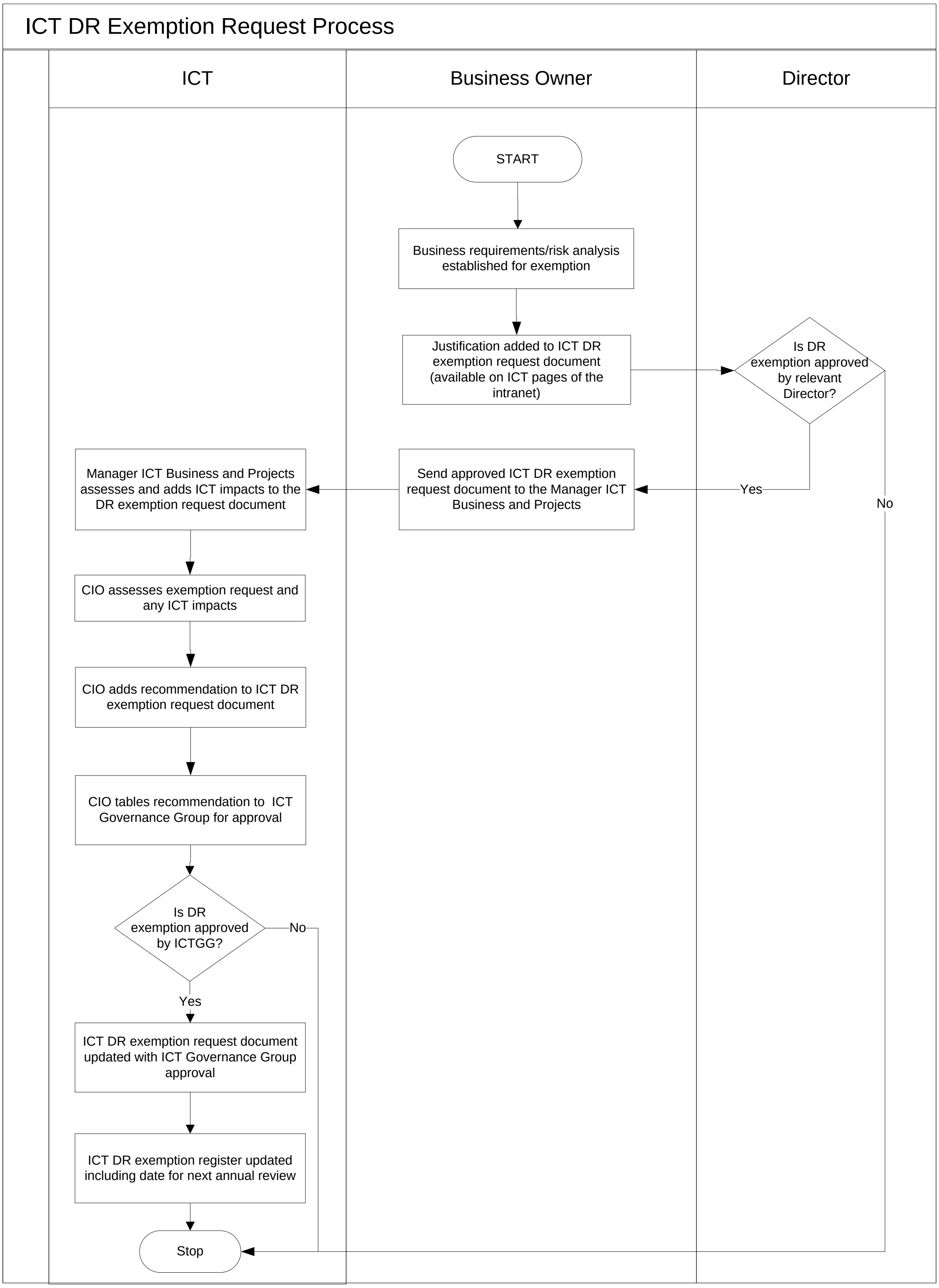
All other environments

2.18 The impact of losing an exempt solution/service should be considered before an exemption request is submitted. This includes the impact on all other production, test, staging, demonstration and DR environments.

3 Related forms

› ICT DR Exemption Request Form

Appendix 1


ICT DR Exemption Request Process
ICT
Business Owner
Director
START
Business requirements/risk analysis established for exemption
Justification added to ICT DR exemption request document (available on ICT pages of the intranet)
Is DR exemption approved by relevant Director?
Yes
No
Send approved ICT DR exemption request document to the Manager ICT Business and Projects
Manager ICT Business and Projects assesses and adds ICT impacts to the DR exemption request document
CIO assesses exemption request and any ICT impacts
CIO adds recommendation to ICT DR exemption request document
CIO tables recommendation to ICT Governance Group for approval
Is DR exemption approved by ICTGG?
No
Yes
ICT DR exemption request document updated with ICT Governance Group approval
ICT DR exemption register updated including date for next annual review
Stop