Assessment Information

CoreTrustSeal Requirements 2017–2019

Repository:	Australian Antarctic Data Centre
Website:	http://data.aad.gov.au/
Certification Date:	20 November 2018
This repository is owned by:	Australian Government, Antarctic Division

Core Trustworthy Data Repository Requirements

BACKGROUND INFORMATION

Context

R0. Please provide context for your repository.

Repository Type.

Domain or subject-based repository

Institutional repository

National repository system; including governmental

Research project repository

Other (please describe)

Comments

The Australian Antarctic Data Centre (AADC) serves as a data repository for the Australian Antarctic program (AAp).

The AADC is a "Domain or subject-based repository" because the AADC only deals with Antarctic and subantarctic data.

The AADC is an "Institutional repository" because it deals with multi-discipline scientific research, and is the primary repository for the AAp (other repositories are allowed for AAp researchers providing they have been pre-approved by the AADC).

The AADC is a "National repository system; including governmental" because the AAp is managed by the Australian Antarctic Division (AAD), which is a division of the Australian Federal Government, and is responsible for Australia's Antarctic and subantarctic interests. The AAp mandates that all researchers catalogue and archive their data with the AADC (or an alternative repository approved by the AADC).

The AADC is a "Research project repository" because the AAp directs Australian scientific efforts in the Antarctic and subantarctic, and requires scientific data to be catalogued and archived in the AADC (or an approved alternative).

Furthermore, the AADC was created to meet Australia's Antarctic Treaty obligations - specifically the part of the treaty that says, "to the greatest extent feasible and practicable scientific observations and results from Antarctica shall be exchanged and made freely available".

To see where the AADC fits within the AAD, see the following organisational chart: http://www.antarctica.gov.au/about-us/organisation-chart

Brief Description of the Repository's Designated Community.

The Australian Antarctic Program is focused on conducting world-class science of critical national importance and global significance that delivers on Australian Antarctic policy and operational priorities.

This includes managing Australia's presence and administering the Australian Antarctic Territory and the Southern Ocean, and the subantarctic Territory of Heard Island and McDonald Islands (HIMI) and their adjacent waters.

The Australian Antarctic Program utilises combined sea, air and continental transport capabilities to undertake wide-ranging marine, ice and aviation-based research activities, personnel transfer, station operation and resupply, and waste management and removal.

Antarctic science is a national priority and is the key mechanism through which Australia achieves its national interests in Antarctica. The Australian Antarctic Science Strategic Plan (2011–12 to 2020–21) guides the conduct of Antarctic science.

Major science programs and individual research projects are reviewed periodically in line with national and global research priorities. Collaborative research programs are also conducted with other Australian agencies, research institutions and international bodies.

The target community and intended users of the AADC are primarily researchers within the AAp. A smaller secondary group of users are researchers from outside the AAp, generally from other national Antarctic organisations, or other national or international universities or other research organisations that have a strong Antarctic focus. Finally, as the bulk of our data are freely available to anyone, the final group of users in our designated community is, "anyone else".

99.9% of our data contributors are from within the AAp.

Level of Curation Performed.

B. Basic curation – e.g. brief checking; addition of basic metadata or documentation
C. Enhanced curation – e.g. conversion to new formats; enhancement of documentation
D. Data-level curation – as in C above; but with additional editing of deposited data for accuracy

Comments

The AADC uses a range of curation levels depending on the quality of the data received. The AADC provides three basic tools to users in order to manage their data:

1) A project management tool - for keeping track of the data obligations related to an AAp project, and for the completion of Data Management Plans. https://data.aad.gov.au/aadc/projects/

2) A metadata authoring tool - for creating and editing metadata records that accompany data. https://data.aad.gov.au/metadata

3) A data submission tool - for uploading data into the AADC data archive. https://data.aad.gov.au/metadata

Provided a user has adequately prepared their dataset for archival, and have provided an appropriate amount of detail in their metadata record, then only "Basic curation" is needed. However, as every metadata record and dataset must be checked by the AADC metadata officer, then it is possible to adhere to reasonably stringent quality guidelines.

"Enhanced curation" takes place when the metadata officer reformats some datasets - for example, converting excel spreadsheets into csv format for increased storage longevity and assimilation with other data repositories (such as data.gov.au). Most submitted metadata records also require editing by the metadata officer in order to make them suitable for publication. Occasionally the metadata officer must liaise with the metadata author/data submitter in order to add more information to the metadata record, or to alter the submitted dataset.

"Data-level curation" occasionally takes place when submitted datasets can be improved or further utilised by being added to existing databases, or by having some data analysis performed on them.

Options "B" and "C" are the most routinely used levels of curation at the AADC.

Outsource Partners. If applicable, please list them.

The AADC does not explicitly outsource data repository activities, but it does allow AAp researchers to store their data at other approved repositories (for example, world data centres, other Antarctic or government repositories). Alternative repositories are vetted by the AADC manager to ensure that they are suitable. A copy of the criteria by which repositories are considered for approval are provided in **ANNEX A**. These criteria are maintained in an internal wiki.

Other Relevant Information.

The AADC maintains a data policy which governs data management activities within the AAp - https://data.aad.gov.au/aadc/about/data_policy.cfm

Furthermore, the AADC metadata catalogue and data repository are utilised by many other organisations.

1) The Global Change Master Directory (GCMD) provides metadata support to the international Antarctic community, providing national Antarctic portals for each country, as well as amalgamating all Antarctic metadata into the Antarctic Master Directory.
2) The Australian Ocean Data Network (AODN) harvests ocean related AADC metadata and data for use in the AODN Data Portal.
3) The Australian National Data Service (ANDS) harvests all AADC metadata for inclusion in its metadata catalogue.
4) The Australian Bureau of Meteorology (BoM) harvests all AADC metadata records for their own purposes.
5) Thomson Reuters harvests all AADC metadata for their Data Citation Index.
6) The Australian Government harvests AADC metadata for their data.gov.au tool (which brings together datasets from all across the Federal Government).

All AADC metadata records have a supporting citation for researchers to use. Many of these citations include a dataset DOI.

Reviewer Entry

Accept or send back to applicant for modification:
Accept

Comments:

ORGANIZATIONAL INFRASTRUCTURE

I. Mission/Scope

Compliance Level: 4

R1. The repository has an explicit mission to provide access to and preserve data in its domain.

The Australian Antarctic Strategic Plan 2010-11 - 2020-21 (http://www.antarctica.gov.au/__data/assets/pdf_file/0019/27307/AASSP_final-published-version_Apr-2011.pdf) identifies data management as an important ongoing activity for the Australian Antarctic program. Some excerpts are below:

"It is only by actively encouraging unfettered, timely access to scientific observations and measurements at the local, regional and global scale that we can hope to understand ecosystem processes and the earth system more generally, predict and address the consequences of global change and manage our resources in a sustained way. By making the output of the program widely and globally accessible through multiple communication channels, the full impact of the program can be realised in helping to address these complex system questions."

"The main outcomes that will be delivered through our approach to data and information are those that result in:

- efficient, interoperable and internationally networked data infrastructure delivered through collaboration
- enhanced public and researcher access to data
- minimisation of restrictions on data exploitation
- preservation of source data in a manner that permits long-term re-usability
- increased reliance on open source technologies and methodologies
- improved capacity to integrate multidisciplinary data to help derive innovative products and/or drive new scientific discovery
- maximised knowledge of the topographic, habitat and bathymetric characteristics of Antarctic and subantarctic territories and seas at regional and local scales."

The AADC also has a data policy (http://data.aad.gov.au/aadc/about/data_policy.cfm) which has been approved and endorsed by the executive of the AAD. The data policy clearly states what the responsibilities of the AADC are to AAp scientists, and what the data obligations of AAp scientists are.

The summary of the data policy is copied below:

Australian Antarctic Data Centre (AADC) Responsibilities

The AADC will ensure that:

- A wide range of Antarctic scientific data are managed for the long-term and made available in an easily accessible form,
- Metadata records are managed for all Australian Antarctic scientific research data and are made available for public searching in an effective form,
- Australian Antarctic program data are included in SCAR and other international data systems,
- It maintains current best practice in relation to its repository management functions and related systems,
- It maintains confidentiality of data during embargo periods,
- It facilitates the custodian's right to be cited as the source of published data,
- Information is provided to scientists on the resources that are available to support their work and advice is available on the design of data collection programs and effective data management strategies through assistance with developing Data Management Plans,
- Where possible individual datasets will be grouped into larger, aggregated data repositories to build more comprehensive data resources covering across the Antarctic, subantarctic and Southern Ocean.

AAp Scientist's Data Management Responsibilities

AAp Scientists will ensure that they:

- Comply with all aspects of the AAp Data Policy,
- Contact the Data Centre to discuss data issues preferably before submission of a Data Management Plan,
- Submit data (raw, processed and ancillary), derived products and associated metadata in an acceptable form to the Data Centre within the timelines set for data submission which is normally before the project's end date (see Table 1 for exceptions to project duration embargo periods).
- Make provision for the management of any physical samples in an appropriately catalogued collection,
- Provide updated information on progress against tasks in the Data Management Plan in annual Progress Reports (note this might be undertaken in collaboration with the AADC if the AADC is providing services to the project), and
- Adopt the norm of citing data used in their research by linking to metadata (or dedicated data papers) in peer reviewed publications.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

II. Licenses

Compliance Level: 4

R2. The repository maintains all applicable licenses covering data access and use and monitors compliance.

As a consequence of Australia's adherence to the Antarctic Treaty System and specifically Article (III).(1).(c), the Commonwealth of Australia will make AAp data publicly available via a Creative Commons "Attribution Only" license (see the Creative Commons Web site for more detail at http://creativecommons.org.au/learn/licences). Whenever a work is copied or redistributed under this type of Creative Commons licence, the original creator (and any other nominated parties) must be credited as the source of the data. This license has no other restrictions on use, however, all AAp data users are strongly urged to adopt the norms of behaviour anticipated of participants in the Polar Information Commons (PIC) community (see http://www.polarcommons.org/ethics-and-norms-of-data-sharing.html). A PIC badge, with links to these norms, is presented on all AADC metadata records.

As well as being badged with the CC-BY and PIC logos, each metadata record has a citation for the dataset prominently placed in order to encourage correct citation practices. For example - https://data.aad.gov.au/metadata/records/AAS_4326_microalga_toxicity

However, data archived with the AADC are not necessarily made publicly available immediately. We liaise with the contributing scientist to determine if the data can be made immediately public, or if it needs to be embargoed (for example because related papers have not yet been published).

Of course, while the AADC recommends that users cite their data sources according to the guidelines of a CC-BY licence, such a thing cannot easily be forced, and it is unrealistic to follow every dataset that has ever been downloaded from the AADC. However, the AADC does undertake to perform occasional "spot checks" to ensure that scientists are self-citing their data, or that AADC held data has been correctly cited by others. One such recent check did uncover an instance where CSIRO scientists had published a paper with incorrect citations - http://dx.doi.org/10.1038/sdata.2016.43. When contacted about it by AADC staff, the authors amended their published data set and also published a formal corrigendum correcting the citations: https://www.nature.com/articles/sdata2016111.

This has also been noted in section 11 of the AADC internal wiki detailing processes [**ANNEX B**]. This document is available on request to metadata@aad.gov.au. IT restrictions prevent the wiki being placed on a public site.

Further information about the conditions of use of data that we hold at the following link - https://data.aad.gov.au/aadc/about/condition_of_use.cfm

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

III. Continuity of access

Compliance Level: 4

R3. The repository has a continuity plan to ensure ongoing access to and preservation of its holdings.

The AADC is funded by the Australian Government as part of the Australian Antarctic Division, which is a division of the Department of Environment and Energy. As such it has considerable funding stability. The activities of the AADC are considered highly important by both the AAD and the Department of Environment and Energy, and it is extremely unlikely that funding will be removed.

In the unlikely event that something were to happen though, our metadata and data holdings would be secure through the following means:

1) The metadata catalogue would be preserved at the GCMD (which maintains the master copy of our metadata records). Copies of all our metadata records would also be available from ANDS, and subsets would exist at the AODN and various other organisations.
2) Data would be transferred to data.gov.au - which is an initiative of the Australian Government to provide data management services for its various departments - those that do not have a dedicated data repository (many of them do).
3) Data would also be transferred to the Institute for Marine and Antarctic Studies (IMAS). IMAS is part of the University of Tasmania, and has its own (new) Antarctic data centre for managing data arising from University Antarctic programs.
4) Ocean related data would be transferred to the AODN Data Portal, and to the Marine National Facility.
5) Some of our data holdings are also already available through other institutions like GBIF and OBIS.

This has also been documented in section 12 of the AADC internal wiki [**ANNEX C**] - this document is available on request. Contact metadata@aad.gov.au. IT restrictions prevent the wiki being placed on a public site.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

IV. Confidentiality/Ethics

Compliance Level: 4

R4. The repository ensures, to the extent possible, that data are created, curated, accessed, and used in compliance with disciplinary and ethical norms.

The AADC maintains five levels of "release status" for datasets - public, embargoed, confidential, and AAD only. For complete details, see the data policy - http://data.aad.gov.au/aadc/about/data_policy.cfm.

- public - the data are publicly available according to the conditions of a CC-BY licence.
- embargoed - the data are not publicly available, but it is envisioned that they will become so within a reasonable period of time.
- confidential - the data are not publicly available, and it is unlikely that they ever will be.
- AAD only - the data are only available to employees of the Australian Antarctic Division.
- In Review - the data are available via a specific link and password (intended for use by journal reviewers before publication).

A standard measure is that when a scientist provides data to the AADC, unless requested otherwise, we will embargo the data for a period of two years. This is to give the scientist time to publish their findings. This two year time frame is flexible though, and the AADC will not publicly release data without first getting the okay from the responsible scientist. If this is not possible (because the scientist can no longer be contacted, or is deceased), then approval to release the data can be obtained from the Chief Scientist of the AAD.

The five types of release status are used depending on the data archived. Most of our data are public, or at least will become public in the foreseeable future after a period of restriction (embargoed). Some data that we archive can never be made public (confidential data). The only way that confidential or embargoed data can be distributed is with the express written permission of the responsible scientist or data owner.

While the AADC does not require evidence that research has been carried out legally and ethically, the office of the AAD that is responsible for allocating funding to approved scientific projects is also responsible for ensuring that legal and ethical standards are met. Thus by the time data reaches the AADC for archival, we can be sure that legal and ethical guidelines have been followed. It is unlikely that the AADC will take any further action on ethics considerations for its data holdings (for example by adding a question about it to our data management plans) for the following reasons:

1) As mentioned above, ethics approvals are the province of an entirely different section of the AAp, and are not an AADC related activity.
2) Avoiding duplication of questions for researchers is a high priority for us - if researchers already have to go through an extensive ethics process with the ethics office we do not want them to have to repeat the effort with the AADC - all that does is create a perception that we are "wasting their time".

3) We have full confidence in the ethics office of the AAp and know that if projects do not comply with their findings they will not be approved, and therefore will not even be considered by the AADC with regards to data management.

Data are stored on secure servers at the AAD which are maintained according to Australian Government protocols. See later questions for details on IT processes.

Metadata records do contain contact information for scientists or data owners, but generally work contact details are used. Furthermore, contact details are typically provided by the users themselves under the understanding that they will be made available in the metadata record. Finally, contact details are typically not made available via the AADC, but only in the full version of our metadata records which resides at the GCMD (which is a component of NASA and required to adhere to US Federal Government standards).

Should someone wish to request access to an embargoed or confidential dataset, they would generally contact the AADC first, who would then pass the request onto the responsible scientist/data owner. As mentioned above, data are only released once written approval is obtained by the AADC from the responsible scientist/data owner.

All metadata and data uploads, and all requests for embargoed/confidential data pass through the AADC metadata officer. Having all these pass through a single person ensures that all metadata/data/requests are dealt with consistently.

Reviewer Entry

Accept or send back to applicant for modification:
Accept

Comments:

V. Organizational infrastructure

Compliance Level: 4

R5. The repository has adequate funding and sufficient numbers of qualified staff managed through a clear system of governance to effectively carry out the mission.

The AADC (https://data.aad.gov.au/) is part of the Australian Antarctic Division (http://www.antarctica.gov.au/), a division of the Federal Australian Government that is responsible for managing Australia's Antarctic interests, with a primary focus on the conduct of scientific work. As such it is a publicly funded organisation.

The AADC currently employs the approximate equivalent of 7 full time staff members.

AADC staff are divided into the following areas:

- 1 Manager, who is responsible for the overall running and direction of the AADC.
- 1 metadata officer who is principally responsible for the cataloguing and archival of scientific data arising from the AAp.
- 2 GIS officers who are responsible for maintaining the current mapping program within the AAp, as well as dealing with place name issues.
- 3 IT developers who maintain and develop AADC systems and tools, as well as working on specialist databases for disseminating particular scientific data.

All staff are able to access a budget for ongoing training and professional development, as well as a budget for attending events such as WDS biennial meetings.

We are part of the Australian Antarctic Division's Science Branch - hence we have constant and direct contact with the scientists providing us with scientific data.

Because of its Antarctic ties, the AADC is a part of the SCAR group, the Standing Committee on Antarctic Data Management (http://www.scar.org/data-products/scadm), and the SCAR Group, the Standing Committee on Antarctic Geographic Information (http://www.scar.org/data-products/scagi).

Reviewer Entry

Accept or send back to applicant for modification:
Accept

Comments:

VI. Expert guidance

Compliance Level: 3

R6. The repository adopts mechanism(s) to secure ongoing expert guidance and feedback (either in-house, or external, including scientific guidance, if relevant).

The AADC does not have an external advisory board as such, but in the past it has occasionally engaged with external experts for advice or assistance. In the early 2000s two reviews were conducted of the AADC - one of the entire AADC and one of the GIS section. Furthermore, the AADC gained accreditation as a Nature Approved Repository in 2014 [**ANNEX D**]. This required the AADC to undergo an accreditation much like this one.

However, as we are part of the "Standing Committee on Antarctic Data Management", which is a SCAR committee, we are required to work towards the aims set out in their terms of reference (http://www.scar.org/scadm/scadm-tor). There is a fair degree of overlap between the aims of SCADM and the aims of the WDS. Furthermore, because we are a part of SCADM we are able to leverage off the expertise of other Antarctic data centres for advice, guidance or development should we ever need to.

Also, the AADC has occasionally engaged organisations such as the Australian National Data Service who provided funding and expertise in order to set up a dataset DOI minting service for AAp scientists.

The AADC communicates with its scientific users through various outreach activities - such as giving seminars, running training sessions on how to use metadata/data tools, email announcements and poster displays.

A "support centre" is included in the AADC website to allow users to make requests, or provide feedback (https://data.aad.gov.au/aadc/requests/).

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

DIGITAL OBJECT MANAGEMENT

VII. Data integrity and authenticity

Compliance Level: 4

R7. The repository guarantees the integrity and authenticity of the data.

In order to upload a dataset to the AADC, a user must use the upload form at http://data.aad.gov.au/metadata. The form requires users to answer several questions about their dataset (release status, whether it is the "master" dataset, etc.). The form then creates a formal record of the dataset and links it to an AAp project as well as an AADC metadata record. Some sections of the form are automatically completed depending on the AAp project selected, and whether it has a Data Management Plan (older projects preceded the use of DMPs).

See R11 for details on AADC processes regarding the receipt of data/metadata for archival.

The AADC does have a versioning system for datasets. Users or AADC staff can nominate a dataset for replacement with an updated dataset. The replaced dataset is then date-stamped and transferred to a replacement directory where it can no longer be downloaded. The new dataset is then placed in the publicly accessible directory (and then embargoed if necessary). AADC staff also have the ability to archive a dataset if it is no longer relevant (which is date stamped and transferred to an archive directory where it can no longer be downloaded). Thus different versions of datasets are kept and maintained.

Occasionally data are also uploaded into specialised databases to allow users to more powerfully query the datasets. In these cases, raw copies of the dataset are also kept with the associated metadata record.

Metadata records are also versioned - if a metadata record is later updated, the metadata officer will check the updates before loading, and will also add a note to the metadata record indicating when the record was updated and by who (in the "DIF Revision History" field). Past versions of metadata records have been kept since 2009.

All metadata are stored in the GCMD DIF standard, and all metadata are available via an OAI-PMH service (http://data.aad.gov.au/oai/). See R15 for more information on other metadata standards the AADC uses for distribution.

Because the vast majority of AAp scientific work is project based, the AADC has access to a project database which lists personnel associated with each project. Thus when users submit metadata and data for a project, it is a simple matter to check the name to ensure that the submission is legitimate. Furthermore, as several staff in the AADC have been working there for approximately twenty years, there is a great deal of personal knowledge relating to "who's who". In the rare instances where a name cannot be identified, then the

metadata officer will write to the Chief Investigator of the relevant AAp project to ensure that the submitting individual has authority to submit metadata/data on their behalf.

All admin processes have been well documented on the AADC internal wiki in the event of sudden staffing changes [**ANNEX E**]. These documents are available on request to the AADC. Contact metadata@aad.gov.au. IT restrictions prevent the wiki being placed on a public site.

wiki - Assisting users to create metadata records
wiki - Process metadata records - load records into AADC database - send records to GCMD
wiki - Promote use of DOIs and administer this process
wiki - Loading data into the EDS

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

VIII. Appraisal

Compliance Level: 4

R8. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for data users.

The AADC Data Policy (https://data.aad.gov.au/aadc/about/data_policy.cfm) requires that each AAp project complete a Data Management Plan (DMP - https://data.aad.gov.au/aadc/projects/dmp/AADC_example_data_management_plan.pdf) during their application phase. Projects are not able to progress to the approval stage unless they have a satisfactory DMP (as judged by AADC staff). The DMP outlines what data to expect from each project, when to expect it, who to expect it from, and where the data will be archived (as some datasets are archived in other data repositories).

Once an AAp project has collected data, datasets can be uploaded to the AADC via the following link - https://data.aad.gov.au/metadata

In terms of a "Collection Development Policy", the AADC's mission is to archive data arising from the AAp. Although in rare circumstances, we have occasionally archived Antarctic related data from outside of the AAp. This has happened because a researcher has approached us with a need to archive their Antarctic/subantarctic data, and they have not had access to a suitable repository within their own organisation or research institution.

The AADC does not publish a list of preferred formats, but we do provide guidance that datasets should not be archived in proprietary or uncommon formats. Where possible we recommend that formats such as .csv, .txt, .pdf, netcdf, etc. should be used. All submitted datasets are checked by the metadata officer to confirm file formats. If a non-preferred format is used, AADC staff will do their best to arrange for the submitter to change formats, or provide enough supporting documentation or access to software (in extreme cases) if they are unable to do so.

Metadata records are also submitted at the same link as provided above. The metadata officer will check the metadata record for completeness, and ensure that it adequately describes its associated dataset. Once the metadata officer is satisfied (often after dialogue with the submitting user), the metadata record is formally loaded and assigned a status of "complete". Owing to the diverse range of scientific disciplines covered by the AAp, AADC staff are unable to comprehensively judge whether a metadata record completely describes a dataset (so that said dataset could be re-used in 100 years). However, every care is taken to ensure that the metadata record is as detailed as possible, and that it is therefore quite likely that the metadata record accurately describes its associated dataset.

The AADC uses the DIF metadata standard as its "foundation" standard. Metadata records are also converted into other standards for distribution. See R15 for more information.

A full rundown of metadata and data procedures are available on the AADC internal wiki [**ANNEX E**]. A copy of the wiki is available on request to the AADC. Contact metadata@aad.gov.au. IT restrictions prevent the wiki being placed on a public site.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

IX. Documented storage procedures

Compliance Level: 4

R9. The repository applies documented processes and procedures in managing archival storage of the data.

An AADC internal wiki is used to provide documentation on processes and procedures in the event of unexpected staffing changes. Copies of the documents on the wiki are publicly available on request to the AADC. Contact metadata@aad.gov.au. IT restrictions prevent the wiki being placed on a public site, but copies of the relevant pages from the wiki are annexed to this form.

All data are stored on Australian Antarctic Division servers and the IT department (which provides computing infrastructure for the AADC) also ensures that regular back-ups of all servers are made, including offsite storage. If data need to be recovered, the IT department will arrange that. The AAD is required to adhere to the IT policy/guidelines of our parent government department, the Department of Environment and Energy. As these guidelines have been developed for Australian Federal Government Departments, they are quite explicit in what is expected. As such, the policy includes a set of minimum standards that the AAD is required to abide by, including such things as:

- Server maintenance
- Server security (physical and online)
- Virus protection
- Data storage, back-up and recovery

http://www.naa.gov.au/information-management/managing-information-and-records/disposal/NAP/index.aspx, http://www.naa.gov.au/information-management/managing-information-and-records/storing/storing-digital/index.aspx, https://www.asd.gov.au/infosec/ism/ and https://www.asd.gov.au/infosec/mitigationstrategies.htm.

The AADC also has a preservation plan documented on our internal wiki, which addresses data storage. This is addressed in section R10. Copies of the wiki are publicly available on request to the AADC. Contact metadata@aad.gov.au.

Processes and procedures for backups, storage including offsite, patch updates etc. are provided by the AAD ICT Department and documented internally (by the AAD ICT Department) within the AAD ICT Knowledge Database confluence and to the Service Desk system (ServiceNow—which we are currently migrating our Knowledge Database to). It is the responsibility of ICT to ensure that Servers are adequately maintained. Changes go through the AAD ICT Change Advisory Board (ITIL Term).

Data recovery services are provided by the AAD ICT Department in accordance with their processes outlined at the URLs above.

AAD ICT and the Data Centre meet on a weekly basis to discuss risks outstanding issues and new Service requests. We use an ITIL (international industry Service Management Framework) based Service Desk System which has agreed SLA's configured within in to log and managed the Service Request, Incidents and Problems (ITIL Term). We follow the Departmental Risk Management Framework and process which is based on the ISO Risk Management standard.

Archival copies are monitored by the AAD ICT Department in accordance with their processes outlined at the URLs above.

Storage media is handled and monitored by the AAD ICT Department in accordance with their processes outlined at the URLs above. However, the AADC is currently seriously looking at moving all of our data storage into the cloud with a company like Amazon Web Services.

ANNEX F details AAD ICT Management Processes.

Reviewer Entry

Accept or send back to applicant for modification:
Accept

Comments:

X. Preservation plan

Compliance Level: 4

R10. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

Supplementary information to the Data Policy - https://data.aad.gov.au/aadc/about/data_policy.cfm.

Data shall be stored on AAD servers, or if impractical, stored at approved external repositories (as detailed in the Data Management Plans for each project).

AAD servers are maintained by the AAD ICT department, and it is their responsibility to ensure that the servers are adequately maintained, backed up, etc. The AADC makes requests to the AAD ICT department as needed for more storage, new equipment, new technology, etc. See the attached documents at R9 for full details on the AAD ICT departments processes.

Data held by the AAD servers are maintained in suitable formats - preferably long lived formats such as .csv, .txt, .pdf and so on, as opposed to proprietary formats. Where this is not possible, AADC staff will ensure that files are updated to more recent formats (e.g. .xlsx instead of .xls). As staffing resources allow, periodic checks (every decade) are made over all files in the data holdings to ensure that file formats are as up to date as possible. The AADC typically does not have a list of preferred formats, and does not enforce particular formats. This is owing to the fact that the AAp covers a broad range of scientific disciplines. Instead we work with researchers to ensure they understand how important it is that their data are suitably archived in the most appropriate format. We recommend to users that wherever possible files are archived in long lived formats such as .csv, .txt, .pdf and so on. Most datasets are compressed and stored as zip files. A zip file may contain only a single file, or a large collection of files. Each of these zip files is linked to a metadata record, and also noted in a data cataloguing system which we have developed to manage our collection of datasets. Each dataset is assigned an ID number, which is unique to our system only. Also, many of our datasets are also incorporated into much larger databases - for example our biodiversity database, http://data.aad.gov.au/aadc/biodiversity/. This not only greatly increases the likelihood of long-term storage, but also greatly increases the value of the data by allowing direct comparison with other similar datasets.

In the event that data are only available in unsuitable, proprietary formats, then copies of the associated software will also be made available. Archival in such formats is strongly discouraged.

Except in rare and unusual circumstances, AADC data are not to be deleted from the AAD servers. If data are deemed to be no longer relevant (for example - AADC staff have updated a map series of an Antarctic station) then they should be archived or replaced (removed from public access - using the archive/replace process in the EDS). Copies of archived/replaced data should be maintained, along with their accompanying metadata records. Data deletion is generally only acceptable in the case of in-house developed AADC data

where we are able to make an appropriate call as to whether they are worth keeping and maintaining, or deleting (for example, out-dated maps which may pose a risk to safety). Data archived in the AADC by AAp researchers are generally never deleted.

The preservation plan is stored on an AADC internal wiki, but is also publicly available on request to the AADC. Contact metadata@aad.gov.au. IT restrictions prevent the wiki being placed on a public site.

When a scientist agrees to complete a scientific project in the AAp, they are required to sign a form indicating that they understand that any data they collect remains the property of the Commonwealth of Australia. Thus the individual scientists do not own their own data, the AADC (as the official representative of the Australian Government) does.

The AADC also maintains a data policy (http://data.aad.gov.au/aadc/about/data_policy.cfm) which clearly outlines the obligations of both scientists and the AADC with regard to data management. As part of that policy, the AADC agrees to ensure that, "...Antarctic scientific data are managed for the long-term and made available in an easily accessible form".

During the "upload your data" process used by users submitting data to the AADC, users are required to agree to the terms and conditions of the AADC regarding the archival of their data (http://data.aad.gov.au/aadc/about/condition_of_use.cfm).

The AADC works with the Antarctic Science funding body at the AAD to ensure that scientists comply with their data management obligations. If scientists do not comply, they can have funding withheld, or future projects rejected.

Reviewer Entry

Accept or send back to applicant for modification:
Accept

Comments:
It is expected that AADC publishes its preservation plan (or summary information) by the time of its next certification.

XI. Data quality

Compliance Level: 4

R11. The repository has appropriate expertise to address technical data and metadata quality and ensures that sufficient information is available for end users to make quality-related evaluations.

Once an AAp project has collected data, datasets can be uploaded to the AADC via the following link - http://data.aad.gov.au/metadata

Upon receiving a dataset, AADC staff will then manually perform a series of checks on the files - these checks are documented in the AADC internal wiki (copies available on request - metadata@aad.gov.au), and briefly are: 1) can the data files be opened, 2) are the files in a suitable format, 3) are the data appropriately described by the accompanying metadata record, 4) do the data have appropriate contextual information (dates, locations, units, etc.), 5) have abbreviations or acronyms been fully explained, and 6) if times are included, is the time zone specified.

Where possible, copies of the data files may be made to preserve them in a more stable, long-term format. For example, an excel spreadsheet may be copied as a csv file. If AADC staff are unhappy with a dataset, they will either make changes to the dataset in consultation with the submitting scientist, or request that a new, updated (and improved) dataset be submitted in its place.

Owing to the diverse range of scientific disciplines covered by the AAp, AADC staff are unable to make formal judgments on the veracity or quality of the scientific data.

Once AADC staff are satisfied with the dataset, it is formally approved and loaded into the database.

Metadata records are also submitted at the same link as provided above. The metadata tool used by the AADC has some automatic validation processes - it ensures that all mandatory elements have been created, and that dates are entered in the correct format. Users are unable to submit a metadata record without all the mandatory elements. The metadata officer will then check the metadata record for completeness to ensure that it adequately describes its associated dataset. Once the metadata officer is satisfied (often after dialogue with the submitting user), the metadata record is formally loaded and assigned a status of "complete". Owing to the diverse range of scientific disciplines covered by the AAp, AADC staff are unable to comprehensively judge whether a metadata record completely describes a dataset (so that said dataset could be re-used in 100 years). However, every care is taken to ensure that the metadata record is as detailed as possible, and that it is therefore quite likely that the metadata record accurately describes its associated dataset.

Furthermore, all metadata records undergo another validation process at the GCMD. This process is performed by GCMD validation tools and GCMD staff.

Every AADC metadata record has prominently placed at the top of the record a citation that researchers can use to cite that metadata record and dataset (https://data.aad.gov.au/metadata/records/AAS_4029_Tracer_Particle). Several years ago, the AADC engaged with ANDS to set up a dataset DOI minting service, and the AADC has the capability to create dataset DOIs for the datasets held within its repository. To date almost 800 datasets held at the AADC have an assigned dataset DOI. Thomson Reuters harvests this information for use within its data citation index.

All metadata are stored in the GCMD DIF standard, as stipulated by SCADM, the Standing Committee on Antarctic Data Management (http://www.scar.org/scadm/the-amd-metadata). The DIF standard is compliant with the ISO 19115 metadata standard, and all AADC metadata records are automatically converted to 19115 format (and also into various profiles of the 19115 standard). All metadata records are available via an OAI-PMH service (http://data.aad.gov.au/oai/). See R15 for more information on other metadata standards the AADC uses for distribution.

Should members of the general scientific community (designated community) wish to contact the AADC about a particular dataset, they can do so via our support page - https://data.aad.gov.au/aadc/requests/. Occasionally we receive requests for more information about a dataset (if they feel the metadata record is lacking). In these cases we endeavour to contact the scientist responsible for the metadata record to obtain the appropriate information. These requests are documented in an internal JIRA database for tracking and resolution.

This is also the mechanism by which our designated community can comment on and/or rate AADC data and metadata. As the majority of our data holdings are public, anyone can download the data and then provide us with feedback if they wish. If such comments prove to have merit (after consultation with either the original researchers, or in-house experts), then they will be acted upon.

An internal wiki documents these processes for AADC staff. Copies of the relevant documents from this internal wiki are annexed to this form, and are also available on request to the AADC. Contact metadata@aad.gov.au. IT restrictions prevent the wiki being placed on a public site.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

XII. Workflows

Compliance Level: 4

R12. Archiving takes place according to defined workflows from ingest to dissemination.

To properly articulate data management workflows, the AADC provides three basic tools to users in order to manage their data:

1) A project management tool - for keeping track of the data obligations related to an AAp project, and for the completion of Data Management Plans. https://data.aad.gov.au/aadc/projects/
2) A metadata authoring tool - for creating and editing metadata records that accompany data. https://data.aad.gov.au/metadata
3) A data submission tool - for uploading data into the AADC data archive. https://data.aad.gov.au/metadata

These tools provide clear workflows allowing users to catalogue and archive the data identified in their data management plans - scientists are required to identify the datasets a project will collect and ultimately archive, they are required to write a metadata record for each dataset, and they are required to archive each dataset in an appropriate repository - these tools guide them through the process.

An internal wiki has also been set up in the AADC to provide documentation on workflows, procedures and processes for AADC (to manage data that have been submitted to the AADC for archival) in the event of unexpected staffing changes - (copies of the relevant documents have been uploaded with previous questions, and are also available on request to the AADC. Contact metadata@aad.gov.au).

In order to clearly communicate to users about data management requirements, the AADC maintains a data policy (http://data.aad.gov.au/aadc/about/data_policy.cfm) which clearly spells out the obligations for both scientists and AADC staff with regard to data management.

With regards to the tools above, they have the following levels of security:

1) Project management tool - a log in is required, and only those listed on that particular project are able to access that project and its Data Management Plan.
2) Metadata authoring tool - no log in is required, but metadata records are not automatically loaded, but have to be checked by the metadata officer first, who will confirm that the submission is genuine (generally very straight forward).
3) Data submission tool - a log in is required, but the dataset cannot be accepted until it has been approved by the metadata officer.

Qualitative and quantitative checking of data management plans, metadata records and datasets takes place within the AADC. Submitted data management plans are checked by a panel of AADC staff, and compared

against AAp project submissions to ensure they are as accurate as possible. Invariably this will require a back and forth dialogue with users to get the plan right.

Submitted metadata records and datasets are checked by the metadata officer to ensure that they are of an acceptable level of quality before being accepted into the AADC.

As per the AADC data policy (linked above), the AADC is required to archive all data from the AAp.

Because the AADC is an approved Nature Scientific Repository, we occasionally also handle data archival for Antarctic related scientists who do not have an appropriate repository for archiving their data. A very small percentage of data held in the AADC falls under this category. These datasets and accompanying metadata records are held to the same standards as those arising from the AAp.

The AAp covers a very broad range of scientific disciplines. This does mean that AADC staff are therefore unable to comment on the quality of the scientific work undertaken, as we are not experts on all types of scientific work conducted in the AAp. We take at face value the fact that the science is "good".

Typically data received by the AADC are stored in their original formats. Where possible, files may be saved in different formats to increase their likelihood of long-term preservation - for example, an Excel spreadsheet will be saved in .csv format. Whenever this is done, copies of the original file are also kept.

All AADC workflows and processes are documented in an internal wiki (relevant pages of which have been annexed and are available on request to the AADC: contact metadata@aad.gov.au). Should a workflow or process change, then it is documented in the wiki. The bulk of the data management work is carried out by one staff member (the metadata officer), which obviously simplifies the process of managing change.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

XIII. Data discovery and identification

Compliance Level: 4

R13. The repository enables users to discover the data and refer to them in a persistent way through proper citation.

The AADC metadata catalogue is searchable via a comprehensive tool on the AADC site. The search tool can be found here - https://data.aad.gov.au/metadata. The search tool operates on the AADC collection of DIF metadata (the GCMD standard used by the international Antarctic community).

Furthermore, the AADC metadata catalogue is available for harvesting through the use of WEBDAV. The WEBDAV folders of AADC metadata (in various metadata standards/profiles) are available here - http://webdav.data.aad.gov.au/metadata/.

The AADC metadata catalogue (in each of the various standards/profiles) is harvested by a number of other organisations. AADC metadata is also available through the following tools/organisations (by no means a comprehensive list, as these organisations are often, in turn, harvested by other tools/organisations):

- The Global Change Master Directory
- The Antarctic Master Directory
- The Australian National Data Service
- Data.gov.au
- The Australian Ocean Data Network
- Thomson Reuters
- The Bureau of Meteorology

The AADC is the single largest contributor to the Antarctic Master Directory (a metadata portal hosted by the Global Change Master Directory which compiles metadata records from all National Antarctic Data Centres).

Each harvested metadata record in a format other than DIF includes a "point-of-truth" URL to direct the user back to the "master copy" on the AADC site. All records on the AADC site prominently include a citation for the metadata record/dataset. Many of these citations include a dataset DOI - e.g. - https://data.aad.gov.au/metadata/records/AAS_4326_microalga_toxicity

The AADC has the capability to mint dataset DOIs for its datasets. All AADC metadata records have a supporting citation for researchers to use. Many of these citations include a dataset DOI. Not all AADC records contain a dataset DOI for one or more of the following reasons:

1) In the opinion of the AADC, some of our datasets do not warrant the assignation of a dataset DOI.
2) DOIs are not automatically assigned, thus as the AADC began archiving data long before the advent of

DOIs, there is a significant back catalogue of datasets which must be individually assessed and have their metadata records updated before DOIs can be assigned.

Finally, every metadata record at the AADC is assigned a UUID so that if a record is harvested in a different format duplicate records can be identified.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

XIV. Data reuse

Compliance Level: 4

R14. The repository enables reuse of the data over time, ensuring that appropriate metadata are available to support the understanding and use of the data.

The AADC understands that the role of a data repository is not just to preserve data, but to make it available for re-use. To that end many of the files stored in the AADC are publicly available (some are not, for reasons explained earlier). The vast majority of files are directly available as downloads, and can be accessed without a login. Some files, owing to their large size, are available only on request. The files are then temporarily placed on a cloud file-transfer service (such as Cloudstor).

See earlier questions for details on the process of archiving data and metadata in the AADC.

The AADC also continually updates metadata records - when time allows, an inventory/update of the entire metadata holdings has been taking place. The inventory/update has been going for several years now and is expected to be finished by the end of 2019. As well as updating information in the metadata record, the accompanying datasets have also been examined. Where possible data are converted to "long-lived" formats (e.g. Excel to csv), but if not, then formats are updated to more modern versions (e.g. .xls to .xlsx). If data cannot be updated, they are kept in existing formats. This inventory process will occur roughly every decade.

The AADC also has a preservation plan documented on our internal wiki. Copies of the wiki are publicly available on request to the AADC. Contact metadata@aad.gov.au. See also section R10 for more information on the preservation plan.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

TECHNOLOGY

XV. Technical infrastructure

Compliance Level: 4

R15. The repository functions on well-supported operating systems and other core infrastructural software and is using hardware and software technologies appropriate to the services it provides to its Designated Community.

The AADC strives to meet all of its international and national interoperability requirements. All metadata from the AADC are stored in the NASA DIF standard, but are also made available in ISO19115 format, and three 19115 profiles (ANZLIC - used by the Australian Government; MCP - Marine Community profile used by Australian marine organisations; ANDS - a subset of 19115 standard used by the Australian National Data Service to transform to RIF-CS, the metadata standard they use). The AADC is also currently adding the EML standard for biological data. All metadata are made available to other organisations via an OAI-PMH server (http://data.aad.gov.au/oai/).

The NASA DIF standard is regularly reviewed and updated by NASA. The AADC will always use the latest version of the DIF standard, and has no desire to deviate from this standard. ISO standards go through a regular review process, and the AADC is currently in the process of updating our ISO metadata from the 19115 standard to the 19115-1 standard (as part of Australian Government requirements).

A software inventory is not maintained. However, the new AADC manager has a strong focus on shifting AADC infrastructure into the cloud, possibly with a company such as Amazon Web Services. In the next year (by the end of 2019), it is likely that the AADC will use cloud services for the storage, back-up, recovery and delivery of all its data holdings.

Currently though, the AADC, as a part of the Australian Antarctic Division, takes advantage of its much larger IT infrastructure. The Australian Antarctic Division has a dedicated IT department who are responsible for running daily back-ups of all shared computer systems, and also responsible for storing regular back-ups offsite. In the event that a data restore is required, the IT department is generally able to organise this in a time frame that ranges from one hour to one week (depending on the size of the restore needed, and how far back through the back-ups they need to go).

The AAD is required to adhere to the IT policy/guidelines of our parent government department, the Department of Environment and Energy. As these guidelines have been developed for Australian Federal Government Departments, they are quite explicit in what is expected. As such, the policy includes a set of minimum standards that the AAD is required to abide by, including such things as:

- Server maintenance

- Server security (physical and online)

- Virus protection

- Data storage, back-up and recovery

http://www.naa.gov.au/information-management/managing-information-and-records/disposal/NAP/index.aspx, http://www.naa.gov.au/information-management/managing-information-and-records/storing/storing-digital/index.aspx, https://www.asd.gov.au/infosec/ism/ and https://www.asd.gov.au/infosec/mitigationstrategies.htm.

Should more storage be required, the AADC makes a request for more server space from the IT department. AADC servers are upgraded as deemed necessary by the IT department according to their policy.

AADC servers run the latest version of CentOS operating system with the latest updates and patches applied weekly or on demand hosted on a VMWare vSphere virtualised environment managed by the AAD IT department.

Applications and services are delivered using Docker containers for modularity and ease of deployment behind a mixture of Nginx and Citrix NetScaler reverse proxies using SSL.

The AADC has access to bandwidth speeds of 1 GB per second, which has thus far proven sufficient to meet web traffic in and out.

Processes and procedures for backups, storage including offsite, patch updates etc. are documented internally within our Knowledge Database confluence and to the Service Desk system (ServiceNow—which we are currently migrating our Knowledge Database to).

The Department of Environment recently released a revised ICT Security policy in 2018.

It is the responsibility of ICT to ensure that Servers are adequately maintained. Changes go through the AAD ICT Change Advisory Board (ITIL Term).

It should also be noted that the AAD as an organisation has existed for approximately 60 years, and enjoys strong bipartisan support from the federal government (we are part of the federal government). While IT policy documents may refer to "long-term" as 2–4 years, this is more a reflection on the nature of government documents than a belief that "long-term" is only 2–4 years. Australia has significant strategic and scientific interests in the Antarctic, and as the AAD is Australia's lead Antarctic organisation, it is reasonable to assume that the AAD will be around for many, many years to come.

If more detail is required, questions should be directed to the Department of Environment and Energy (http://www.environment.gov.au/). Note that owing to federal government restrictions, Freedom of Information requests may need to be made to access certain documents.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

XVI. Security

Compliance Level: 4

R16. The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.

The AAD is required to adhere to the IT policy/guidelines of our parent government department, the Department of Environment and Energy. As these guidelines have been developed for Australian Federal Government Departments, they are quite explicit in what is expected. See R15 for more information.

Backup procedures and processes are documented in R15.

The data servers that the AADC uses are stored within secure rooms of secure buildings. Access to the buildings and rooms are controlled by electronic key passes. Only Australian Antarctic Division staff members have access to the buildings, and only authorised IT personnel have access to the rooms containing the servers. The server room at the Australian Antarctic Division is in fact secured at a higher level than normal because it is a Federal Government facility.

The rooms containing the servers are protected by an inergen based fire extinguishing system. Offsite back-ups are similarly protected from fire. Earthquake activity in Tasmania is virtually non-existent, so the rooms are not protected against seismic activity. The server room is also temperature controlled (and monitored), and is sufficiently water protected (in-floor water sensors, and outflow pipes). A large UPS has been installed in the room in the event of a power failure.

The servers are also protected by comprehensive anti-virus software.

Access to the network is controlled by the IT department, who set permissions for users in the administration sections of their systems. Access is only provided to AADC personnel and IT department personnel. However, archived data are all stored in a web accessible folder, so that members of the public can download publicly available data.

The Australian Antarctic Division's firewall is maintained and configured by the IT department.

AAD ICT and the Data Centre meet on a weekly basis to discuss risks outstanding issues and new Service requests. We use an ITIL (international industry Service Management Framework) based Service Desk System which has agreed SLA's configured within in to log and managed the Service Request, Incidents and Problems (ITIL Term). We follow the Departmental Risk Management Framework and process which is based on the ISO Risk Management standard.

See R15 for further details on the AADCs relationship with the AAD regarding IT.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

APPLICANT FEEDBACK

Comments/feedback

Some feedback about the questionnaire—I felt that I was often repeating answers in many of the questions, as there was a fair degree of overlap.

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

Trusted Digital Repository Definition

A trusted digital repository is one whose mission is to provide reliable, long-term access to managed digital resources for a designated community, now and in the future.

What Generally Characterises a Sustainable Repository

- accepts responsibility for the long-term maintenance of digital resources on behalf of its depositors and for the benefit of current and future users;
- has an organisational system that supports not only long-term viability of the repository, but also the digital information for which it has responsibility;
- demonstrates fiscal responsibility and sustainability;
- designs its system(s) in accordance with commonly accepted conventions and standards to ensure the ongoing management, access, and security of materials deposited within it;
- establishes methodologies for system evaluation that meet community expectations of trustworthiness;
- can be depended upon to carry out its long-term responsibilities to depositors and users openly and explicitly; and
- has policies, practices, and performance that can be audited and measured.

The Alternate Repository Must be Able to Demonstrate the Following as a Minimum:

On-Line Storage

1. Designated on-line storage medium with a regular back-up, maintenance and disaster recovery plan.
2. Secure physical access to storage medium.
3. Controlled and authenticated access to content on storage medium.

Data Submission Guidelines

1. Guidance for depositors on formats and requirements for accompanying documentation.
2. Demonstrated commitment to curation practises that preserve data for future access and use (e.g. archiving using open formats or ingestion to continuously upgraded databases).
3. Evidence of integrity checks performed on submitted data.

On-line Data Access System

1. Publicly accessible system for providing access to submitted data with appropriate security and an adequate resource discovery interface.
2. Ability to persistently and uniquely identify data sets (e.g. with digital object identifiers; DOIs).

Policies

1. A published data policy that addresses issues such as copyright, data licensing, data citation, and metadata requirements.
2. Appropriate and clear open-access data licensing (preferably a CC-BY license or CC-0 waiver).

Medium To Long-Term Institutional Backing

1. Evidence that the repository will be backed/funded for the next 10 years, and/or an agreed handover plan with the AADC in case of funding changes.

11 - Other

1. Checking citations
2. Metadata template
3. Downloading data from BoM
4. Sending large datasets to researchers
5. State of the Environment data
6. Deleting metadata records
7. Distribute AWS data
8. World Data System/Core Trust Seal Duties

- Checking citations
  Occasionally spot checks should be made to determine if data citations are occurring correctly. Either by following up with scientists to see if they are self-citing their own data, or if we know of data that are being used elsewhere (for example that have been recently downloaded or requested), checking to see if that data has been correctly cited. XXXX has performed some spot checks like this in the past on datasets.
- Metadata template

  Latest copy of the basic metadata template to distribute to offline users.

  Template for Basic AADC Metadata Records.docx
- Downloading data from BoM
  Under a new MoU signed in late 2014, BoM are now providing Antarctic meteorological data to the AADC free of charge. The AADC can then redistribute these data to anyone. On the 2nd of every month, the data are placed on an FTP server by BoM, and an alert is sent to XXXX. The files MUST be downloaded during the course of the month, as the new monthly data will overwrite the old data. The data should be copied to XXXX the filenames will need to be changed so that files are not overwritten. At the beginning of the filename, enter the year and previous month - for example, if the file DS016_AADC_AWS.zip is downloaded on December 2nd, change the filename to 2014-11-DS016_AADC_AWS.zip (i.e. NOVEMBER, as the data are for the previous month).
  The monthly email comes from the address: XXXX - Oracle Web Server. They FTP address for downloading the data is: XXXX. The email subject is: Automated Bureau of Met (TCZ system) Job Extraction on ftp server
  Upper Air and One-Minute data are stored in month-by-month files in their respective folders.
- Sending large datasets to researchers

  Occasionally we receive requests for access to very large datasets. Currently (2019-09-17), datasets under 2 TB in size can be placed on sites such as Cloudstor (which can be used to send data to anyone in the world), but for file sizes larger than this AADC developers will need to use Amazon Web Services to deliver the data. The developers are currently working on a system to allow users to download very large datasets with an installed tool.
- State of the Environment data
  The metadata officer is also responsible for uploading data into the SoE system. It most cases

this is a manual entry task. In 2013, the SoE list of indicators was culled down to a bare minimum of indicators that are still being supported.

- 1 - Monthly mean air temperatures at Australian Antarctic Stations - arrives in an automatic email from XXXX at the beginning of each month. Data are cut and paste as a block of text from the email (current month only) into http://data.aad.gov.au/aadc/admin/soe/met_data_entry.cfm

1.

- 2 - Highest monthly air temperatures at Australian Antarctic Stations - arrives in an automatic email from XXXX at the beginning of each month. Data are cut and paste as a block of text from the email (current month only) into http://data.aad.gov.au/aadc/admin/soe/met_data_entry.cfm
- 3 - Lowest monthly air temperatures at Australian Antarctic Stations - arrives in an automatic email from XXXX at the beginning of each month. Data are cut and paste as a block of text from the email (current month only) into http://data.aad.gov.au/aadc/admin/soe/met_data_entry.cfm
- 4 - Monthly mean lower stratospheric temperatures above Australian Antarctic Stations - arrives in an automatic email from XXXX at the beginning of each month. Data are cut and paste as a block of text from the email (current month only) into http://data.aad.gov.au/aadc/admin/soe/met_data_entry.cfm
- 5 - Monthly mean mid-tropospheric temperatures above Australian Antarctic Stations - arrives in an automatic email from XXXX at the beginning of each month. Data are cut and paste as a block of text from the email (current month only) into http://data.aad.gov.au/aadc/admin/soe/met_data_entry.cfm
- 8 - Monthly mean atmospheric pressure at Australian Antarctic Stations - arrives in an automatic email from XXXX at the beginning of each month. Data are cut and paste as a block of text from the email (current month only) into http://data.aad.gov.au/aadc/admin/soe/met_data_entry.cfm
- *The email from XXXX contains two months of data, if the entire email is cut and paste into the loader, rather than just the most recent month, then the overlap will cause those values to be added together – e.g. temperatures for Heard Island in December could be listed as 10 degrees, rather than 5 degrees. If this happens, the extra entries will need to be manually deleted using the search and then edit functions.*
- 9 - Daily records of total column ozone at Macquarie Island - data are obtained from WOUDC and then manually entered via the "data entry" form. Go to:

  http://www.woudc.org/data/MetaQuery/metaquery_e.cfm
  Category: Total Ozone
  Platform: Station 29
  Type: Dobson
  (seems to work better in IE than in Chrome)
- 10 - Daily broad-band ultra-violet radiation observations using biologically effective UVR detectors - data are obtained from XXXX on a regular basis and manually entered. Data are also attached to the metadata record.
- 11 - Atmospheric concentrations of greenhouse gas species - data should be obtained from XXXX. Developer assistance may be required to load the data.
- 31 - Annual population estimates of Southern Elephant Seals at Macquarie Island - data are obtained from XXXX. Census occurs every October. Manually enter data.
- 48 - Station and ship person days - data are obtained from Polar Medicine and manually entered.
- 49 - Medical consultations per person year - data are obtained from Polar Medicine and manually entered.
- 51 - Biological Oxygen Demand (BOD) of wastewater discharged from Australian Antarctic Stations - data are entered by station doctors. Station doctors will need to be trained to use the

SoE system every year. Doctors have generic log ins. Search the AADC User database for “exmo” (in the email address) to find the four station doctor usernames.

- 52 - Suspended solids (SS) content of wastewater discharged from Australian Antarctic Stations - data are entered by station doctors. Station doctors will need to be trained to use the SoE system every year. Doctors have generic log ins. Search the AADC User database for “exmo” (in the email address) to find the four station doctor usernames.
- 54 - Amount of waste incinerated at Australian Antarctic Stations - I believe that XXXX organises this, and plumbers on station manually enter the data.
- 57 - Monthly incinerator fuel usage of Australian Antarctic Stations - data are provided by "operations", but not sure who by at the moment. Manual data entry. Station plumbers sometimes keep this up to date.
- 61 - Total potable water consumption at Australian Antarctic Stations - I believe that XXXX organises this, and plumbers on station manually enter the data.
- 62 - Water levels of Deep Lake, Vestfold Hills - the Davis Station Leader appoints someone to take these readings once a month. Data are sent to the metadata officer for manual entry. Photos of the lake and surrounds, as well as photos of the pole are taken and saved at XXXX.
- 83 - Quality of Potable Water at Australian Antarctic and Subantarctic Stations - data are entered by station doctors. Station doctors will need to be trained to use the SoE system every year. Doctors have generic log ins. Search the AADC User database for “exmo” (in the email address) to find the four station doctor usernames.

- Deleting metadata records
  When deleting a metadata record, the following steps must be taken:
- Use the delete tool under the "Admin AADC Only" button.
- Go to XXXX and delete all copies of the record in each of the subfolders - EXCEPT for the copy in the "Deleted" folder.
- Distribute AWS Data
- Occasionally I get requests for copies of our AWS data from this tool - http://data.aad.gov.au/aadc/aws/ (Extract and Download Data link) - basically because the tool only lets you get data a month at a time, and sometimes users want data for many, many months. I have extracts of all the data from the system in this folder - XXXX - Data extracts should you ever need to hand it out.
- World Data System/Core Trust Seal Duties
- As a WDS regular member we are required to carry out several reviews of other data centres every year to evaluate them for Core Trust Seal accreditation. Past reviews are held here - XXXX. Details of our reaccreditation process that we went through in 2017 and 2018 are held here - XXXX.

12 - What happens to the data if the AADC ceases to exist

The AADC is funded by the Australian Government as part of the Australian Antarctic Division, which is a division of the Department of Environment and Energy. As such it has considerable funding stability. The activities of the AADC are considered highly important by both the AAD and the Department of Environment and Energy (and are included in the Strategic Plan), and it is extremely unlikely that funding will be removed.

In the unlikely event that something were to happen though, our metadata and data holdings would be secure through the following means:

1) The metadata catalogue would be preserved at the GCMD (which maintains the master copy of our metadata records). Copies of all our metadata records would also be available from ANDS, and subsets would exist at the AODN and various other organisations.
2) Data would be transferred to data.gov.au - which is an initiative of the Australian Government to provide data management services for its various departments - those that do not have a dedicated data repository (many of them do).
3) Data would also be transferred to the Institute for Marine and Antarctic Studies (IMAS). IMAS is part of the University of Tasmania, and has its own (new) Antarctic data centre for managing data arising from University Antarctic programs.
4) Ocean related data would be transferred to the AODN Data Portal, and to the Marine National Facility.
5) Some of our data holdings are also already available through other institutions like GBIF and OBIS.

Contact would need to be made with whomever is managing each of these repositories at the time. Data would need to be backed up and transferred quickly - as an interim measure, the RDS facility at the University of Tasmania has access to very large storage which could hold our data until final resting points are found.

From: Scientific Data
Sent: Friday, 19 December 2014 12:53 AM
To: AADC
Cc: Scientific Data
Subject: RE: Australian Antarctic Data Centre respository evaluation [SEC=UNCLASSIFIED]

Dear AADC,

Thank you for completing the repository evaluation questionnaire. We have now had the opportunity to evaluate the Australian Antarctic Data Centre, and I am pleased to let you know we will be including this in the list of repositories that we recommend to our authors.

Regarding facilitation of confidential peer review, I suggest that a SciData specific login that we could share with our reviewers would be adequate to allow our reviewers confidential access to the data. Another possibility is that we may ask potential authors to additionally deposit data with Dryad or figshare just for duration of the peer review process. Going forward we will look at this on a case by case basis, and work with you to find the best mutually beneficial solution.

We will shortly be adding the Australian Antarctic Data Centre to our repository webpage. Please do let me know how you might be planning to spread the news to your existing user base, as we could be able to assist you with that in some way. Please also let me know if you would like Scientific Data to assist you in publicising inclusion of the Australian Antarctic Data Centre as a Scientific Data approved repository to the wider scientific community. We can use our social media platforms to help with this, and we can also co-ordinate our outreach with yours if you think it would be worthwhile to do so for a bigger 'splash'.

Due to the Christmas break, I suggest we postpone publicizing this news until the week beginning January 5th, as I think it will have more impact at that time. I will however endeavour to get the Australian Antarctic Data Centre onto our online repository page this week.

Kind regards,
Scientific Data

-----Original Message-----
From: AADC
Sent: 15 December 2014 05:24
To: Scientific Data
Subject: RE: Australian Antarctic Data Centre respository evaluation [SEC=UNCLASSIFIED]

Hi Scientific Data

Please find attached the filled questionnaire - happy to provide additional detail if needed.

Many thanks

AADC

> -----Original Message-----
> From: Scientific Data
> Sent: Tuesday, 9 December 2014 10:20 PM
> To: AADC
> Cc: Scientific Data
> Subject: Australian Antarctic Data Centre respository evaluation
> [SEC=UNCLASSIFIED]
>
> Dear AADC,
>
> Many thanks for your email. We have a formal questionnaire (attached
> here), the answers to which help us with the repository evaluation
> process. I have answered some questions based on the information you
> have already provided, but please feel free to edit that text if
> necessary.
>
> In order to be considered at our next repository evaluation meeting I
> will require the completed form to be returned to me by Wednesday 17th
> December. However we do meet fairly regularly, so in case you are
> unable to meet this deadline, I will put the Australian Antarctic Data
> Centre forward for consideration at a subsequent meeting.
>
> If you have any questions about the journal or our repository
> evaluation process, please do not hesitate to email me.
>
> Kind regards,
> Scientific Data >

>
> --
> Data Curation Editor, Scientific Data
> Nature Publishing Group
>
>

> The Macmillan Campus, Trematon Walk, N1 9FN, London, UK
> http://www.nature.com/scientificdata/
>
>
>
>
> -----Original Message-----
> From: AADC
> Sent: 04 December 2014 04:56
> To: Scientific Data
> Subject: RE: your recent work in Nature: invitation to submit a

> follow- up manuscript to Scientific Data [SEC=UNCLASSIFIED]
>
> Hi Scientific Data
>
> Following NIWAs enquiry, I'd be happy to put the Australian
> Antarctic Data Centre up for consideration as a recommended repository
> for Scientific Data. Some brief points against your criteria:
>
> - The AADC was established in 1996 and was amongst the first National
> Antarctic Data Centres, with the mandate of providing long-term
> management of Australia's Antarctic data. We, and our data policy, are
> an integral part of the Australian Antarctic program. All scientists
> conducting research under the Australian Antarctic programme are
> required to make their data publically available (usually, but not
> necessarily, through us) with a metadata record (this must be with us).
> Our metadata records are published through the GCMD and harvested by a
> number of other organisations.
>
> - Data custodians have an embargo period to allow them to publish
> their work, which is generally two years but may be shorter or longer
> in some cases. After that period, all data are made publically
> available except for a small number of sensitive data sets (e.g.
> commercial-in- confidence fishing data). Non-public data have a public
> metadata record and so are still publically discoverable.
>
> - Data submitted to us undergoes quality checking by our staff.
> Depending on the nature of the data, it is typically either integrated
> into a larger database or made available as a standalone data file.
>
> - We issue DOIs - at the moment these are issued routinely on new data
> sets, and as-needed on old (existing) ones.
>
> - We are a WDS Regular Member and are an active participant in various
> data fora (including e.g. SCADM, the SCAR Standing Committee on
> Antarctic Data Management).
>
> Our data policy can be found here:
> http://www1.data.antarctica.gov.au/aadc/about/data_policy.cfm
>
> If you require anything else (or a more formal application) please let
> me know.
>
> Regards
>
> AADC
>
>
> ---
> Manager (acting), Australian Antarctic Data Centre Australian
> Antarctic Division Channel Highway, Kingston 7050 AUSTRALIA

>
>
>
>
>
>From: Scientific Data
> Date: Thursday, 4 December 2014 12:28 am
> To: NIWA, Scientific Data
> Cc: NIWA
> Subject: RE: your recent work in Nature: invitation to submit a
> follow- up manuscript to Scientific Data
>

> Dear NIWA,
>
    > <snip>
>
> If you are in contact with the maintainers of the Australian Antarctic
> Data Centre, please do encourage them to get in contact with us so
> that we can consider whether it should be formally listed among our
> recommended repositories, for the benefit of our future authors.
>
> And, please do let me know if you have any further questions while
> preparing your Data Descriptor manuscript.
>
> Best regards,
>
>Scientific Data
>
  > --
> Managing Editor, Scientific Data
> Nature Publishing Group
>

> Web: http://www.nature.com/scientificdata/
> Blog: http://blogs.nature.com/scientificdata/
> Twitter: http://twitter.com/ScientificData
> Video: http://www.youtube.com/watch?v=hrHM3bUym3g
>

1 - Assisting users to create metadata records

Users can now be directed to the new metadata tool here
- http://data.aad.gov.au/metadata/ (Describe) - this is the preferred method of creating metadata records. If users log-in first, then the tool will help keep track of their submissions. Logging-in is not essential to create or edit metadata records, but it is essential to upload a dataset.

Alternatively, for users working offline (e.g. on the ship), or for those users who find the new metadata tool too complex, then you can use the metadata word template
- https://data.aad.gov.au/eds/3623/download. The word template will require much more effort from the metadata officer to convert into a DIF record.

Once the user has completed the metadata record with the new tool, the record will then need to be processed.

Note that the AADC Metadata Tool will automatically populate a large number of fields in order to streamline the process and make it easier for users and AADC staff. When AADC staff are logged into the tool, then they are given an "Admin" section at the end of the wizard. All automatically populated fields bar one appear on this tab (the geographic region of "Polar" appears on the spatial tab).

2 - Process metadata records - load records into AADC database, send records to GCMD

+2

Processing Metadata

Flowchart

AADC Metadata Tool (User) > AADC Metadata Tool (Admin) > Load XML file into AADC database > Email to GCMD

Metadata Word Template > AADC Metadata Tool (User) > AADC Metadata Tool (Admin) > Load XML file into AADC database > Email to GCMD

See also the AADC Metadata Writing Guide.

1. Metadata record received from general user - records from users will be incomplete.
    a. When a user completes a metadata record, the XML version is emailed to XXXX.
    b. Copy the XML file to the Upload area - XXXX
    c. Go to the metadata admin page - https://data.aad.gov.au/metadata/admin and go to "Import and Convert". Import the record.
    d. Go to the metadata pages - https://data.aad.gov.au/metadata - and find the record (it will be the most recent entry in the "Latest Updates" box).
    e. Click on "Edit record" to complete the record.
2. Metadata record being created by AADC user
    a. AADC users will be able to create a complete record from scratch, as they have access to the Admin tab (it is still worth checking the record though).
3. When completing a metadata record, there are a number of fields that are mandatory.

a. Mandatory fields enforced by the tool for general users
    i. Entry ID
    ii. Entry Title
    iii. Description
    iv. Personnel
    v. Science Keywords
b. Mandatory fields auto-populated by the tool
    i. Data Centre
    ii. Originating Centre
    iii. IDN Node
    iv. Related URLs
    v. Dataset Citation - Creator, Title, Series, Publisher, Online Resource
    vi. Geographic Location - Polar
    vii. DIF creation date, DIF revision date
    viii. Use Constraints
    ix. Extended metadata - UUID, extraction date, keyword version
c. Mandatory fields that admins must ensure are present
    i. Instrument (if you get stuck some nice generic ones are "Visual Observations", "Cameras", "Computer", "Surveying Tools", "GPS", "Microscopes")
    ii. Platform (if you get stuck some nice generic ones are "Field Survey", "Laboratory", "Fixed Observation Stations", "Ships", "Aircraft", "Satellites")
    iii. Dataset Citation - Version (version of the dataset - for new records and datasets this will be "1").
    iv. ISO Topic Category
    v. Temporal Coverage
    vi. Spatial Coverage
d. If you are going to create a Dataset DOI for the dataset, the following field must also be completed
    i. Dataset Citation - Dataset Release Date (YYYY-MM-DD)
e. If a user has provided a non-standard keyword in the science keywords, instrument or platform fields, try and find a suitable match (often there is one), and move the user keyword to the "Additional Keywords" section.
f. If there is a dataset to be linked to the record (one that has been uploaded via the EDS), and a link to "Related URL" of the "GET DATA" type. Insert the URL (e.g. https://data.aad.gov.au/eds/4844/download) and add a description like, "Download the dataset". Ensure the "Distribution Information" on the admin tab has been completed - set Media to "HTTP", Fees to "Free" and complete the other fields as appropriate. Ensure that in Size there is a space between the number and the units - e.g. 1 MB, not 1MB.
g. The references field - this will most likely need to be manually entered by AADC admins. To make life easier for users we give them the option of pasting their publication references in as a block of text. HOWEVER, these do NOT accurately translate into the AADC metadata tool when using the edit function (item 1e

above) - AADC admins will need to manually re-enter the publication references from the XML into the separate subfields so that they are stored correctly.

h. Ensure that "Access Constraints" has an appropriate statement in it - e.g. "These data are publicly available for download from the provided URL." "These data are not yet publicly available."

i. Check the altitudes, depths and data resolution values on the spatial coverages tab (compare them to the original XML). Until I finish updating these manually, they may need fixing in the tool.

j. Make a note in DIF Revision History (admin tab) about what changes were made. e.g. "2019-01-30 - record update by John Smith to provide more detail in the description field."

k. It is best to replace non-standard characters such as e acute and the degrees symbol (e.g. with "e" and "degrees" in this case). Never use "&" or "<" or ">" in the metadata record, as they cause problems with the XML outputs.

4. Ideally, AADC users will complete as much of a record as possible, ensuring it is as detailed as possible. If you are unsure, look at other recent metadata records for examples.
5. Submit the record to yourself.
6. Copy the XML file to the Upload area - XXXX
7. Go to the metadata admin page - https://data.aad.gov.au/metadata/admin and go to "Import and Convert". Import the record.
8. Go to the metadata pages - https://data.aad.gov.au/metadata - and find the record (it will be the most recent entry in the "Latest Updates" box).
9. Click on "Admin "AADC Only" - select "Edit record".
    a. Mark the record as "Complete" (if appropriate)
    b. Check the data status (selecting multiple options possible)
        i. "Metadata record points to data" - are the data linked to the metadata record? Data can be stored anywhere.
        ii. "Data held by AADC" - are the data stored in the AADC?
        iii. "Data is downloadable..." - are the data linked to the metadata via a link from the EDS?
        iv. "Linked to reports" - does the data have a downloadable report attached (e.g. publication)?
    c. Link the record to one or more AAS projects - click save.
10. If a Dataset DOI is required, click on "Request DOI". Follow the prompts. After the DOI has been requested, go to the DOI admin page - https://data.aad.gov.au/aadc/doi/admin/.
    a. Click on "Pending DOI Requests"
    b. "Submit to ANDS". If all the DOI required metadata fields are present, a DOI will be minted (created).
    c. Insert the DOI into the metadata record (either directly into the XML, or via the AADC tool). The DOI goes into Dataset Citation - Dataset DOI.
    d. Use the prefix "doi:" before pasting the DOI number.
    e. Copy the record to the upload area, import and convert it.
    f. If the DOI is for a dataset that has not been made public, it will need to be deactivated until the data are public.
        i. Go to DOI admin - https://data.aad.gov.au/aadc/doi/admin/

   ii. Search for the Entry ID of the associated record - e.g. "ASAC_875"
   iii. Click on "Deactivate" and confirm.
   iv. When the DOI needs to be reactivated, click on "Activate".
11. Place an XML copy of the record into the correct "Upload Completed" folder - e.g. - XXXX - this acts as version control.
12. Email the submitting user to let them know you've loaded their record.
13. Importing a metadata record will automatically schedule it for conversion into other formats by the XSLTs.
14. All metadata records are stored in XXXX.
    a. The particular folder depends on the format - all our records are natively stored in the "dif" folder, and are converted into other formats and placed in those folders (e.g. "iso").

3 - Ensure metadata records are converted into ISO "flavours", and are accessible in OAI-PMH folders (automatic process)

AADC metadata records are made available to a number of other organisations in various profiles of the ISO 19115 format. We make our metadata available for harvesting in the following formats:

1. DIF (standard GCMD format)
2. ISO 19115 (standard ISO format)
3. ISO-ANDS (a cut down version of an ISO 19115 record which is used as an intermediate step to be transformed into RIFCS format for ANDS)
4. ISO-ANZLIC (ANZLIC profile of the ISO 19115 standard)
5. ISO-MCP (Marine Community Profile of the ISO 19115 standard)
6. ISO-AODN - only three records that are required to be in MCP2.0 format. Converting to MCP2.0 requires manual intervention as MCP2.0 requires the inclusion of AODN keywords (which we don't use, and have to be entered manually).
7. EML - Biological datasets that have been properly prepared for use in GBIF/OBIS and have been placed on the aadc IPT (data.gov.au/ipt) are converted to EML format. Actually I think all records with an ISO keyword of "BIOTA" are converted to EML, but only the prepared datasets are loaded onto the IPT.
8. ISO 19115-1 - this is the new ISO format.

These metadata records are all automatically placed in OAI-PMH accessible folders at XXXX and made available at http://webdav.data.aad.gov.au/metadata/ to whoever needs them.

The conversion process occurs automatically every two hours.

6 - Promote use of DOIs and administer this process

The metadata officer also needs to actively promote the use of DOIs. There are some general instructions for AADC staff here: Citation Cheat Sheet for AADC Staff

Specifically for the metadata officer though, if a processed dataset can be made public, then the researcher should be asked if they would like a DOI. If researchers have submitted a dataset that cannot yet be made public, but the expectation is that it soon will be, or if they need a DOI for a publication (and the data cannot be made public until the publication has been published), then a DOI can still be assigned, but it should be **deactivated** until the data can be made public - at which point it can be **reactivated**.

Process for creating a DOI

1) Update the metadata record to ensure that it is of a high quality. "Dataset Citation > Dataset Release Date" MUST be set in order to get a DOI.

2) Process and load the metadata record.

3) Find the metadata record on the AADC website - eg use this tool
- https://data.aad.gov.au/metadata/records

4) Click "Request DOI" and follow the prompts.

5) Go to DOI Admin - https://data.aad.gov.au/aadc/doi/admin/ - and navigate to the DOI requests page - find the metadata record and click "Submit to ANDS".

6) If successful, the DOI will be displayed. If not, the page will tell you what is missing from the metadata record.

7) Update the metadata record again, and enter the DOI into "Dataset Citation > Dataset DOI" - use a prefix of "doi:" and then the number.

8) Process and load the metadata record.

9) If the data are still embargoed, find the metadata record on the AADC website, and click "Deactivate DOI". Once the data are released, the DOI can be "activated".

8 - Loading data into the EDS and performing data validation checks

Loading data into the EDS

The EDS tool is available here - https://data.aad.gov.au/metadata - "Upload".

Users are strongly encouraged to use this tool to upload their data. There is a 4 GB limit. If datasets are larger than that, then alternative means of data transfer (such as Cloudstor) must be used.

The form is fairly straightforward to use.

AADC Admins only:

1) Is a log on required - usually the answer is no.

2) Select an AADC admin - select the appropriate person.

3) Which group - this determines where the file will be stored (e.g. Science datasets). The extra picklist is for GIS users.

4) Spatial database - GIS users only, everyone else select no.

5) Checked and approved - tick this once you have confirmed the files can be opened and look okay.

6) Custom file name - only use if you want to give the file an alternative name (other than the metadata ID). Do not include ".zip" in the name.

7) Submitted by - AADC users can select other users if they are uploading data on someone else's behalf.

All users:

8) Current user - details of logged in user

9) Project - select an AAS project if appropriate

10) Dataset details - if an AAS project with a Data Management Plan has been selected, you can select an item from the DMP as the dataset. This will auto-fill some fields. Otherwise complete them manually.

11) Submission type - if "replacing" you will need to select which dataset is being replaced - you will be prompted to do so.

12) Raw or processed - pick one.

13) Release status - public - public; embargoed - locked away for the time being; confidential - locked away probably forever; AAD only - only available to AAD staff; Review - see below.

14) Master dataset - pick one

15) Contact me - only for users having problems

16) Drag and drop multiple files

17) Metadata details - enter the Entry_ID of the related metadata record, or complete one of the other fields

18) Agree to the terms and then submit.

Furthermore, AADC Admins can also set the release status of a file to "Review" - this will make a file available to download by anyone with the correct log in and password (XXXX/XXXX). This is intended for use by journal reviewers who will need to access a dataset. They will need to be provided with the direct link to the download file -
e.g. https://data.aad.gov.au/eds/4653/download - as long as they are not already logged in, they will be prompted to log in (use the account above), and the dataset should download. For all other users (except AADC admins), the file will remain "embargoed".

For AADC admins, once the file has been approved, a download link will be generated, and will appear in this form. Admins can search for datasets here
- https://data.aad.gov.au/metadata/admin

Performing data validation checks

When a dataset is received it must be checked to ensure that it is suitable for archival. Use the following checklist.

1) Can the data files be opened? If there are only a handful of files, open them all, if there are a great many files, open a random selection.

2) Are the files in a suitable format? Proprietary formats should be rejected wherever possible in favour of non-proprietary formats. If this is not possible then appropriate software/support should be provided with the data so that it can be re-used. Formats such a .csv, .txt, .pdf, etc. should be used where possible. If a clean conversion can be made (e.g. a simple .xslx file to .csv), then the original file can be discarded. If the conversion may result in a loss of information (e.g. a more complicated .xslx file), then retain the original as well as the converted file in the archive.

3) Are the data appropriately described by the accompanying metadata record? Does the metadata record contain sufficient information to allow a knowledgeable user to interpret it and re-use it?

4) Does the data have appropriate contextual information? Specifically dates, locations and units.

5) Have abbreviations or acronyms in the data been explained in full?

6) If times are included in the dataset, is the timezone specified? Local time, UTC, etc.

If the answer to any of these is "no", then the data must go back to the submitting scientist for clarification.

AAD ICT

Current and Proposed Backup retention policy

Introduction

The current number of backup copies kept by ICT both on disk and tape are becoming difficult to manage. The below outlines the current retention policy in use and a proposed change the will reduce the pressure on both infrastructure and staffing in managing our backup solution.

It's important to note that ICT's backup strategy is designed for the recovery of data lost either from a system failure / disaster or the accidental loss of data. The backup system is not used to archive data as no data is removed from the production system during back up.

Summary of Changes

Currently Tape copies occur every quarter and are kept forever. This poses a number of issues.

- Recovery of data older than the current generation of tape requires access to legacy technology. The cost of storage and cost of recovery of this data is significant to the organisation.
- Reducing the frequency of tape copy significantly improves the organisations ability to manage and store the media and reduce the overall operational expense of the backup service.
- By reclassifying a number of backups to only be retained on disk we can further reduce costs associated with this data by removing their reliance on tape. Archived Scientific data poses the largest amount of data stored within the AAD system.
- As part of the archiving process of this data alternative paths for large data storage are being established with AARnets cloudstor storage offering. It should be encouraged that any data, at the end of its functional lifespan and suitable for archiving offsite is migrated on to a system such as this to further reduce costs associated with data storage by the organisation.

The restore points for data stored on disk, as they are currently implemented, are limited.

- There is a gap in recoverable business data for the medium term, we are rely on quarterly tape copies to restore medium term data (1-3 years). Tape recovery is a much more resource intensive process than disk recovery.
- By introducing a more consistent and extensive medium term copy policy, while reducing use of frequent short term copies we can provide better coverage to the business without requiring more storage resources. This will also reduce the number of tapes we require per year leading to further savings.

Long Term changes

Over the long term (2-4 years) we will see a reduction in data stored on tape and a significant amount of duplicate data currently directed at tape storage will be eliminated. This will make the viability of using cloud services, as an alternative to tape, a possible solution for general data. This level of storage would also allow us to significantly reduce the risks associated with long term storage of data and tapes at M2.

Summary of proposed policy

- **Up to 14 days,** hourly recoveries (within business hours) will be available for most data on Disk at Kingston
- **Up to 30 days,** recoveries will generally be available from Daily copies on Disk at both Kingston and M2.
- **Between 30 days and 2 years,** recoveries will available from weekly copies from Disk
- **Between 1 year and 6 years,** recoveries will be available from a Yearly copy on Tape
- **Beyond 6 years,** Data will not be available for recovery
    - Existing data will be immediately affected by this change.
    - Data older than 6 years, that is not currently on disk, will be removed.

Glossary of terms

Disk – refers to disk based storage, backups stored on disk are available quickly, without manual handling of media and often can be available to the end user to self-manage a data recovery without ICT intervention. There are a Primary and Secondary sites containing disk storage.

Tape – refers to media either inside a tape library or stored in a tape storage facility. Recoveries from often require manual handling and are not available to the end user to manage. Tapes are initially located at M2 after 6 months are move the Kingston storage facility for long term storage. While tape can store data for a number of years the technology of tape drives has a finite lifetime. In practice recovery of tape data is limited to 2 generations of tape technology which last a total of 6 years.

Copy – a point in time version of the data being backed up.

Retention – Time a copy is kept before it is overwritten, specified in cycles (number of full copies) or in a time period.

Primary Site - Disk storage at Kingston, in the Davis Building.

Secondary Site - Disk storage at the M2 ICT Facility.

Proposed Retention Policy

Backups are categorised according to a combination of their data type and backup retention requirements.

Production Virtual Machine Data

The primary purpose of this backup is limited to recovery in emergency or disaster situation such as loss of the Kingston Computer Facility.

The working data used by the business is captured and backed up using the remaining policies. This policy is only designed to capture the state of a running operating system that can be restored in the event of a complete loss of a site or system.

Current Retention

- Daily for 30 days on Primary Site
- Daily for 75 Days on Secondary Site
- 3 Months on Tape

Proposed Retention

- Daily for 30 Days on Primary and Secondary Site

Backup Frequency and location	Current retention	proposed retention
Daily Primary Site	30 Days	30 Days
Daily Secondary Site	75 days	30 Days
Tape	Infinite	none

Key Savings

- This would save around 170-200 tapes per year (~$10,000) and have little impact on our DR capability.

Technical Details

- VMware backups
- Only on Netapp
- kgs-vs-nfs SVM (VMware NFS)
- kgs-vs-block SVM (VMware exchange block mounts)

Production Database Data

Current Retention

- Hourly, 12am to 10pm for 28 days on Secondary Site
- Daily for 28 days on Secondary Site
- 3 months on Tape

Proposed Retention

- Hourly, from 2am to 12am over 14 days on Secondary Site
- Daily for 30 days on Secondary Site
- Weekly for 2 years on Secondary Site
- Yearly for 6 years on Tape

Backup Frequency and location	Current retention	proposed retention
Hourly Primary Site	1 per hr x 28 days	1 per hr x 30 days
Daily Secondary Site	30 days	30 days
Weekly Secondary Site	Nil	104 (2 years)
Tape	Infinite	1 per year for 6 years

Key Savings

- Long term tape storage no longer be required. The number of tapes required per year would drop to approximately half with no significant disruption to our ability to recover data.

Technical Details

- SQL Client Backups

- SharePoint Backups
- 2 Schedules at 0030 and 0045 to spread impact

Production Application Data

Defined as Email Data, Active Directory (Identity) data as other key application data.

Currently

- Daily M-F for 28 days on Secondary Site
- 3 months on tape on Secondary Site

Proposed Retention

- Daily for 30 days on Secondary Site
- Weekly for 2 years on Secondary Site
- Yearly for 6 years on Tape

Backup Frequency and location	Current retention	proposed retention
Daily Secondary Site	28 Working Days	30 days
Weekly Secondary Site	Nil	2 years (104)
Tape	Infinite	1 per year (over 6 years)

Key Savings

- Long term tape storage no longer be required. The number of tapes required per year would drop to approximately half with no significant disruption to our ability to recover data.

Technical Details

- Standard Client Backups (File level)
- Exchange Backups (TASDAG)
- Active Directory Backups

Non Production, Database and Application Data [New]

Targets Development, Testing and other Non-Production systems.

Currently

- 12am to 10pm for 28 days on Secondary Site
- 3 months on Tape

Proposed Retention

- Daily for 30 days - secondary site.

Backup Frequency and location	Current retention	proposed retention
Hourly Secondary Site	1 per hr x 28 days	Nil
Daily Secondary Site	Nil	30 days
Weekly Secondary Site	Nil	Nil
Tape	Infinite	Nil

Key Savings

- Tape storage no longer be required.

Technical Details

- Standard Client Backups (File level)
- SQL Clients

Standard File Share Data

Targets File shares used.

Currently

- 2 hourly 8am - 6pm for 28 days on Primary Storage
  - *Users can restore files from this copy without ICT assistance.*
- Daily for 28 days on primary and secondary storage
- 3 months on Tape

Proposed Retention

- Hourly between 7am and 7pm for 14 days on primary storage.
  - *Users can restore files from this copy without ICT assistance.*
- Daily for 30 days on Primary and Secondary Storage
- Weekly for 2 years on Primary and Secondary Storage
- Yearly for 6 years on Tape

Backup Frequency and location	Current retention	proposed retention
Hourly Primary Site	2hr x 28 days	1hr x 14 days
Daily Secondary Site	28 Days	30 days
Weekly Secondary Site	Nil	2 years (104)
Tape	Infinite	1 per year (over 6 years)

Key Savings

- Long term tape storage no longer be required. The number of tapes required per year would drop to approximately half with no significant disruption to our ability to recover data.

Technical Details

- Standard Client Backups (File level) –on a single client kgs-fs03
- Hourly backups accomplished using VSS
- Current system uses weekly synthetic fulls and daily incrementals to achieve retention
- Netapp Clients
- Kgs-vs-data SVM

Scientific File Share Data [New]

Targets file shares used for scientific datasets that has little to no changes over time. Data is not retained on tape, if offsite storage is required it is suggested that cloud services are used as a repository for this data. Due to the nature of the data and its lack of regular changes only daily changes are kept.

Users of these systems can restore files from disk without ICT assistance.

Currently

- 2 hourly 8am - 6pm for 28 days on Primary Storage
  - *Users can restore files from this copy without ICT assistance.*
- Daily for 28 days on primary and secondary storage
- 3 months on Tape

Proposed Retention

- Hourly between 7am and 7pm for 14 days on primary storage.
  - *Users can restore files from this copy without ICT assistance.*
- Daily for 30 days on Primary and Secondary Storage
- Weekly for 2 years on Secondary Storage

Backup Frequency and location	**Current retention**	**proposed retention**
Hourly Secondary Site	2hr x 28 days	1hr x 14 days
Daily Secondary Site	28 Days	30 days
Weekly Secondary Site	Nil	2 years (104)
Tape	Infinite	Nil

Key Savings

- This would be a significant policy change to consider, it primarily affects the data centre (science_archive share) and atmos (atmos share). The impact in removing tape storage from the mix of recovery options would need to be considered by IT and the Business units.
- This would save around 100 tapes a year (~$6,000) , with further savings over time.
- It would save 14-21 days of data transfer time from the tape backup period each quarter.

Technical Details

- Netapp ONLY
- kgs-vs-data SVM (some volumes)

Australian Government

Department of the Environment and Energy

Australian Antarctic Division

ICT Change Management Process

DOCUMENT CONTROL

File [RM8] ref:	Responsible Officer: **ICT Change Manager**	Authorising Officer: **ICT Manager**	Authorisation Date:
Version: **1**			
Location of Master Copy:			Review Date: **May 2017**
Location of Hard Copies/Points of Use:			
Business Classification: Unclassified			

VERSION HISTORY

Revision number	Year of Operation	Authorisation Date	Date of Next Review
1	2017-2018		

AMENDMENT HISTORY

Revision Number	Location of amendment (i.e. page #, para #, etc)	Addition / Deletion / Update	Description of amendment	Data amended	Author
1	n/a	Update	New document		XXXX
2	Pages 7, 9, 10, 11, 12, 13, 19, 20, 21	Addition / Update	Changes to process		XXXX
3	5.1 (page 19)	Update	Added meeting agenda		XXXX

Contents

1. Introduction

The Change Management process is designed to identify, treat and minimise risks for ICT changes through a standardised methodology. The Australian Antarctic Division (AAD) manages a medium size, business critical enterprise ICT environment that embraces change management. Through the change management process the AAD aims to facilitate efficient and prompt handling of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of changes.

1.1. Objectives

This document states the Change Management process used by the AAD and aims to achieve the following objectives:

- Define the change model for AAD.
- Define the workflow for a Normal Change.
- Define the minimum documentation required for a Normal Change.
- Define the process for Standard Changes and Emergency Changes.
- Define the communication methods for the change process.
- Outline reporting objectives to improve the Change Management process.

1.2. Scope

The definitions of the document only apply to the AAD's ICT Change Management process and does not represent the other process areas including Incident or Problem.

2. Change Overview

2.1. Definition of a Change

The AAD formally embraces the ITIL definition of a Change:

> *"The addition, modification or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items"*

Any changes that affect AAD systems that are marked as Configuration Items (CI) should be logged as a Change Request to go through the formal change process. This includes, but is not limited to:

- Server changes
- Infrastructure changes
- Network changes
- Software changes
- Application Changes
- Telecommunications changes

Sometimes, changes can be so insignificant that they do not warrant a Change Request. A change is not needed when:

- Standard software is being installed on multiple PCs
  - Ø If there is a larger number, a Change Request may be required at the discretion of the ICT Change Manager.
- The affected users or PCs are fewer than five.
- The item being worked on is not defined as a CI.
- The ICT Change Manager has waived the need for a specific change.

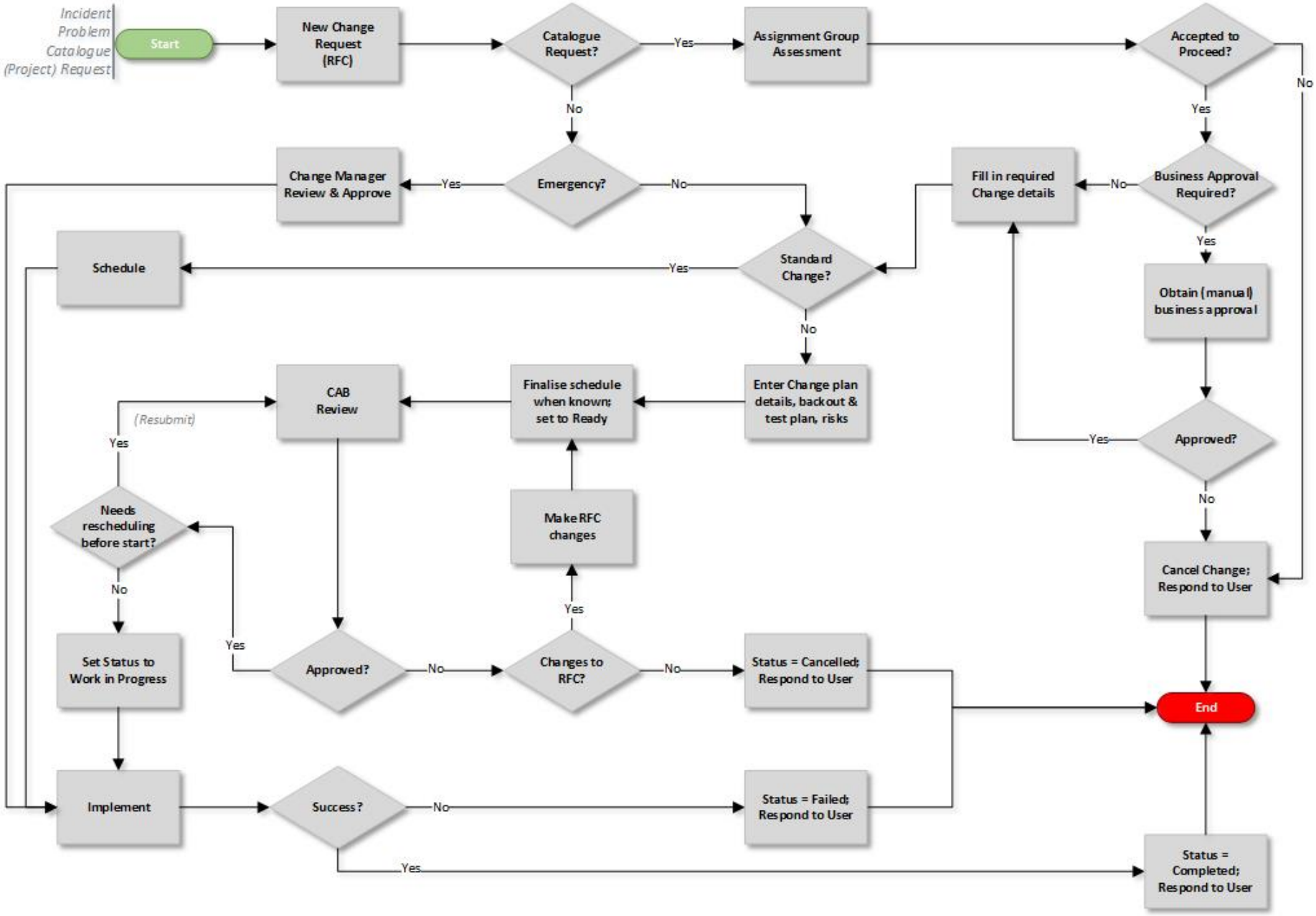
2.2. Change Process Overview

A change is initiated when there is a "request for change" (RFC) made. RFCs can be created from multiple sources:

- From an Incident that requires a change to a system or application to resolve the issue.
- From a Problem as a result of identifying a root cause and the change required.
- From the Service Catalogue when users request specific items from the catalogue that must go through change control to be fulfilled.
- From an enhancement request to make changes to an existing system or application, or create a new system or application.

2.2.1. Change Process Workflow

The process flow for all changes is shown on the next page.


Incident
Problem
Catalogue
(Project) Request
Start
New Change Request (RFC)
Catalogue Request?
Yes
Assignment Group Assessment
Accepted to Proceed?
No
Yes
Business Approval Required?
No
Fill in required Change details
Yes
Obtain (manual) business approval
Approved?
Yes
No
Cancel Change; Respond to User
End
Emergency?
Yes
Change Manager Review & Approve
No
Standard Change?
Yes
Schedule
No
Enter Change plan details, backout & test plan, risks
Finalise schedule when known; set to Ready
CAB Review
(Resubmit)
Yes
Needs rescheduling before start?
No
Set Status to Work in Progress
Implement
Success?
No
Status = Failed; Respond to User
Yes
Status = Completed; Respond to User
Approved?
Yes
No
Changes to RFC?
Yes
No
Make RFC changes
Status = Cancelled; Respond to User

2.3. Change Risk Assessment

Every change that is created must be assessed for its risk to the business. Regardless of the change type, an assessment must be made of what the impact would be to the business if the change failed, and the likelihood of that occurring.

2.3.1. Risk Matrix

The below Change Matrix must be used to govern the risk of any change:

		IMPACT				
		Negligible	**Minor**	**Moderate**	**Major**	**Severe**
LIKELIHOOD	**Rare**	LOW	LOW	MEDIUM	MEDIUM	HIGH
	Unlikely	LOW	MEDIUM	MEDIUM	MEDIUM	HIGH
	Possible	LOW	MEDIUM	MEDIUM	HIGH	CRITICAL
	Likely	MEDIUM	MEDIUM	HIGH	HIGH	CRITICAL
	Certain	MEDIUM	HIGH	HIGH	CRITICAL	CRITICAL

2.3.2. Impact and Likelihood Definitions

Impact	Negligible	Change most likely will not cause a loss of service
	Minor	Change might cause loss of service for less than 10 minutes
	Moderate	Change causes loss of service for less than 30 minutes
	Major	Change causes loss of service for more than 30 minutes and/or causes reputational risk
	Critical	Change causes loss of service that places people or organisational reputation at risk
Likelihood	Rare	There is no foreseeable reason why this change would fail
	Unlikely	There is some opportunity for the change to fail but the chance is unlikely (25%)
	Possible	There is at about a 50% chance the change will cause a failure
	Likely	There is about a 75% chance the change will cause a failure
	Certain	It is 100% certain that the change will cause a failure

The Risk will be calculated by ServiceNow. You will only need to supply the impact and likelihood to the change record.

2.4. Change Codes

Some fields in an RFC are static values that need to be assigned to the RFC to enable workflow or provide meaningful reporting. These codes are detailed below.

2.4.1. Categories

- Applications
- Hardware
- Infrastructure
- Network
- Security
- Software
- Telecommunications
- Other

2.4.2. Closure Codes

- Successful
- Partially Successful
- Unsuccessful and Rolled Back
- Unsuccessful Not Rolled Back
- Withdrawn

2.5. RFC Documentation

The minimum documentation required for each change within ServiceNow is as follows:

- When creating an RFC (Draft and Ready):
  - Ø Short Description – for most changes this will be copied from the Incident, Problem or Service Catalogue request, but it should briefly describe the change that is to be made
  - Ø Description – a full description of the change
  - Ø Planned start and end dates and times on the Schedule tab
  - Ø Risks – in addition to the risk category from the impact and likelihood matrix, a description of the major risks must also be stated
  - Ø Change Plan – this outlines how the change is to be implemented, step-by-step; some changes may be implemented by a Release Manager, so knowledge of what needs to be done should not be assumed
  - Ø Backout Plan – a clear step-by-step plan of how to reverse the change if it has not been successful, also with no assumed knowledge
  - Ø Test Plan – the testing that is to be performed to confirm the change is successful prior to being implemented into a production system; this plan needs to document testing steps and expected outcomes so that the success of testing can be validated.
- When implementing a change (Work in Progress):
  - Ø Actual start and end times – when starting and ending implementation
  - Ø Notes (Additional Comments) – note any discrepancies or variations to the change plan when the change is being implemented.

- When closing a change (Completed):
  - Ø Closure Code – indicating the success or failure of the change
  - Ø Close Notes with further details as required.

Documentation can be provided in attachments, but each relevant field should clearly state which attachment should be referenced for each field.

3. Change Types

There are three types of change used within the AAD environment:

STANDARD CHANGE

- ► Pre-approved
- ► Performed frequently
- ► Predictable outcome
- ► Known low risk
- ► Minor impact

NORMAL CHANGE

- ► Non-repetitive
- ► Comprehensive plan
- ► CAB approval required

OUT OF CAB CHANGE

- ► Expedited Normal Change

EMERGENCY CHANGE

- ► Restore a business critical service.
- ► Same day implementation.
- ► ICT Manager or ICT Change Manager approval required.

Each of these change types are explained in more detail in the following sections.

3.1. Standard Change

A Standard Change is a change that regularly occurs within the organisation, which has been pre-assessed by CAB and whose risks are well known and treatable. A list of approved standard changes are available in ServiceNow.

3.1.1. Standard Change Workflow

Standard changes are minor changes that have previously been performed frequently and are deemed to be regular, low-risk changes, or standardised changes that can be requested by end users via the Service Catalogue.

- The RFC is created using a form selected from the Standard Change item list.
- In the case of changes requested by users from the Service Catalogue, the RFC will be created as a Standard Change upon saving the request.
- The following fields need to be included in a Standard Change. These details should be in either the Record Producer templates for Service Catalogue requests or in the defined Standard Change:
  - Ø The Change Plan – steps for implementing the change
  - Ø If available, the backout plan if the change is unsuccessful and needs to be reversed.

- For Service Catalogue requests, the specific details of the user's requirement will have been passed into the RFC from a series of questions they were asked in the request form.
- Make any adjustments or additional notes in the RFC as required for the change.
- Once the change is ready to be implemented in the change window, the status should be set to **Work in Progress** while the work is being done.
- Once work is completed, verify the change has been implemented successfully.
- If the implementation has failed, implement the rollback plan if there is one available, then set the status to one of the **Unsuccessful** options accordingly.
- If the implementation was successful, change the status to **Completed**.
- Set the Closure Code as appropriate, and provide closure notes.

3.1.2. Standard Change Approval Process:

For a Standard Change to be created, the type of change must be considered by CAB for approval to accept the change as low risk. The nominated change must meet the following requirements:

- The change must have occurred within the environment at least 5 times.
- The change must be considered a low risk change. Medium and High risk changes cannot be a standard change.
- Documentation on the change implementation and rollback strategies are available on the Knowledge Portal. This change implementation must be followed each time.
- The window in which the change will normally occur will not interfere with service continuity.

To nominate a Standard Change to CAB, the requester must provide the following documentation to the ICT Change Manager for tabling at a CAB meeting:

- A list of the previous change numbers (at least five) for review.
- The implementation and rollback procedure document.
- The proposed change window.

It is the responsibility of the CAB to assess the request and ensure that:

- The risk of failure as a result of implementing this change is a *low* risk.
- The change can be implemented with minimal supervision.
- That the implementation and rollback strategy is sufficient to correct any issues.
- That the lead time and change window has been repeatedly established such that it does not interfere with service continuity.

Once approved by CAB the Standard Change Template may be created in ServiceNow.

Any changes then created using this standard template are deemed to be pre-approved and can proceed without further ICT Change Manager or CAB approval, however, any other approvals (such as business approval) must still be sought as appropriate. The ICT Change Manager has the authority to review any standard changes currently in progress to ensure they are meeting requirements as previously approved.

3.2. Normal Change

A normal change is any change that does not fall into the category of a Standard or Emergency change. Normal changes are irregular and typically have higher risk profiles. All normal changes will be assessed and approved by the Change Advisory Board (CAB).

3.2.1. Normal Change Workflow

Normal changes will typically come from Incidents, Problems, and Requests which have been through a development cycle. The steps for a Normal Change are as follows:

- The RFC is created in **Draft** mode as a Normal Type, with all relevant details entered. Some fields may have been copied from the initiating Incident or Problem.
- The change must be scheduled for implementation at an appropriate future date and time within the allowed change window to allow for necessary reviews and approvals.
- The details needed for the change must be entered:
  - Ø A short description to title the Change
  - Ø A description or justification for the Change
  - Ø Impact and Likelihood should be set to an accurate level
  - Ø A category to represent what this Change is affecting
  - Ø A brief description of the risks
  - Ø The plan for implementing the change
  - Ø The backout plan if the change is unsuccessful and needs to be reversed
  - Ø A plan for testing the change before it is implemented into production
  - Ø The planned start and end date and time
- Click the Request Approval button in preparation for the next CAB meeting.
- The CAB will review the change and approve it if it meets all requirements and the risk is deemed acceptable.
- Once the change is ready to be implemented on the planned date, the status should be set to **Work in Progress** while the work is being done.
  - Ø If the planned date changes, you must alter the Revised start and end dates to reflect the new schedule.
- Once work is completed, verify the change has been implemented successfully.
- If the implementation has failed, implement the rollback plan if there is one available, then set the status to one of the **Unsuccessful** options accordingly.
- If the implementation was successful enter the Actual Start and End dates to reflect when the change occurred.
- Change the status to **Completed**.
- Set the Closure Code as appropriate, and provide closure notes.

3.2.2. CAB Review and Approval

Once an RFC has moved to the Ready status, the ICT Change Manager can produce a list of changes for discussion at the regular CAB meeting. Once a change has been reviewed and approved or declined, the ICT Change Manager needs to:

- Note the date of the CAB meeting.
- Make appropriate notes in CAB recommendation.
- Approve or Reject the change as appropriate.
- Return the change for further information if required.

3.3. Out of CAB Changes

An Out of CAB Change is a Normal change that is scheduled before the next CAB meeting.

Out of CAB Change Process	► An Out of CAB (OOC) Change is a Normal change with an implementation date before the next scheduled CAB meeting. ► This Change must be Endorsed by at least one CAB member (with no objections) and approved by the ICT Manager or ICT Change Manager before you can proceed.

If you require Out of CAB (OOC) approval for a Normal Change, set the following options:

1. **Check** the option **Out of CAB Approval**
2. Click **Update**

This will notify the Change Advisory Board (CAB) members of the OOC Change.

Once Approved:

3. You will be notified by email
4. The change can commence as planned

If Rejected:

5. You will be notified by email
6. The Change must not proceed
7. The Change Request will be reviewed by CAB

3.4. Emergency Change

An Emergency Change is a change that must occur as soon as possible to resolve a major incident. The Emergency change template is available in ServiceNow.

3.4.1. Emergency Change Workflow

An Emergency Change is a change that follows an expedited process. During normal business hours, an RFC **must** be created in the system, though with fewer fields than available in a Normal Change. The ICT Change Manager or delegate must approve the change before it is implemented into production.

- The RFC is created in **Draft** mode as an Emergency Type.
- Enter as much information as possible to explain the need for the emergency change.
- Place the RFC into a **Ready** status.
- ServiceNow will notify the ICT Change Manager and ICT Manager that the emergency change needs to be approved.
- The ICT Change Manager or ICT Manager will review the change and set it to Approved or Rejected as appropriate.
- Once approved, implement the change (**Work in Progress**), updating the RFC with the work dates and appropriate Closure Code, and setting status to **Completed**.

If an Emergency Change is required outside normal business hours:

- Notify the ICT on-call officer.
- Create an Emergency Change in ServiceNow.
  - This sends an email to the ICT Manager, ICT Change Manager.
- The ICT on-call officer will follow this up by calling the ICT Manager and ICT Change Manager.
  - If the ICT Manager and ICT Change Manager are unavailable, the ICT on-call officer is permitted to approve the change.
- The ICT on-call officer will provide support to coordinate the change.
- All changes made must be documented in the Emergency Change Request.

4. Roles and Responsibilities

4.1. ICT Change Manager Responsibilities

It is the responsibility of the ICT Change Manager to manage all change activity within the scope of the defined change management process. The ICT Change Manager will oversee the management of change as per the following sections.

4.1.1. Normal Change

The ICT Change Manager will be responsible to chair CAB. Responsibilities include:

- Generating a review list of all normal changes awaiting approval.

- Ensuring that the risk stated on the change is appropriate and is accepted by CAB.
- Documenting any outcomes in the notes of the appropriate change.
- Managing the status of each change including approval and rejections.
- Communicating with stakeholders as appropriate.

4.1.2. Standard Change

The ICT Change Manager will manage the lifecycle of all Standard changes, including:

- Reviewing proposed Standard Changes to ensure they meet the relevant criteria.
- Ensuring Standard Changes are being handled and implemented correctly.
- Conducting periodic review of Standard Changes to ensure currency for risk and relevance.
- Retiring Standard Changes.

4.1.3. Emergency Change

The ICT Change Manager is responsible for the Emergency Change process, including:

- Making sure all Emergency Changes requested during business hours receive approval.
- Ensuring Emergency Changes have valid reasons for expedited implementations.
- Educating and encouraging business and ICT staff to use better planning for changes.
- Reviewing any Emergency Change that has been implemented out of hours under the exemption process in Section 3.3.

4.1.4. Governance

The ICT Change Manager is responsible for overseeing the governance of the Change Management Process and contributing in the following areas:

- Review the Change process and identify areas for improvement as necessary.
- Document any process improvements and submit to CAB for consideration and approval.
- Update the Change Management Process Documentation as required.

4.1.5. Day to Day Activities

The ICT Change Manager is responsible for overseeing the day to day management of change activities to ensure:

- ICT staff who implement changes are sufficiently trained and familiar with the Change Management process.
- That all changes are occurring within their scheduled windows.
- That changes are not occurring without prior approval.

4.2. Change Advisory Board Responsibilities

It is the responsibility of CAB to ensure that a consistent approach is being used when managing change. The members of the CAB will ensure that the requirements of each change type are being addressed to reduce risk for each change activity.

4.2.1. Standard Change

When asked to approve a new Standard Change, the CAB is responsible for ensuring that the following quality control areas are considered:

The risk of failure as a result of implementing this change is low risk:

From the list of previous Normal changes provided by the ICT Change Manager, CAB will investigate the success rate of these changes and consider any issues that did or could have occurred. Based on this investigation CAB will assess if the change is always likely to be low risk in nature.

The change can be implemented with minimal supervision:

CAB will review the information provided with the proposed Standard Change, along with the history of previous changes of this type, to ensure there is sufficient information to step the implementer through the process without requiring assistance.

That the implementation and rollback strategy is sufficient to correct any issues:

CAB will ensure that a rollback strategy is documented and has been tested for correctness. CAB will ensure that this document is available on the Knowledge Base to ensure that any staff member actioning the change knows what to do if something goes wrong.

That the lead time and change window has been repeatedly established such that it does not interfere with service continuity:

CAB will assess the provided change window to ensure that it is not within a period of known business activity and that the change can be implemented with minimal or no downtime.

CAB will approve the creation, modification or removal of standard changes as appropriate, to be actioned by the ICT Change Manager.

4.2.2. Normal Change

CAB will be responsible for ensuring that any changes raised by the ICT Change Manager are governed and approved within the Change Management Process Guidelines. CAB will be responsible for:

- Ensuring that the risk level provided is correct for the given change.
- Assessing any documentation supplied to ensure that it is comprehensive and accurate enough for its purpose.
- Ensuring that appropriate approvals are sought if the risk of a change breaches the risk thresholds listed in the Risk Matrix (section 2.3).
- Openly discussing the technical details and operational risks of the change and requesting advice from appropriate parties if the technical details or risks are not well understood.
- Ensuring that there is an appropriate, documented rollback plan for each change.
- Making sure the change window specified includes sufficient time for rollback.
- Ensuring relevant staff are given sufficient notice of when the change will occur.

CAB reserves the right to approve, seek clarification, or reject any change request based on the above criteria. CAB will defer approval rights to the Business Owner should the risk of the change breach the threshold listed in the Risk Matrix (section 2.3).

4.3. Approver Responsibilities

Approvers in the Change Management process include:

- ICT Change Manager
- CAB Members
- ICT Manager
- Business Owner

Before approving a change, approvers are responsible for:

- Considering and fully understanding all information available.
- Considering the business or reputational risk.
- Considering any associated costs.
- Considering implications if the change is to occur.

4.4. Information Technology Security Advisor Responsibilities

It is the responsibility of the Information Technology Security Advisor (ITSA) to assess each change to ensure that it doesn't:

- Breach any security guidelines specified by the agency.
- Expose any confidential data to unauthorised parties (Confidentiality).
- Intentionally or unintentionally alter user data (Integrity).
- Increase the likelihood of data not being able to be accessed (Availability).

Should the ITSA find that the change has one or more of the above risks it is their responsibility to advise CAB of the specific area of concern. Should the ITSA not be satisfied with the corrective actions of CAB, the ITSA must raise the concern directly with the ICT Manager in the form of a written report.

5. CAB Meetings

CAB meetings are held on a regular basis to review any requested Normal Changes that require approval, and to review change implementation outcomes of the prior period.

Meetings will be held **weekly**. The **prior period** is the week before the current meeting. The CAB meeting is to discuss changes to be implemented in the week up to the next CAB meeting.

The meeting agenda and process is as follows:

- All changes needing to be included in the CAB meeting must be at a Ready status no later than 10:00am on the day of the meeting.
- The ICT Change Manager will generate two reports as soon as practical after 10:00am and will forward the reports to the CAB meeting attendees:
  - Ø A report on all Ready changes that are due to be implemented within the period covered by the CAB meeting
  - Ø A report on all changes implemented within the prior period.
- CAB members will review the list of changes prior to the meeting to familiarise themselves with the requested changes.
- Any change seeking approval at a CAB meeting must have representation at the meeting (either the Change Coordinator or a nominated delegate). Any change that does not have representation will be automatically rejected unless prior notification is given to the ICT Change Manager with a legitimate reason for the absence.
- The CAB meeting will be convened by the ICT Change Manager and will firstly review the Ready change list as prepared earlier the same day.
- Each change will be reviewed and discussed by CAB and the change coordinator. CAB will then approve or give reasons for rejection.
- Once all submitted requests for change have been discussed, the CAB will then discuss any changes performed in the prior period with emphasis on unsuccessful or partially successful changes, to determine courses of action to be taken with regard to these changes.
- If there have been any Emergency Changes in the prior period, these should be discussed with regard to outcomes and mitigating future occurrences.
- Following this, the ICT Change Manager will then raise any requests for Standard Changes to be created for discussion with CAB.
- If required, any noted deviations from the normal process for all changes should be raised and discussed.
- The CAB meeting will conclude with any other business items as raised by attendees.

5.1. Change Meeting Agenda

The following is the standard CAB meeting agenda:

Item	Description	Duration
1.	Review change schedule for the proceeding period (7 days)	5 minutes
2.	Review new changes (approval pending)	20 minutes
3.	Review all overdue changes	10 minutes
4.	Review Standard & Emergency changes for the previous period	10 minutes
5.	Review failed & cancelled changes for the previous period	10 minutes
6.	Any other business	5 minutes

6. Communications

Automatic email notifications are generated in ServiceNow for changes generated, and these notifications will be governed by the risk the change presents to the organisation.

Notifications will outline the following information at the appropriate stage:

- A reference number for the change (all notifications)
- A description of the change (all notifications)
- When the change is to be implemented
- What systems and who will be affected
- Who to call in the event of any issues after the change has been implemented

The below table outlines the communications that will occur:

Risk Rating	Notify	Communication Type
Low	ICT Change Manager, Stakeholders	ServiceNow Notification
Medium	ICT Change Manager, Stakeholders	ServiceNow Notification
High	ICT Change Manager, Stakeholders, Business Owner	ServiceNow Notification, and call/meeting with Business Owner.
Critical	ICT Change Manager, Stakeholders, All affected Staff	All staff email, Meeting with Business Owner, ServiceNow notification for CAB and stakeholders

6.1. Notifications

The following table outlines the content of the automated notifications from ServiceNow.

Conditions	To	Content
Approval changes to Approved or Rejected	Created by, Watch list, Assigned to, Requested by	Change Request **${URI_REF}** has been **${approval}**. **Name:** ${requested_by} **Status:** ${state} **Short description:** ${short_description} **Approval:** ${approval} ${approval_history}
All new RFCs	ICT Change Manager (Group)	A request for change has been created. **Number:** **${URI_REF}** **Requested by:** ${requested_by} **Type:** ${type} **Status:** ${state} **Risk:** ${risk} **Short description:** ${short_description} **Category:** ${category} **Assignment Group:** ${assignment_group.name} **Planned Start:** ${start_date} **Planned end:** ${end_date} **What are the risks?** ${u_risks} **Change Plan:** ${change_plan} **Backout Plan:** ${backout_plan} **Test Plan:** ${test_plan} **Impact:** ${impact} **Likelihood:** ${u_likelihood}
Additional Comments changes	Watch list, Requested by,	Change Request **${URI_REF}** has been commented. **Requested by:** ${requested_by}

AND Status is not Draft	Created by, Assigned to	**Status:** ${state} **Short description:** ${short_description} ${comments_and_work_notes}
Assigned to is empty AND Assignment group is not empty AND Assignment group changes	Assignment group	A request for change has been assigned to ${assignment_group}. **Number:** **${URI_REF}** **Requested by:** ${requested_by} **Status:** ${state} **Risk:** ${risk} **Short description:** ${short_description} **Category:** ${category} **Assignment Group:** ${assignment_group.name} **Planned Start:** ${start_date} **Planned end:** ${end_date} **What are the risks?** ${u_risks} **Change Plan:** ${change_plan} **Backout Plan:** ${backout_plan} **Test Plan:** ${test_plan} **Impact:** ${impact} **Likelihood:** ${u_likelihood}
Out of CAB Approval changes to true AND Approval is Requested AND Status is one of Pending, Ready	ICT CAB (Group)	OOC Change Requests must be endorsed before they are approved. Please choose one of the following options: **Endorse** to indicate you accept this change **Tentative** with a description to indicate any concerns you have regarding this change **Deny** with a description to indicate the severe impact this change may cause

		Number: **${URI_REF}** **Requested by:** ${requested_by} **Type:** ${type} **Status:** ${state} **Risk:** ${risk} **Short description:** ${short_description} **Category:** ${category} **Assignment Group:** ${assignment_group.name} **Planned Start:** ${start_date} **Planned end:** ${end_date} **Description/Justification** ${description} **What are the risks?** ${u_risks} **Change Plan:** ${change_plan} **Backout Plan:** ${backout_plan} **Test Plan:** ${test_plan} **Impact:** ${impact} **Likelihood:** ${u_likelihood}
Short description is "Request firewall rule changes for creating a firewall hole or changing priorities on traffic to and from stations"	Event creator	Dear ${requested_by.first_name}, Your request for a change has been received: **${short_description}**. Your request will be reviewed and actioned accordingly. This may require approval from your section manager. This request is not available in the ServiceNow portal, but you can review the request here: Number: **${number}**. Please contact the ICT Service Desk if you have any questions about this change or you wish to make changes.

7. Reporting

The following reports will be available regarding Change Management:

Description	Contents
Change Calendar	A calendar of all upcoming changes
Ready Change Requests	A list of all Ready and Normal change requests (for CAB)
In Progress Change Requests	A list of changes in progress
Change Requests by Risk	A list of change requests by risk
Change Requests for next week	A list of Change Requests scheduled for next week
Changes Implemented	A list of all changes implemented within the specified date range

Australian Government

Department of the Environment and Energy

Australian Antarctic Division

ICT Incident Management Process

2017-2020

Document Control

File [RM8] ref:	Responsible Officer: **ICT Incident Manager**	Authorising Officer: **ICT Manager**	Authorisation Date: **24/05/2017**
Version: **1**			
Location of Master Copy: \\aad.gov.au\files\ICT\Shared\Projects\Service Desk Replacement Project\Process Docs			Review Date: **April 2020**
Updates to be added into the related ServiceNow KB article.			
Business Classification: **Unclassified**			

VERSION HISTORY

Revision number	Year of Operation	Authorisation Date	Date of Next Review
1	2017-2020	24/05/2017	April 2020

AMENDMENT HISTORY

Revision Number	Location of amendment (i.e. page #, para #, etc)	Addition / Deletion / Update	Description of amendment	Data amended	Author
1	n/a	Update	New document	all	XXXX
1.1	4.1	Deletion	Altered New incident notification due to incompatability for incidents logged by email.	Removed "Dear ${caller_id.first_name},""	XXXX
2	2.2.2	Deletion	Altered priority matrix	Removed (5) VERY LOW	XXXX
2.1	2.2.4	Update	Amended definition of VIP users	Removed 'All EL2' Included SCTOs	XXXX
2.2	2.2.5	Update	Amended default priority of email logged tickets	Changed standard user to (4) LOW Changed VIP user to (3) MEDIUM	XXXX
2.3	2.3.1	Deletion	Amended SLA table	Removed (5) VERY LOW	XXXX
2.4	2.3.1	Deletion	Deleted one of the key points	Removed pause conditions as SLA timer does not pause	XXXX
2.5	4.1	Addition	Amended Resolved notification	Additional line of text advised user to reply to re-open the incident	XXXX

Contents

1.0 Introduction

The Incident Management process is designed to restore service to ICT systems and infrastructure that are not working as required. The Australian Antarctic Division (AAD) operates two tiers of support to directly support its staff with additional vendor support for non-standard issues that arise.

1.1 Purpose

The purpose of this document is to state the Incident Management process used by the AAD. This document aims to achieve the following objectives:

- Define Incident workflow, processes, and definitions
- Outline the Service Level Agreement for resolving Incidents
- Provide a way to manage customer expectations around Incidents
- Outline reporting objectives to improve the Incident Management process

1.2 Objectives

The objectives of this document are to:

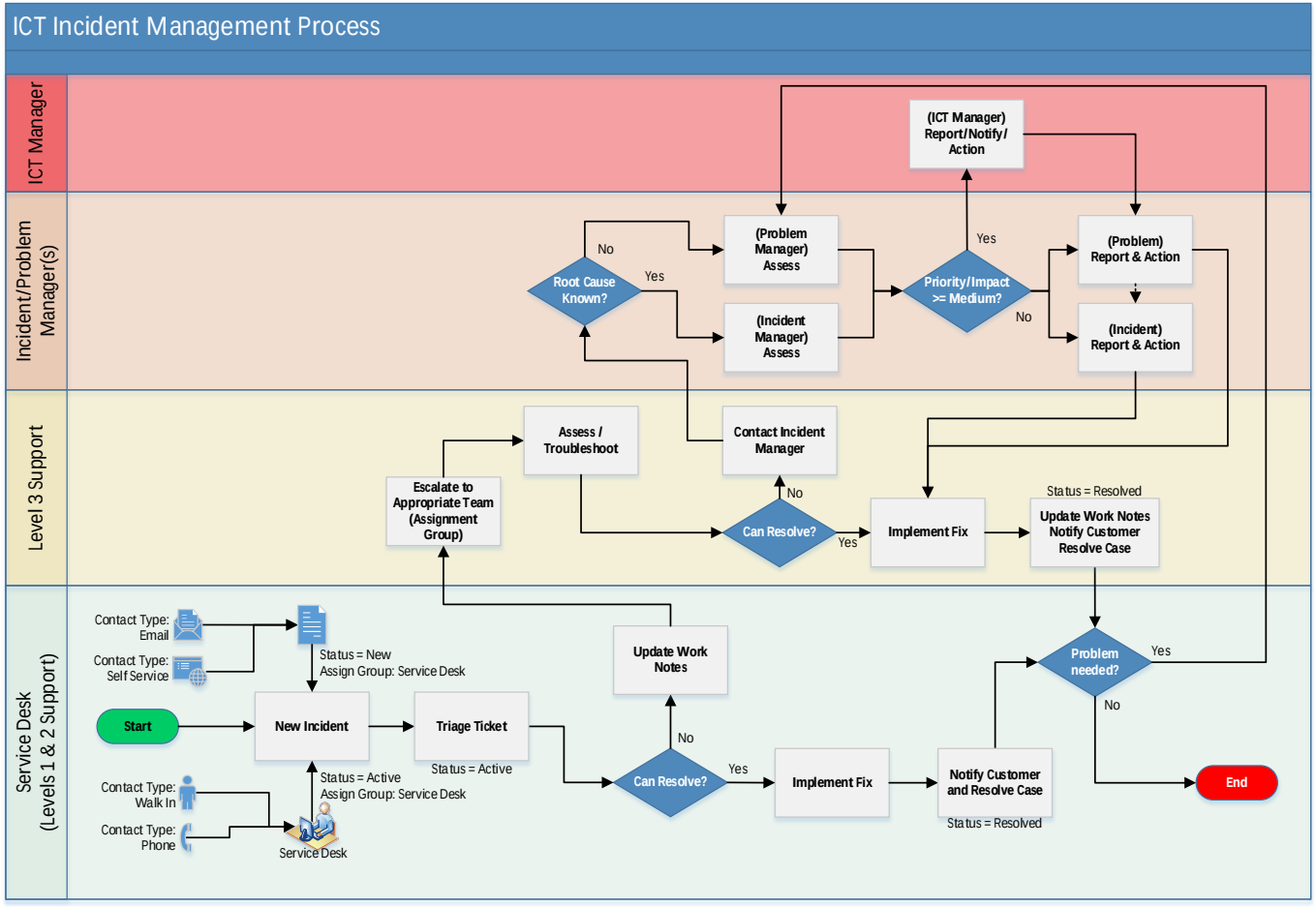
- Define the Incident workflow
- Define the classification of Incidents
- Define the Impact, Urgency, and Priority of Incidents
- Outline the Service Level Agreement for starting and resolving Incidents
- Define the escalation path for Incidents that can't be resolved with the Service Desk
- Provide a robust foundation with the view to improving the customer's experience

1.3 Scope

The definitions of the document only apply to the AAD's Incident Management process and do not represent the other process areas including problem or change.

2.0 Incident Management Process

2.1 Workflow



2.2 Incident Classification

To effectively classify an Incident, two areas are used; categorisation and priority. When used properly these two areas will indicate what needs attentions and what impact it is having on the organisation.

2.2.1 Categorisation

The categorisation process classifies Incidents in order to derive two benefits:

1. Easier to route work to the correct teams if necessary
2. Reporting - provide analytics around where the organisation can focus to reduce Incidents

The category hierarchy used for incidents is Category, Type and Item. Each category contains dependant sub-categories.

The table below defines the top level categories (Category and Type) and their dependencies:

Category	Type
Applications	Administration
	Bug/Error
	Database
	Data Quality
Communications	Email
	Online Meeting
	Skype
Hardware	Desktop
	Laptop
	Tablet
	Non-SOE Computer
	Monitor
	Peripherals
	VC Equipment
Identity Management	Reset Password
	Unlock Account
	Account Management
	Department of Environment
Printers	MFD Print
	Personal Printer
	Label Printer
	Scanner
Network	Connectivity
	Firewall
	Proxy
	Wall Socket

	Wireless
Remote Access	Authentication
	Virtual App
	Virtual Desktop
	VPN
Software	SOE Software
	Non-SOE Software
Servers & Storage	Servers
	Website
	Storage
	File Shares & Data
Security	Virus Alert
	Security Event
Telecommunications	Desk Phones
	Mobile Phones
	Satellite Phones
	Radios

2.2.2 Priority

The below Impact/Urgency Matrix should be used when assessing priority:

		IMPACT		
		(3) LOW	**(2) MEDIUM**	**(1) HIGH**
URGENCY	**(3) LOW**	(4) LOW	(4) LOW	(3) MODERATE
	(2) MEDIUM	(4) LOW	(3) MODERATE	(2) HIGH
	(1) HIGH	(3) MODERATE	(2) HIGH	(1) CRITICAL

2.2.3 Impact

Impact is defined by the number of users that are affected as shown in the table below.

IMPACT	(3) LOW	(2) MEDIUM	(1) HIGH
	Single User	Section/Station	All AAD

2.2.4 Urgency

Urgency is defined by the maximum allowable time required to find a solution.

URGENCY	(3) LOW	(2) MEDIUM	(1) HIGH
	Incident is not time sensitive.	As soon as possible or VIP user.	An immediate and sustained effort is required using all available resources until resolved.

VIP users are flagged in ServiceNow by the "VIP?" checkbox and strictly include the following:

- Executive (including SES and EL2 in management roles)
- Polar Medicine Unit (PMU)
- Crisis Management & Recovery team (CMR)
- Station Leaders and Station Communications and Technical Officers (SCTOs)

2.2.5 Incidents raised by email

The default priority for an incident raised by email is set by a condition as defined in the table below;

User type	PRIORITY
Standard User	(4) LOW
VIP User	(3) MEDIUM

In ServiceNow VIP users are defined by a VIP checkbox.

2.2.6 When Incidents are not Incidents

If the user accidentally raises an Incident that is not an Incident, please use the category of Inquiry/Help, then the appropriate subcategory for the purpose.

2.3 Response and Resolution Times

2.3.1 Service Level Agreement (SLA)

PRIORTY	RESPOND	RESOLVE	TOTAL	WINDOW
(1) CRITICAL	0.5	4	4.5	24x7, 365 days
(2) HIGH	1	8	9	0830 – 1700, Mon – Fri
(3) MODERATE	4	38	42	0830 – 1700, Mon – Fri
(4) LOW	17	85	102	0830 – 1700, Mon – Fri

Key Points:

- Respond, Resolve and Time are displayed in hours.
- Total Response Time (Total) = Respond + Resolve.
- Time includes any escalations or activities that need to occur to bring the resolution to closure.

2.4 Resolution and Closure

The following considerations should be observed before resolving an Incident:

- The user confirms the Incident can be closed.

- The user requests that the Incident can be closed.
- The Incident is to be set to Resolved by the assignee.
- If the Incident is reoccurring it should remain open and linked to a problem.
- If an Incident is linked to a problem, the Incident should be left open until the problem is resolved.
- If the user cannot be contacted via email or phone within the Priority 4 (P4) SLA response time, the Incident can be resolved 4 business days after last contact.

If a workaround is being used to temporarily correct a recurring behaviour, the problem manager should be asked to raise a problem and for a root cause to be established and rectified. Once a Problem Record has been created, assign the Incident to the problem and place it in the 'Awaiting Problem' Status. If the user calls again about the same Incident, raise a new case for each recurring Incident, as this will assist in reporting the true impact of the Problem.

There is a tiered approach to closure codes for incidents. This is shown in the table below:

Tier One	Tier Two	Description
Resolved by	Problem	Resolved by the problem management process.
	Change	The incident was resolved by a change managed by the change management process.
	User	Resolved by the user, no further action required.
	Incident Process	Resolved by the incident management process.
	Workaround	A solution aimed at reducing or eliminating the impact of the known incident.
Provided	Advice	Advice provided.
	Training	Formal training provided.
	Link to Knowledge Base	The user has agreed to resolve their incident by following a knowledge base article.
NFA *(No Further Action)*	Duplicate	A duplicate incident was raised in mistake.
	Cannot Reproduce	The incident cannot be reproduced.
	Referred to 3rd Party	The incident relates to a software issue which is being addressed by the vendor.
	Outside Scope	The incident falls outside the current Standard Operating Environment.
Withdrawn	No Longer Required	The user no longer needs assistance.
	Raised in Error	The incident was logged by mistake and subsequently needs to be withdrawn.

3.0 Roles and Responsibilities

3.1 Level One and Two Support Responsibilities

It is the responsibility of level one and two support staff to ensure the following:

- That the Incident's details are accurately captured to reflect the cause or symptoms of the issue
- That the Impact and Urgency have been set in accordance with Section 2.2 Classification
- That any triage steps outlined in knowledge articles related to the Incident be carried out prior to Level 3 escalation
- That Incidents that cannot be resolved within a reasonable timeframe be escalated to the appropriate level 3 team after triage
- That Incidents are being treated and resolved in order of priority and SLA set out in Section 2.2 and 2.3
- That all Priority 1 (P1) Incidents are immediately reported to the Incident Manager

If there are any issues with fulfilling these responsibilities the ICT Service Desk Supervisor must be immediately informed.

3.2 Level Three Support Responsibilities

It is the responsibility of Level 3 support staff to assist in the resolution process of all Incidents. Level 3 support staff responsibilities are to:

- Accurately capture existing Incident details to reflect the cause or symptoms of the issue
- Resolve Incidents within the defined SLA
- If an Incident cannot be resolved within the SLA or the root cause cannot be established then the Incident is reported to the Incident Manager
- Change the impact and urgency during the troubleshooting process if required in consultation with the user and/or the Incident Manager.

3.3 Incident Manager Responsibilities

It is the responsibility of the Incident Manager to manage all Incidents within the guidelines of this document. Specifically the Incident Manager is required to:

- Ensure that Incidents are being processed in line with Priority and SLA. Should an Incident breach the SLA, the Incident Manager should become aware of why the breach occurred and facilitate where possible
- Directly manage all active P1 Incidents and be aware of any active P2 Incidents at all times
- Immediately report all P1 Incidents to the ICT Manager
- Provide a post Incident report for all P1 Incidents to the ICT Manager
- Provide advice to, and work with the Problem Manager should level 3 support not be able to resolve an Incident
- Provide monthly Incident reporting for review by the ICT Manager
- Be the communications point between the business and the technical teams for all P1 Incidents

Please note outside of business hours the On Call Officer acts as the Incident Manager.

3.4 ICT Manager Responsibilities

The ICT Manager is responsible for ensuring that the end to end Incident Management process is providing value to the organisation, supported by a robust framework. Specifically, the ICT Manager is responsible for:

- Ensuring that the Incident Management Framework is robust and relevant to the organisation's needs
- Reporting on, and providing advice for all P1 Incidents and Incident trends to the senior executive for consideration
- Organising resourcing based on trends analysis

4.0 Communications

4.1 All Incidents

All Incident communications will be managed by the organisations ITSM tool, ServiceNow.

Communications will occur under the following conditions:

All incident notifications use the *AAD Default Incident Notification* layout.

All incident notifications use the following style:

```
<style>
span.normal {color: black; font-family: verdana, geneva; font-size: 10pt;}
td.listleft {width:160px;border:0px;text-align:left;color: black; font-family: verdana, geneva; font-size: 10pt;}
td.listright {border:0px;text-align:left;color: black; font-family: verdana, geneva; font-size: 10pt;}
</style>
```

All incident notification templates can be found here:
\\aad.gov.au\files\ICT\Shared\Projects\Service Desk Replacement Project\ServiceNow_Templates

Condition	Who Receives	Message
New Incident	Caller	Thank you for contacting the Australian Antarctic Division ICT Service Desk. We have received your request and will respond as soon as possible. To provide additional information, please reply to this email or view incident **${URI_REF}**. **Status:** ${u_status} **Number:** ${URI_REF} **Short Description:** ${short_description}
Incident Assigned to Group	Group	Incident **${URI_REF}** has been assigned to the **${assignment_group}** group. **SLA Due:** ${sla_due}

		Short description: ${short_description} **Status:** ${u_status} **Caller:** ${caller_id.name} **Priority:** ${priority} **Category:** ${category} **Type:** ${subcategory} **Description:** ${description}
Incident Assigned to Me	The assigned to staff member	Dear ${assigned_to.first_name}, Incident **${URI_REF}** has been assigned to you. **SLA Due:** ${sla_due} **Short description:** ${short_description} **Status:** ${u_status} **Caller:** ${caller_id.name} **Priority:** ${priority} **Category:** ${category} **Type:** ${subcategory} **Description:** ${description} ${comments_and_work_notes}
Incident Commented	Caller	Dear ${caller_id.name} Incident **${URI_REF}** has been updated. **SLA Due:** ${sla_due} **Short description:** ${short_description} **Status:** ${u_status} **Caller:** ${caller_id.name} **Priority:** ${priority} **Category:** ${category} **Type:** ${subcategory} **Assigned to:** ${assigned_to.name} **Comments:** ${work_notes}
Incident Commented	Assigned to, Watchlist	Incident **${URI_REF}** has been updated. **SLA Due:** ${sla_due} **Short description:** ${short_description} **Status:** ${u_status}

		Caller: ${caller_id.name} **Priority:** ${priority} **Category:** ${category} **Type:** ${subcategory} **Comments:** ${work_notes}
Incident Resolved	Caller	Dear ${caller_id.name}, Incident **${URI_REF}** has been resolved and will be closed automatically after 10 days. If you feel the issue is unresolved, please contact the ICT Service Desk. **Short description:** ${short_description} **Status:** ${u_status} **Resolved by:** ${resolved_by.name} **Close notes:** ${close_notes} Please **REPLY** to this email to re-open it if this issue has not been resolved to your satisfaction.

4.2 P2 Incidents

In addition to the all Incident notifications a dashboard report should be made available to all ServiceNow users on their home screen displaying all P2 Incidents. In addition, any business area that is affected by a P2 Incident should be notified by either the Service Desk or Incident Manager at minimum by email and if possible by phone. The email communication must be conducted through ServiceNow using the email function available.

4.3 P1 Incidents

When a P1 Incident is confirmed the following communications must occur:

Responsible	Medium	To Who	What it should contain
ServiceNow	email	ICT Manager, Incident Manager	Short description, description, affected business system or configuration item
Incident Manager	phone	ICT Manager	Description, system and impact, cause (if known), restoration time (if known)
ICT Manager	Phone, email	System Owner, stakeholders, anyone	Description, system and impact, cause (if known),

		else	restoration time (if known)

5.0 Reporting

The following reports will be available regarding Incident Management:

Description	**Contents**
Incidents by Priority & Status	All Incidents by status and priority 'changed' this month
Incidents by Assignment Group	All active Incidents by assignment group
Open P1 and P2 Incidents	List of all open P1 and P2 Incidents
Incidents in SLA Breach	List of all breached unresolved Incidents
Incidents not updated	List of all unresolved Incidents not updated in 5 days (42.5 hours)
Incidents by Category	Open Incidents by category
Incidents by Escalation	Unresolved Incidents by escalation (shows about to breach)

Australian Government

Department of the Environment and Energy

Australian Antarctic Division

ICT Problem Management Process

2017-2020

File [RM8] ref: Version: **1**	Responsible Officer: **ICT Problem Manager**	Authorising Officer: **ICT Manager**	Authorisation Date: **1 June 2017**
Location of Master Copy: \\aad.gov.au\files\ICT\Shared\Projects\Service Desk Replacement Project\Process Docs			Review Date: **May 2020**
Updates to be added into the related ServiceNow KB article.			
Business Classification: **Unclassified**			

VERSION HISTORY

Revision number	Year of Operation	Authorisation Date	Date of Next Review
1	2017-2020	1 June 2017	May 2020

AMENDMENT HISTORY

Revision Number	Location of amendment (i.e. page #, para #, etc)	Addition / Deletion / Update	Description of amendment	Data amended	Author
1	n/a	Update	New document	all	XXXX

Contents

1.0 Introduction

The Problem Management process is designed to manage the lifecycle of problems within an ICT environment. Through problem management the Australian Antarctic Division (AAD) aims to reduce and prevent recurring incidents from happening and to minimise the impact on the organisation of incidents that cannot be prevented.

1.1 Objectives

The purpose of this document is to state the Problem Management process used by the AAD. This document aims to achieve the following objectives:

- Define Problem workflow, processes, and definitions
- Define the Service Level Agreement for resolving Problems
- Provide a mechanism for engaging 3rd party resources
- Set customer expectations around resolution processes and times
- Outline reporting objectives

1.2 Scope

The definitions of the document only apply to the AAD's Problem Management process and does not represent the other process areas including incident or change.

2.0 Problem Management Process

2.1 Workflow

2.2 Problem Classification

To effectively classify a Problem, two areas are addressed; categorisation and priority. When used properly these two areas will indicate what needs attention and what impact it is having on the organisation.

2.2.1 Categorisation

The categorisation process classified Problems in order to derive two benefits:

1. Easier to route work to the correct reams if necessary
2. Reporting – providing analytics around where the organisation can focus to reduce Problems.

The table below defines the categories, subcategories (type):

Category	Type
Applications	Administration
	Bug/Error
	Database
	Data Quality
Communications	Email
	Online Meeting
	Skype
Hardware	Desktop
	Laptop
	Tablet
	Non-SOE Computer
	Monitor
	Peripherals
	VC Equipment
Identity Management	Reset Password
	Unlock Account
	Account Management
	Department of Environment
Printers	MFD Print
	Personal Printer
	Label Printer
	Scanner
Network	Connectivity
	Firewall
	Proxy
	Wall Socket
	Wireless
Remote Access	Authentication

	Virtual App
	Virtual Desktop
	VPN
Software	SOE Software
	Non-SOE Software
Servers & Storage	Servers
	Website
	Storage
	File Shares & Data
Security	Virus Alert
	Security Event
Telecommunications	Desk Phones
	Mobile Phones
	Satellite Phones
	Radios

2.2.2 Priority

The below Impact/Urgency Matrix should be used when assessing priority:

		IMPACT		
		(3) LOW	(2) MEDIUM	(1) HIGH
URGENCY	(3) LOW	(4) LOW	(4) LOW	(3) MODERATE
	(2) MEDIUM	(4) LOW	(3) MODERATE	(2) HIGH
	(1) HIGH	(3) MODERATE	(2) HIGH	(1) CRITICAL

2.2.3 Impact

Impact is defined by the number of users that are affected as shown in the table below.

IMPACT	(3) LOW	(2) MEDIUM	(1) HIGH
	≤ 5 Users	Section/Station	All AAD

2.2.4 Urgency

Urgency is defined by the maximum allowable time required to find a solution.

URGENCY	(3) LOW	(2) MEDIUM	(1) HIGH

	Problem is not time sensitive.	As soon as possible.	An immediate and sustained effort is required using all available resources until resolved.

2.3 Problem Resolution

2.3.1 Service Level Agreement (SLA)

PRIORTY	RESPOND	RESOLVE	TOTAL	WINDOW
(1) CRITICAL	1 Day	2 Days	3 Days	24x7, 365 days
(2) HIGH	4 Days	6 Days	2 Weeks	0830 – 1700, Mon – Fri
(3) MODERATE	10 Days	10 Days	1 Month	0830 – 1700, Mon – Fri
(4) LOW	20 Days	40 Days	3 Months	0830 – 1700, Mon – Fri

Key Points:

- Total Response Time (Total) = Respond + Resolve
- Time includes any escalations or activities that need to occur to bring the resolution to closure

2.4 Resolution and Closure

The resolution of a Problem can only occur under the following circumstance:

- That the issue is resolved in a way that ensures that the Problem does not foreseeably reoccur.

Once a Problem has been formally raised, it must be seen through to a conclusion to ensure that the impact and risk have been eliminated. If for some reason the Problem record needs to be closed without the impact and risk being treated, it should be done so with the guidance of the ICT Manager.

The following closure codes are to be used for problems:

Closure Code	Description
Fixed	The underlying root cause has been determined and the necessary action to resolve the problem has been applied.
Resolved by Change	The problem was resolved by a change managed by the change management process.
Workaround	An acceptable alternate solution that avoids the problem.
Software Update/Patch	An update or patch was applied to resolve the problem.
Duplicate	A duplicate problem has been logged.
Cannot Reproduce	The problem cannot be reproduced and is not regularly occurring to allow ongoing investigation.

Withdrawn	The problem has been logged in error and subsequently needs to be withdrawn.
System Limitation	The system does not support the necessary function to resolve the problem.

3.0 Roles and Responsibilities

3.1 Level One and Two Support Responsibilities

It is the responsibility of level one and two support staff to ensure the following:

- That any potential new problem is routed through the Problem Manager for review
- That any related incidents are attached to the correct problem record and placed in a status of 'Awaiting Problem'
- To update the problem manager if new incidents coming in related to a problem are increasing in urgency (increasing in frequency) or the impact to the organisation has changed

If there are any issues with fulfilling these responsibilities the Service Desk Manager must be immediately informed.

3.2 Level Three Support Responsibilities

It is the responsibility of Level 3 support staff to assist in identifying the root cause of the problem and act as technical and/or subject matter experts to assist in the resolution of problems where possible. Level 3 support staff are responsible to:

- Assist the problem manager to establish a root cause or sufficiently document the symptoms of the problem so that a problem manager can seek external assistance
- Advise the problem manager if they feel that the impact or urgency of the problem has been incorrectly assessed or has changed
- Provide the technical resource to fix the problem as appropriate
- Provide information on behalf of the problem manager to third parties to assist with solving the problem
- Assist the problem manager with the creation of any changes that occur to resolve the problem

3.3 Problem Manager Responsibilities

It is the responsibility of the Problem Manager to manage all problems within the guidelines of this document. Specifically the Problem Manager is required to:

- Ensure that problems are being processed in line with Priority and SLA. Should an problem breach the SLA the Problem Manager should become aware of why the breach occurred and facilitate where possible
- Directly manage all active P1 Problems and be aware of any active P2 Problems at all times
- Immediately report all P1 Problems to the ICT Manager

- Provide a post Problem report for all P1 Problems to the ICT Manager
- Provide monthly Problem reporting for review by the ICT Manager

Please note outside of business hours the On Call Officer acts as the Problem Manager.

3.4 ICT Manager Responsibilities

The ICT Manager is responsible to ensure that the end to end Problem Management process is providing value to the organisation, delivered by a robust framework. Specifically, the ICT Manager is responsible for:

- Ensuring that the Problem Management Framework is robust and current to the organisations needs
- Be the communications point between the business and the Problem Manager for all P1 Problems
- Report on, and provide advice for all P1 and P2 Problems to the senior executive
- Organise resourcing based on trends analysis

5.0 Communications

All Problems

All Problem communications will be managed by the organisations ITSM tool, ServiceNow. Communications will occur under the following conditions:

Condition	Who Receives	Message
Problem Created	Problem Manager	Problem ${number} has been created. **Short Description:** ${short_description} **Number:** ${number} **Status:** ${u_status} **Assignment Group:** ${assignment_group.name} **Assignment to:** **Comments and Work notes:** ${comments_and_work_notes}
Problem Assigned to Group	Assignment Group	Problem ${number} was assigned to ${assignment_group.name}. **Short Description:** ${short_description} **Number:** ${number} **Status:** ${u_status} **Assignment Group:** ${assignment_group.name} **Assignment to:**

		Comments and Work notes: ${comments_and_work_notes}
Problem Assigned to Me	Assigned To	Dear ${assigned_to.first_name}, Problem **${number}** has been assigned to you. **SLA Due:** ${sla_due} **Short description:** ${short_description} **Status:** ${u_status} **Caller:** ${caller_id.name} **Priority:** ${priority} **Category:** ${category} **Type:** ${subcategory} **Comments and Work notes:** ${comments_and_work_notes}
Problem Task Assigned to Me	Assigned To	Dear ${assigned_to.first_name}, A problem task was assigned to you. **Short description:** ${short_description} **Status:** ${u_status} **Caller:** ${caller_id.name} **Priority:** ${priority} **Comments and Work notes:** ${comments_and_work_notes}
Problem Commented	Assigned To, work notes list	Problem **${number}** has been created. **SLA Due:** ${sla_due} **Short description:** ${short_description} **Status:** ${u_status} **Caller:** ${caller_id.name} **Priority:** ${priority} **Category:** ${category} **Type:** ${subcategory} **Comments and Work notes:** ${comments_and_work_notes}
Problem Task Commented	Assigned to, Watch list	Problem ${number} has been created. **SLA Due:** ${sla_due} **Short description:** ${short_description} **Status:** ${u_status} **Caller:** ${caller_id.name} **Priority:** ${priority} **Category:** ${category}

		Type: ${subcategory} **Comments and Work notes:** ${comments_and_work_notes}
Problem Resolved	Caller	Dear ${caller_id.first_name}, Problem **${number}** has been resolved and will be closed automatically after 10 days. If you feel the problem is unresolved, please contact the ICT Service Desk. **Short description:** ${short_description} **Status:** ${u_status} **Assigned to:** ${assigned_to.name} **Close notes:** ${close_notes}

P2 Problems

In addition to the all Problem notifications a dashboard report should be made available to all ServiceNow users on their home screen displaying all P1 and P2 Problems. In addition, any business area that is affected by a P2 Problem should be notified by the either the Service Desk or Problem Manager at minimum by email and if possible by phone. The email communication must be conducted through ServiceNow using the email function available.

P1 Problems

When a P1 Problem is confirmed the following communications must occur:

Responsible	Medium	To Who	What is should contain
ServiceNow	email	ICT Manager	Short description, description, affected business system or config item
Problem Manager	phone	ICT Manager	Description, system and impact, cause (if known), restoration time (if known)
ICT Manager	Phone, email	System Owner, stakeholders, anyone else	Description, system and impact, cause (if known), restoration time (if known)

6.0 Reporting

The following reports will be available regarding Problem Management:

Description	Contents

Problems by Priority & State	All unresolved problems by state and priority
Problem Tasks by Assignment Group	All active problem tasks by assignment group
Open P1 and P2 Problems	List of all open P1 and P2 Problems
Problems in SLA Breach	List of all breached unresolved Problems
Problems not updated	List of all unresolved Problems not updated in X days
Problems by Category	Open Problems by category
Problems by Escalation	Unresolved Problems by escalation (shows about to breach)

Australian Government

Department of the Environment and Energy

Australian Antarctic Division

ICT Service Catalogue Process

DOCUMENT CONTROL

File [RM8] ref: Version: **1**	Responsible Officer: **ICT Service Desk Supervisor**	Authorising Officer: **ICT Manager**	Authorisation Date:
Location of Master Copy:			Review Date: **June 2017**
Location of Hard Copies/Points of Use:			
Business Classification: Unclassified			

VERSION HISTORY

Revision number	Year of Operation	Authorisation Date	Date of Next Review
1	2017-2018		

AMENDMENT HISTORY

Revision Number	Location of amendment (i.e. page #, para #, etc)	Addition / Deletion / Update	Description of amendment	Data amended	Author
1	n/a	Update	New document		XXXX
2	Multiple locations	Update	Changes to process necessitating changes to document		XXXX

Contents

Table of Figures

1. Introduction

The ServiceNow Service Catalogue is a self-service module that allows end-users to request consumables, equipment and services. The Service Catalogue has the capability to provide services across the entire Australian Antarctic Division (AAD) business. It has been set up to only provide IT services initially, with a future objective of servicing additional business needs.

The Service Catalogue is set up with definitions of each item available in the catalogue, and can include cost for cost-centre recovery. Tasks are defined for each item that allows the item to be provisioned in a regular manner which allows the requester to view its status. Items requiring manager approval can be routed to the relevant manager before being actioned by ICT and work commencing on provisioning the item.

1.1. Objectives

The purpose of this document is to define setting up and managing catalogue items so that an effective process can be achieved for service delivery to end users. This includes the following objectives:

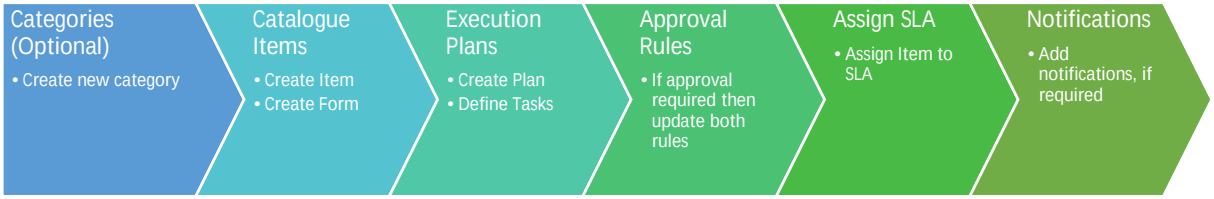
- Define the catalogue structure through categories of items
- Build catalogue items with specific fields for each separate item
- Define the task plan to provision each item
- Establish the appropriate approvals workflow for items needing manager approval
- Ensure users are kept informed through appropriate notifications
- Manage and measure service delivery through appropriate Service Level Agreements (SLAs) on provisioning.

1.2. Scope

The scope of this document is confined to the Service Catalogue application within ServiceNow.

2. Defining the Service Catalogue

There are a number of elements in ServiceNow used to set up the Service Catalogue. The sequence of steps is broadly as follows:

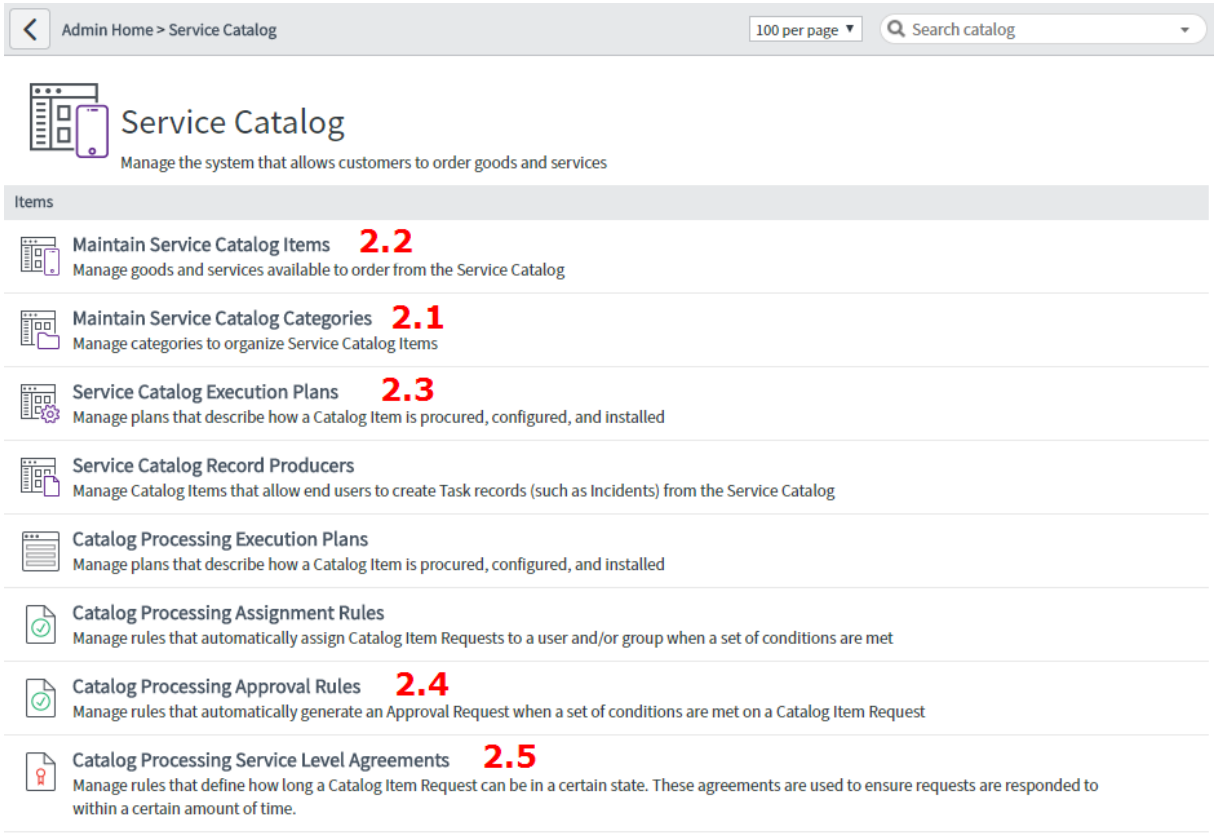


- Define the catalogue categories (section 2.1)
- Create the catalogue items with questions specific to each item, and define who is or is not allowed to request the items (section 2.2)
- Define execution plan tasks, and who each task will be assigned to (section 2.3)
- Define the approval rules (section 2.4)
- Assign a Service Level Agreement (SLA) to each item (section 2.5)
- Define notifications to be sent when items are requested (section 2.6)

Each of these elements is described in the following sections. All steps, except for notifications, can be accessed from:

Application Configuration > Service Catalog

The main Service Catalogue menu is shown below.



Notifications (2.6) is accessed from:

System Policy > Notifications

2.1. Categories

The Service Catalogue is organised by categories which may be established in a multi-level hierarchy.

AAD is using only one category level for the service catalogue as multi-levels do not work in the mobile view for Express ServiceNow.

The core content for each category is:

Field	Description
Title	The name of the category.
Parent	When using multi-levels, this indicates the hierarchy of the category.
Rendering Option	Is always Category Only
Homepage Image	This is the icon displayed against the category in the service catalogue. For consistency, all images used should be exactly 72 pixels wide and no more than 100 pixels high.
Description	A description of what the category contains which will be displayed in the service catalogue.
Available for	Use this tab to add restrictions on who is allowed to access the category, either for security reasons or because it is not relevant for groups of users.

Field	Description
	Restrictions can be based on groups, roles or users. Restricting to users should be avoided if possible; use a group instead even if there is only one member of the group. This can be used in conjunction with **Not Available for**.
Not Available for	Use this tab to add restrictions on who is not able to see the category. This would be used if the list of groups or roles to deny access is smaller than the groups or roles that are allowed access. This can be used in conjunction with **Available for**.

2.2. Catalogue Items

There are three relevant classes of items in the catalogue (other classes are used internally within the system):

- Catalogue Item
- Standard Change Definition
- Record Producer

Each of these are documented in the following sections.

2.2.1. Catalogue Item

Most of the items in the catalogue are this type. This is a standard request item that is then fulfilled primarily by the Service Desk, or another ICT support group.

Each item is defined with some basic information to define the catalogue item and its behaviour in the catalogue.

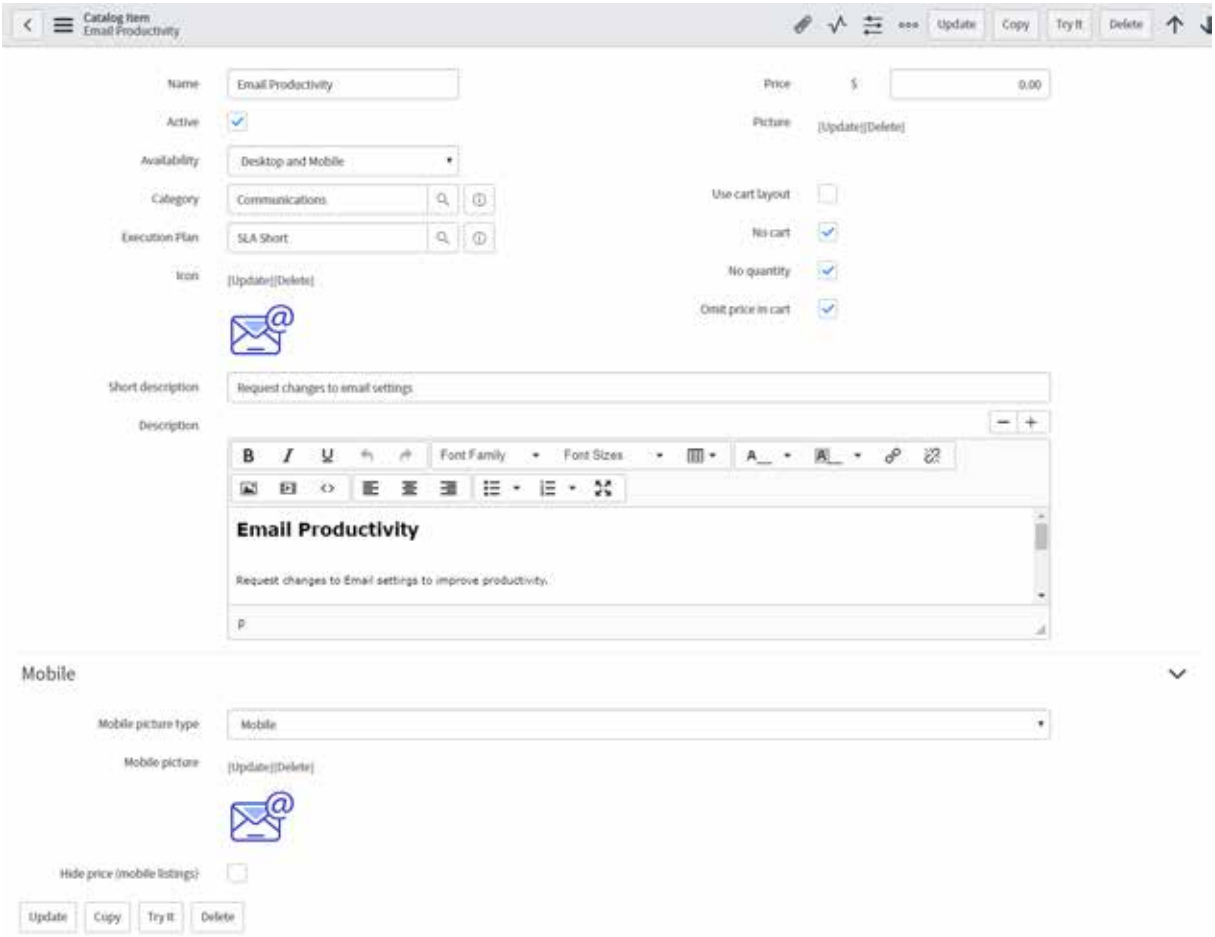


Figure 1: A catalogue item showing basic setup for all items entered into the catalogue

Field	Description
Name	The name of the catalogue item.
Active	If ticked, the item will appear on the service catalogue. When creating a new item, the Active check box will be on by default. This should be disabled while the item is being defined.
Availability	This determines if this item is viewable for selection on the desktop interface, the mobile interface, or both. **Desktop and Mobile** should be selected unless there is a reason not to show the item on one of the interfaces.
Category	This is the pre-defined category the item is grouped into.
Execution Plan	This controls the sequence of tasks that are required to fulfil this item. To enable measurement of fulfilling requests against an SLA, the execution plans are set up for each corresponding SLA. Select the appropriate execution plan from the list of available plans. Refer to section 2.3 for more information.
Short Description	A brief description of the item that shows in the catalogue.
Description	A full description of the item that shows on the catalogue if the user expands **More Information**; it also displays at the top of the page when the item is selected. The text in this field can be formatted using the tools available at the top of the field. Font sizes, colours and styles are available, tables, pictures, links

Field	Description
	and bulleted or numbered lists. The HTML source code can also be accessed directly from the **< >** icon. Each catalogue item must have the following: · A **title** which is the name of the item in bold, 14pt default font · A brief description of the item in default font
Icon	The icon is the image that appears in the catalogue list.
Picture	The picture is the image that appears on the item page when it is selected. All items in the catalogue must use the filler picture that appears as blank but allows the title and text to be indented (CatalogueBlankPicture.png).
Price	The cost of provisioning the item to the end user's cost centre. This is not currently being used but it may be in future.
Use cart layout	The service catalogue has a shopping cart concept similar to Amazon. This checkbox, when selected, allows a user to select multiple items into the shopping cart. As each item requires different activities and SLAs we want each item as a separate request, so this checkbox should be unselected and the following three checkboxes ticked, as follows: No cart No quantity Omit price in chart
Mobile picture type	The mobile interface has the option of using a separate picture. By default, this is set to **Desktop** which uses the same main picture. Select **Mobile** to change the picture.
Mobile picture	This field only appears if type (above) is set to **Mobile**. Add the required picture as needed.
Hide price (mobile listings)	Costs can be hidden from the mobile interface if this checkbox is selected. This is probably a security feature to limit confidential data (buying policies).

Once these details have been entered, the record must be saved to enable further fields on the form. Right-click on the form header and select **Save** (or **Insert and Stay** if the item is being created). A tabbed area will now show below the Mobile section.

2.2.1.1 Variables – Field Definitions

Figure 2: Variables tab showing a list of questions for the catalogue item

The **Variables** tab contains a list of the fields that are displayed when a user selects this item from the catalogue. The columns displayed here are controlled by the cog wheel in the top left. Whichever field is the first column in the row is the field that is the link to the details of the field. Click the **New** button to create a new field.

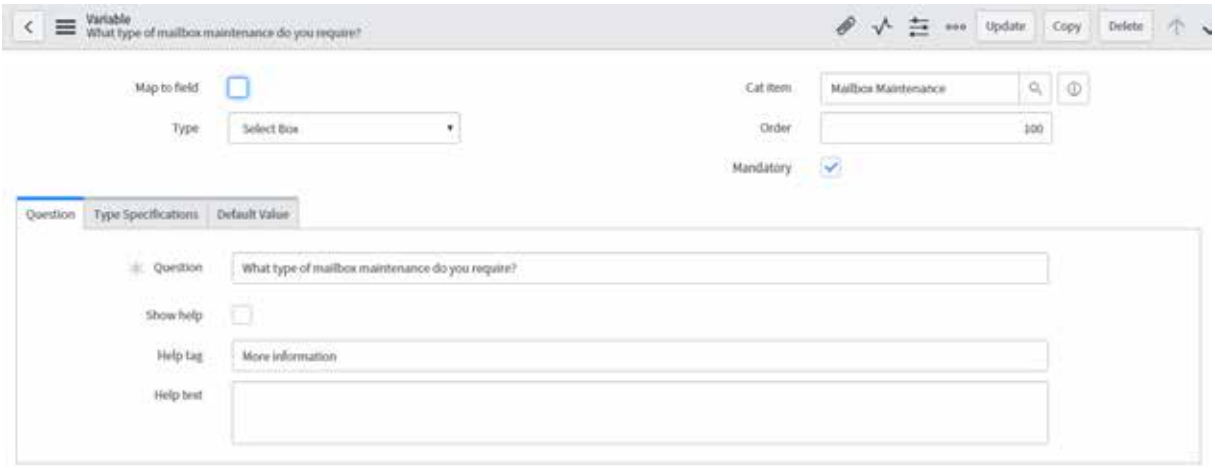


Figure 3: The Question tab when setting up a variable

Figure 4: The Type Specifications tab for a "Select Box" type variable

Figure 5: The Default Value tab for a variable

Field	Description
Map to field	This field is not used for standard catalogue items.
Type	This field determines the type of field that is to appear on the catalogue item form. The options are detailed in the **Field Types** table, below.
Order	The order is to determine the order of the fields on the form.
Mandatory	Select this checkbox if the user must enter a value in the field.
Question	This is the label for the field being defined
Show help	Select this checkbox if the field is to have help to assist the user.
Help tag	This is the label that appears below the field label (Question) that indicates there is further help available. The standard tag is "More Information".
Help text	Provide the information that will assist the user in filling in the required information in this field.

Field	Description
The Type Specifications tab contains variable questions depending on the field Type.	
Use dynamic default	Selecting this check box allows a default value to be used based on the user login (eg. their name).
Default value	Specify the **value** of the default option when using a multiple selection field type, if a default is required. If using a dynamic default, a system field must be used.

Field Types

Field	Description
Single Line Text	A short text field for limited text entry. There are no fields in Type Specifications for this field type.
Wide Single Line Text	A text field that displays at the width of the form. There are no fields in Type Specifications for this field type.
Multi Line Text	An unlimited text entry field. There are no fields in Type Specifications for this field type.
Date	The Date field allows dates to be entered using a calendar pop-up. There are no Type Specifications.
Date/Time	The Date/Time field allows dates to be entered using a calendar pop-up, with a time box to select the time also. There are no Type Specifications.
Reference	The Reference type allows you to specify the name of another table and select the value in one of the fields of that table. Conditions can be added for selecting specific records. The Type Specifications are: Reference: — The name of the table to look up a value Use reference qualifier: — This field is always **Simple** Reference qualifier condition: — Conditions can be added using fields from the reference table. Add conditions by clicking AND or OR, or delete conditions by clicking X.

Field	Description
Select Box	Select Box allows you to create a list of options to choose from in a drop-down field. Only one option can be selected by the user. When using this option for static values, once the question is saved, the options to be included can be added in the Question Choices section that displays at the bottom of the form. Each option must have: · Text – the option to be displayed · Value – a code value that is stored in the database for this text option. This is usually a number to represent the option. The Type Specifications are: Choice table: If required, the name of a table to use for non-static selection values Choice field: The relevant field from the table to use as values Include none: Select this checkbox to include a "none" value which forces the user to select one of the options provided Unique values only: If the table contains duplicates in the field being used, select this checkbox to remove the duplicates from the selection list
Multiple Choice	Multiple Choice provides a list of radio button options for a field where only one option can be selected. Once the question is saved, the options to choose from can be entered in the Question Choices section that then displays. Each option must have: · Text – the option to be displayed · Value – a code value that is stored in the database for this text option. This is usually a number to represent the option. The Type Specifications are: Choice direction: The options can go Across or Down. Include none: Select this checkbox to include a "none" value which forces the user to select one of the options provided
Numeric Scale	A Numeric Scale is a range of numbers presented as radio buttons. The range of the numbers to be used is specified in Type Specifications.
CheckBox	The CheckBox option is a single question requiring a yes/no or true/false answer. Where a series of check box questions is to be used to allow for multiple selections, they should be within a container.
Container Start	A Container Start indicates that the fields following are to be grouped together; for example, a series of check boxes that allow for multiple selections. Container Start has an option to "Display title" which then displays a line and the question entered as the title of the container. The Type Specifications for this field allow the container to be organised as one or two columns. If two columns are used, each set of options needs to be within a separate sub-container.
Container End	Container End indicates the end of a grouping. It has no further fields other than the order. There is no line displayed for container end.
Label	This option allows you to specify a label on the form with no other options other than the order it is to appear in.

Field	Description
Break	Break includes a line within the order specified but has no other fields. If a container has included a title question, as it also then includes a line, a break should be entered next to a container end to indicate the end of the container.

2.2.2. Standard Change Definition

There are two ways standard changes can be defined in the service catalogue. The first is by defining a standard change in the Change module, and the other is by defining a record producer in the catalogue to generate a standard change. Both types are added to the Service Catalogue by default, so the ones created in the Change module must be modified to restrict access so they cannot be requested by end users.

2.2.2.1 Standard Change

Standard changes are changes that are made regularly which have a well-defined process and are low risk to implement. Standard changes are requested and actioned by ICT for common tasks through the change module. However, because ServiceNow automatically places standard changes into the service catalogue, these changes must be restricted to ICT when they are created.

Restricting Standard Changes

1. Access the standard change definition either from the change module or the service catalogue.
2. Click on the **Available For** tab at the bottom of the definition.

Figure 6: The Available For tab

3. Click on the **Edit** button, then select **ITIL Users** in the left list and **Add** it to the right.

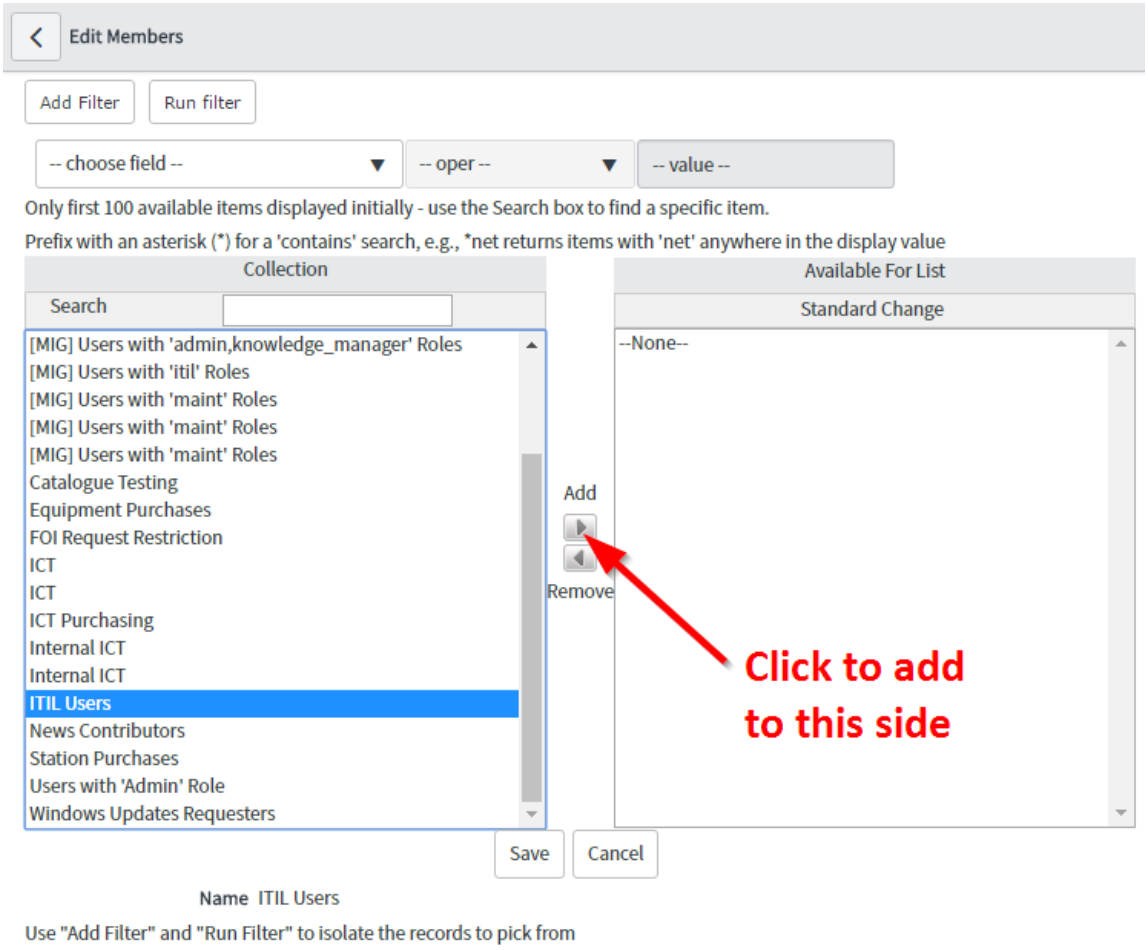


Figure 7: Adding roles to a catalogue item

4. Click on **Save**.

2.2.2.2 Record Producer Standard Change

Record producer standard changes are effectively catalogue items that end users can request, but they are items that need to go through a change control process to be provisioned. Rather than having a standard catalogue item for this where ICT would then have to raise an RFC, using the record producer bypasses the need for the additional work. An example of a standard change end users can request is **Firewall Changes**. This is a standardised process with low risk so it can be requested via the service catalogue.

Create a catalogue standard change using the record producer process as outlined in section 2.2.3 below, using **Change Request** for the table name and **Standard Change** in the execution plan.

2.2.3. Record Producer

Creating a catalogue item using a record producer is very similar to creating a catalogue item directly, but there are some differences on the form used. However, when using a record producer in the catalogue, there also needs to be a template that defines how all data values are mapped to the destination record. Variables used in record producers generally cannot be mapped without creating

corresponding fields in the destination, but short description and description should be used and mapped whenever possible to provide relevant information in the resulting record.

2.2.3.1 Create a Record Producer

Access **Service Catalogue Record Producers** from the Service Catalogue main menu under **Application Configuration**.

The fields required when creating a new record producer are as follows.

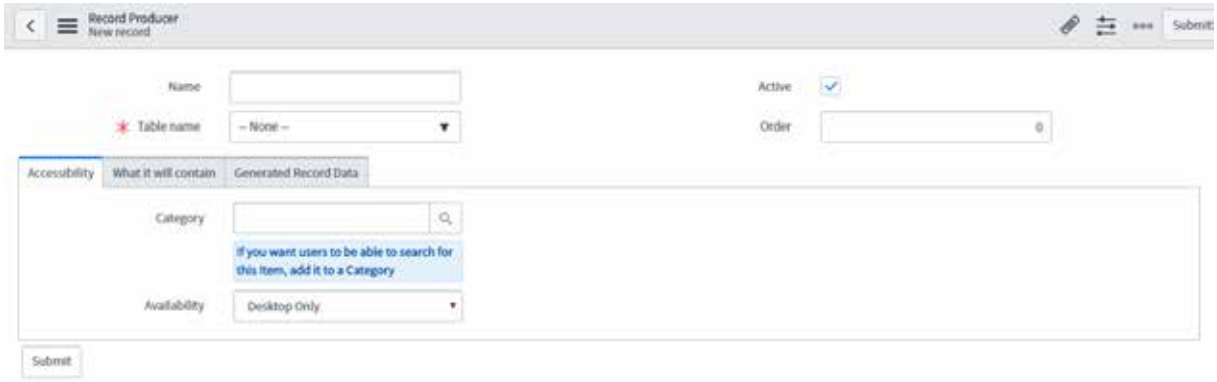


Figure 8: Record Producer and Accessibility tab

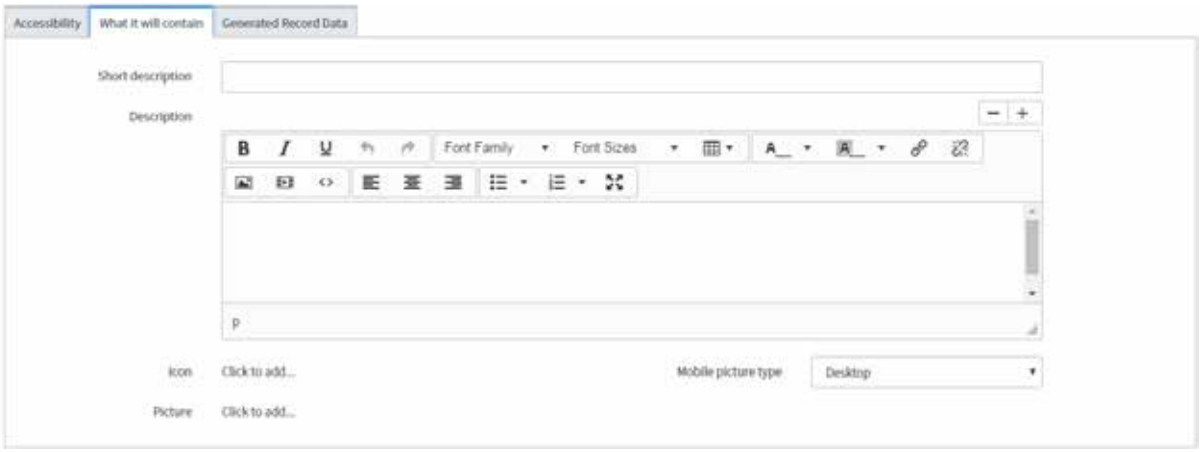


Figure 9: Record Producer What it will contain tab

Figure 10: Record Producer Generated Record Data tab

Field	Description
Name	The name of the catalogue item.
Active	If ticked, the item will appear on the service catalogue. When creating a new item, the Active check box will be on by default. This should be disabled while the item is being defined.

Field	Description
Table name	This is the name of the table the record producer is creating a record for. Typically, this will be **Incident**, **Change Request** or **Requested Item**, however, record producers will also be used when generating records for separate tables used by non-ICT groups.
Order	The order the record producers are listed.
Category	This is the pre-defined category the item is grouped into.
Availability	This determines if this item is viewable for selection on the desktop interface, the mobile interface, or both. **Desktop and Mobile** should be selected unless there is a reason not to show the item on one of the interfaces.
Short Description	A brief description of the item that shows on the catalogue.
Description	A full description of the item that shows on the catalogue if the user expands **More Information**. Once in the item, this will also display at the top of the page. The text in this field can be formatted using the tools available at the top of the field. Font sizes, colours and styles are available, tables, pictures, links and bulleted or numbered lists. The HTML source code can also be accessed directly from the **< >** icon. The standards used for displaying normal catalogue items should also be used here.
Icon	The icon is the image that appears in the catalogue list.
Picture	The picture is the image that appears on the item page when it is selected. As with normal catalogue items, use the blank space default picture to space the title and text away from the navigator panel.
Mobile picture type	The mobile interface has the option of using a separate picture. By default, this is set to **Desktop** which uses the same main picture. Select **Mobile** to change the picture.
Mobile picture	This field only appears if type (above) is set to **Mobile**. Add the required picture as needed.
Template	Create a new template for this record producer using the same name as the name of the item. Refer to section 2.2.3.3 below.
Execution Plan	If the record producer is generating a standard change, the Execution Plan must be set to **Standard Change**. For all other record producers, a new execution plan should be created as for a normal catalogue item. Further information about execution plans is detailed in section 2.3 below.

2.2.3.2 Create Variables

Variables are created for record producers in the same way they are created for normal catalogue items (see section 2.2.1.1). However, with record producer variables, the short description and description fields should be mapped to the destination record to enable capture of identifying information. This requires setting up fields for these values in the record producer. When defining the variables, use the **Map to field** option, as outlined below.

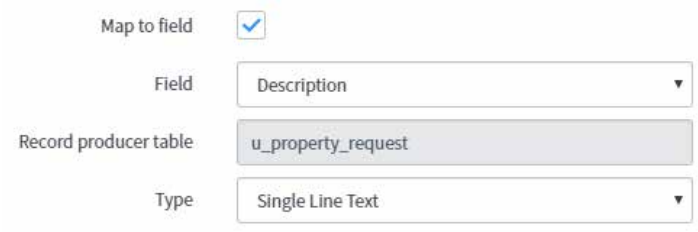


Figure 11: Mapping fields

Field	Description
Map to field	Select the checkbox for short description and description. This option can also be used for any other field on the record producer that maps to a specific field in the target table.
Field	The name of the field on the target table.
Record producer table	The name of the target table. This will have been defined at the record producer definition level.

2.2.3.3 Create a Template

Templates are used to pre-populate fields in a record. They are also required when using a record producer as a number of fields on the target table need to be defined with common defaults.

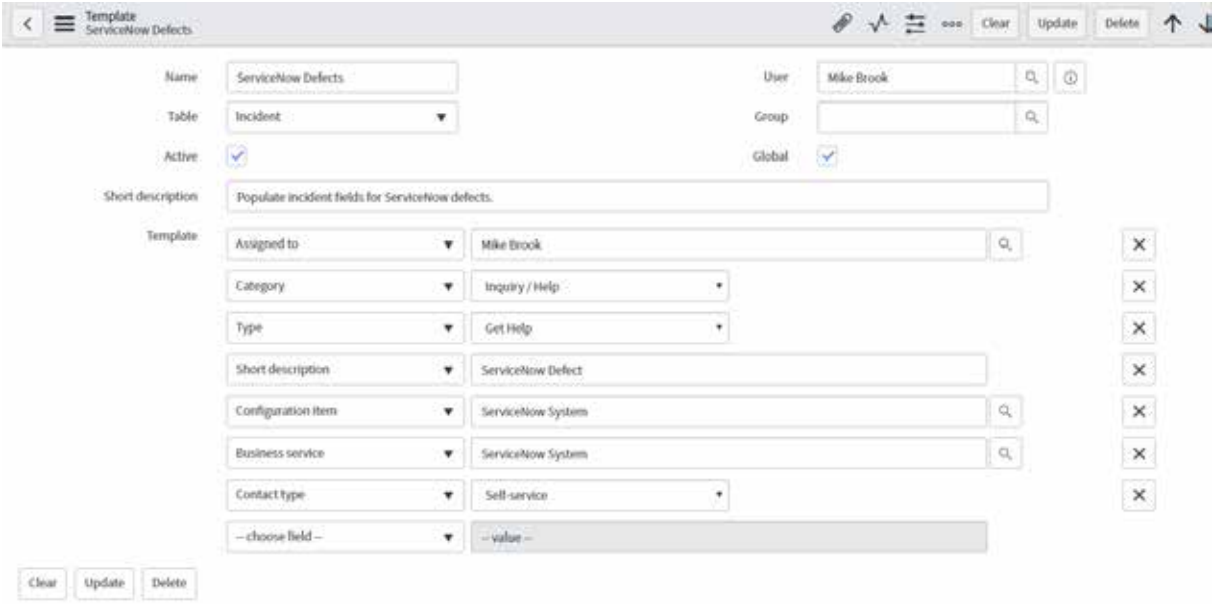


Figure 12: Setting up a Template

Field	Description
Name	The name of the template which should be the same as the name of the catalogue item.
Table	The table the catalogue item is mapping to.
User	Templates can be set up for individual users. For service catalogue record producer templates this should be left blank.

Field	Description
Group	Templates can be set up for groups. For service catalogue record producer templates this should be left blank.
Global	This check box should be selected so that it will activate whenever anyone selects the catalogue item, to generate the required record with the nominated mappings.
Short Description	Brief description of the template.
Template	This requires selecting the field from the destination table and specifying the value that is to be used in that field. As many fields as needed can be added.

2.3. Execution Plans & Assignments

Execution plans are a list of tasks or steps required to fulfil a requested item from the service catalogue. They can also be used for incidents or to implement a change. For the service catalogue these steps may constitute progression toward fulfilment which is displayed to the end user showing discrete parcels of work that clearly indicate how a request is progressing. However, because of limitations with ServiceNow Express, execution plans for catalogue items have been linked to SLAs and there is one task within each execution plan for each relevant SLA required (see also section 2.6). Separate execution plans with required tasks can still be set up for record producer standard changes.

The execution plans have already been defined corresponding to each SLA. An example is shown below.

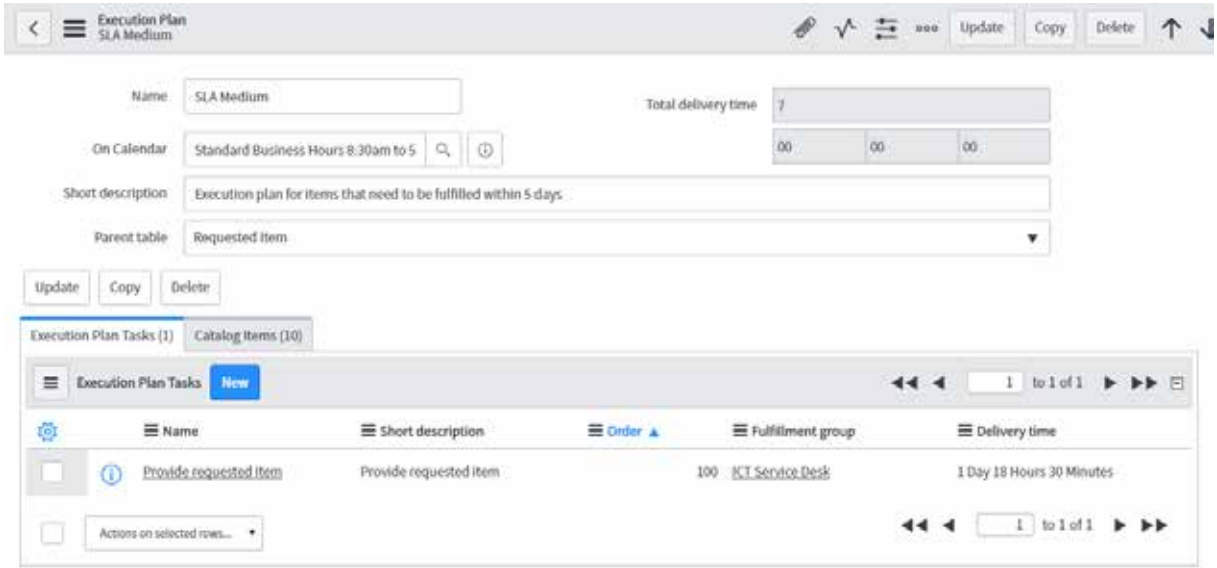


Figure 13: Execution Plan with Tasks

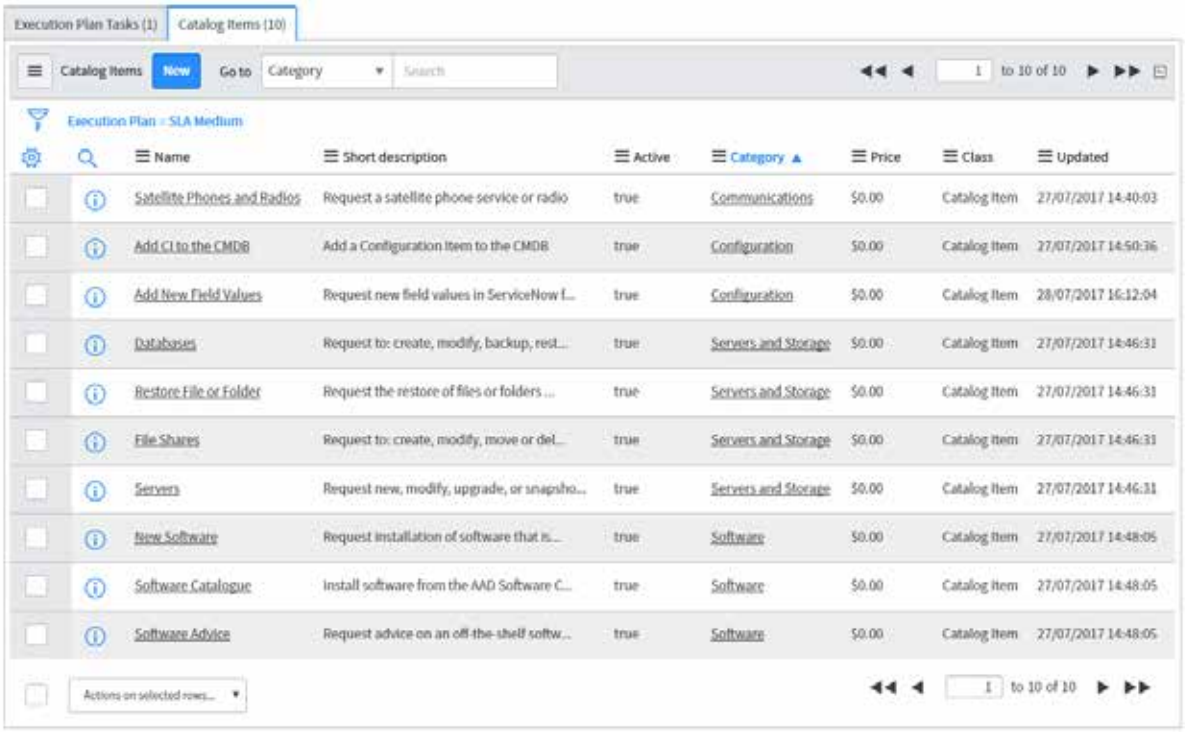


Figure 14: Execution Plan Catalogue Items

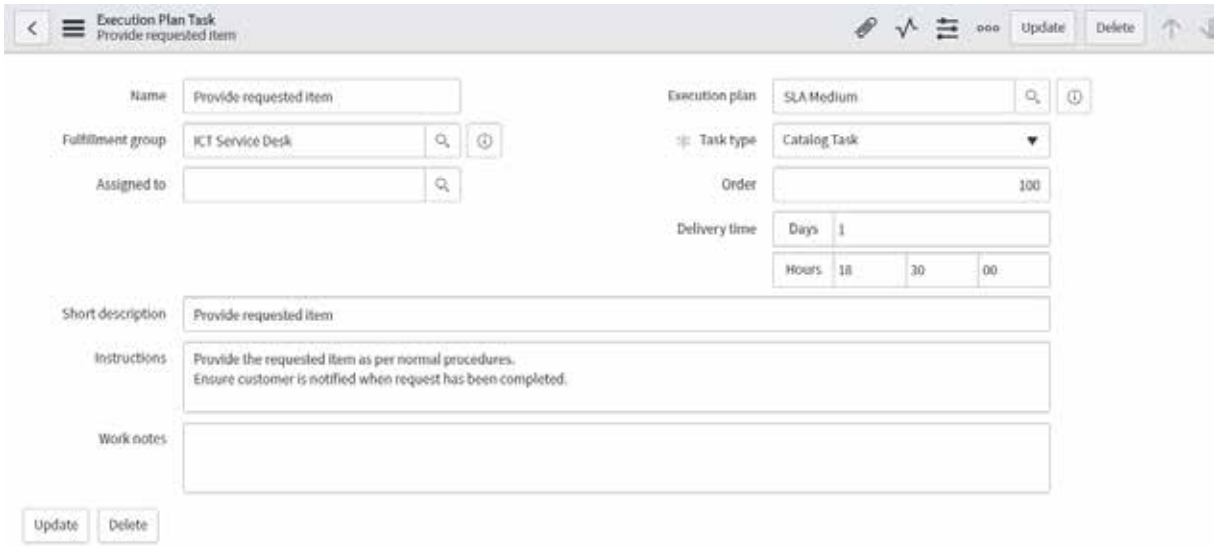


Figure 15: An Execution Plan Task

Field	Description
Name	The name of the execution plan which represents the SLA (or record producer standard changes).
On Calendar	All execution plans should use the standard business hours calendar.
Short description	A short description of the execution plan, including the target SLA time.
Parent table	If the execution plan was created from the service catalogue this will have been filled in, otherwise it should be **Requested Item** for catalogue items. Incidents or Change Request can also be selected.

Field	Description
Total delivery time	This is a display only field that sums the times specified in each task to give total delivery time for the request. The total delivery time includes weekends – so it is **actual** days, not business days.
Execution Plan Tasks	On the Execution Plan Tasks tab, click on New to create new tasks.
Name	This is the name of the task.
Fulfilment Group	Select the group that will perform this task. This will need to be the **ICT Service Desk** who will reassign items to the relevant group once they are received.
Assigned to	This is to assign individuals to a task but this should be left blank so that only the group is assigned initially.
Execution plan	This is the execution plan the task belongs to.
Task type	This should be filled in automatically depending on the table the execution plan was created for.
Order	This specifies the order the tasks are to be completed. When there are multiple tasks they can be undertaken simultaneously in which case they should have the same number; consecutive tasks should have sequential numbers.
Delivery time	This is where the amount of time it will take to perform this task in days, hours, minutes and seconds is entered. The time entered here is based on a 24 x 7 basis regardless of what calendar is used at the execution plan level. Therefore, times need to be converted appropriately. For example, if a task is to take 5 business days, then multiply a standard business day of 8.5 hours (based on the calendar used) by 5 (business days) to give a total of 42.5 hours. This is then represented on a 24 hour basis as 1 day, 18 hours and 30 minutes at the task level. The resulting total time at the execution plan level is 7 days, including a weekend. All execution plan times are shown in the next table.
Short description	A short description of what the task entails.
Instructions	Specify the detailed instructions for performing this task.
Work notes	Specify any additional information that might be relevant to performing the task, such as tips and tricks.
Catalogue Items	This tab lists any catalogue items that use this execution plan.

	SLA			Task Time		
Execution Plan	**Business Days**	**Actual Days**	**SLA in Hrs**	**Days**	**Hours**	**Mins**
SLA Urgent	1hr	1	1		1	0
SLA Short	3d	5d	25.5	1	1	30
SLA Medium	5d	7d	42.5	1	18	30
SLA Long	20d	28d	170	7	2	0
SLA Non Standard	40d	56d	340	14	4	0

Figure 16: Execution Plan Task Times

2.3.1. Default Assignments

Support group assignment only normally happens through definition of execution plan tasks as there could be different groups handling different tasks. To ensure no requests are unassigned two default assignments have been created as follows:

- **Catalogue Default Assignment Requests** – any new service catalogue request created is assigned to **ICT Service Desk**. This includes any items with a class of Catalogue Item.
- **Catalogue Default Assignment ReqItems** – any new request items that are generated from record producers are assigned to **ICT Service Desk**. This covers the scenario where a request that needs approval is generated directly as a request item, bypassing the request table.

2.4. Approvals

By default, all catalogue items created require approval. Therefore, approval rules must be set up to ensure an item is handled appropriately, either by notifying an appropriate manager to approve the item, or setting an auto-approval rule for items that don't require approval.

There are two approval rules set up for AAD: one for items that are auto-approved and one for items requiring approval. If a new item is set up that doesn't need approval, the rules will automatically cover this. However, if the item requires approval, both rules must be modified to add in the item. In addition to this, the definition of catalogue items that need approval must include a user-selected approval field, and there is then a manual process that must be followed by the Service Desk to ensure these items are forwarded to the appropriate manager.

2.4.1. Approval Rules

Each approval rule requires the same basic information. The only differences will be the conditions for each rule and whether approvers are specified or if the item is auto-approved.

Field	Description
Name	The name of approval rule. As all approval rules are in a single table, each rule should be prefixed by the module it applies to (Catalogue, Incident, etc.).
Table	For the service catalogue this will be Requested Item.
Conditions	Catalogue items requiring approval have conditions of: Item **is** <Name of the catalogue item> OR Item **is** <Name of the catalogue item> Catalogue items **not** requiring approval have conditions of: Item **is not** <Name of the catalogue item> AND Item **is not** <Name of the catalogue item>
Generated Approval Data	On the Generated Approval Data tab, select the Auto-approve check box or define the approver parameters.

The first rule for items requiring approval is **Catalogue Approvals by Manager**. This rule lists each Item that requires an approval, as follows:

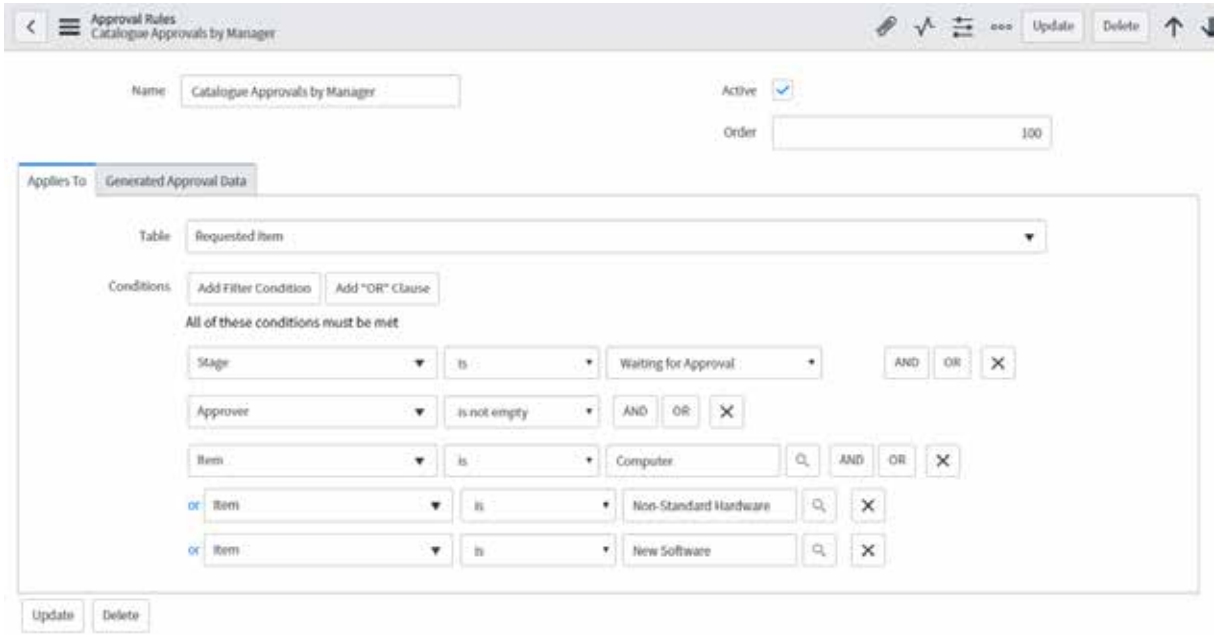


Figure 17: Setting up approvals by manager – conditions

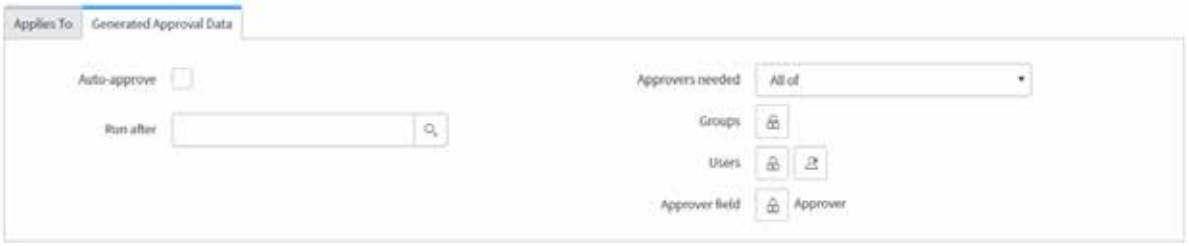


Figure 18: Setting up approvals by manager – assignment

The **Catalogue AutoApprovals** rule lists the same Items as the other rule, but this time selecting Items **other than** these Items to auto-approve.

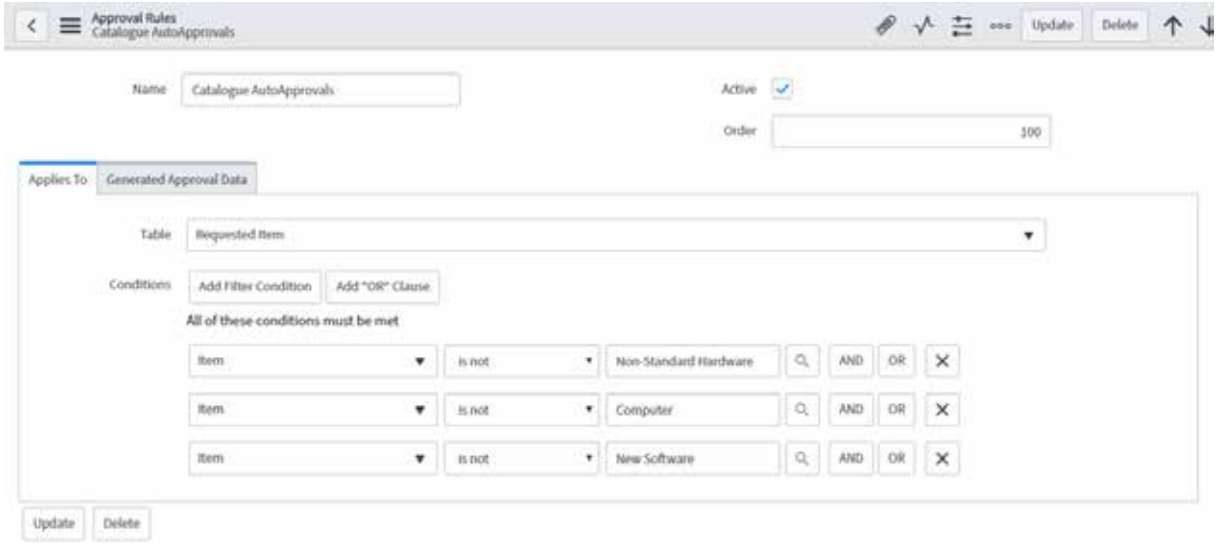


Figure 19: Setting up auto-approvals – conditions

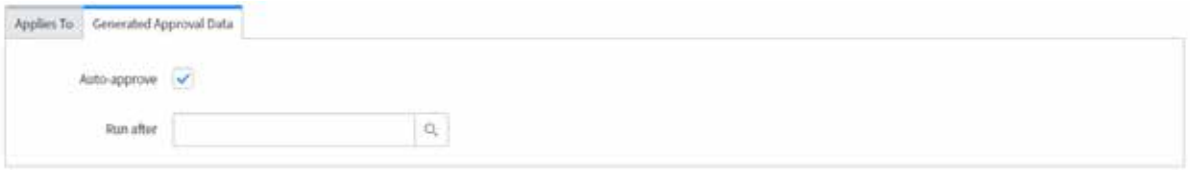


Figure 20: Setting up auto-approvals – assignment

2.4.2. Set Up Catalogue Items Needing Approval

To ensure the correct manager is assigned to items requiring approval, the definition of the items in the catalogue needs to include an approver field that the user nominates. This field must be set up as follows:

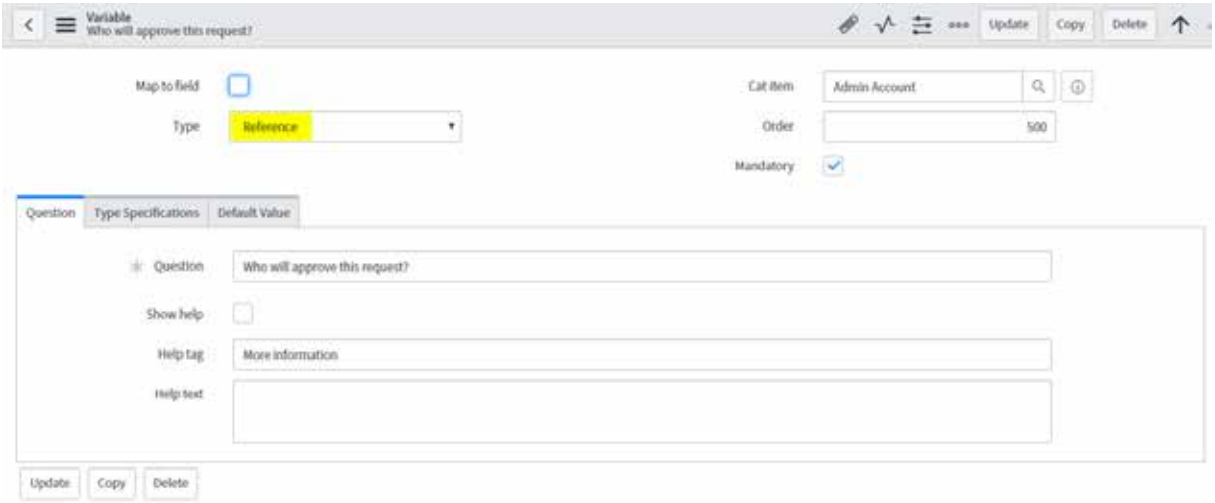


Figure 21: Setting up a Variable for selecting an Approver

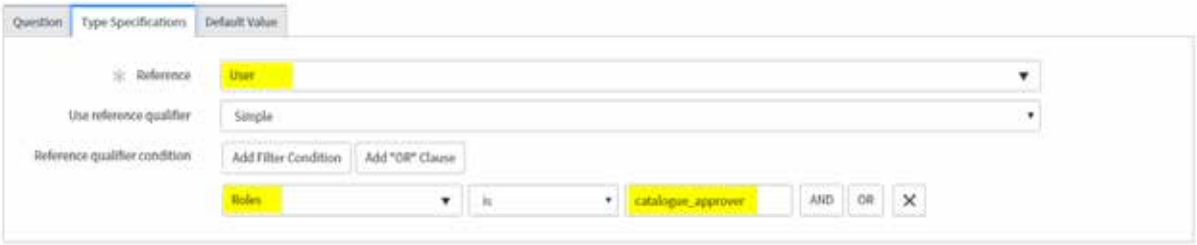


Figure 22: Approver variable reference lookup

- Create a variable with a question of "**Who will approve this request?**" or similar
- Set the variable type to **Reference**
- Set the variable to **Mandatory**
- On the Type Specifications tab, select the **User** table in the Reference field
- Select **Roles** in the filter condition
- Set the operator to "**is**"
- Enter the approval role of "**catalogue_approver**" (enter exactly, as this value cannot be looked up)
- **Update** the variable to save it.

2.4.3. Process Items Needing Approval

When a user selects an item from the catalogue that requires approval, they will need to specify who the approval manager will be. Only the users who have been assigned to the role of an approver will be displayed in the list the user can select from.

Once the user submits the request the item will be initially assigned to the Service Desk. Service Desk staff must open the item and fill in the **Approver** field based on the name the user selected.

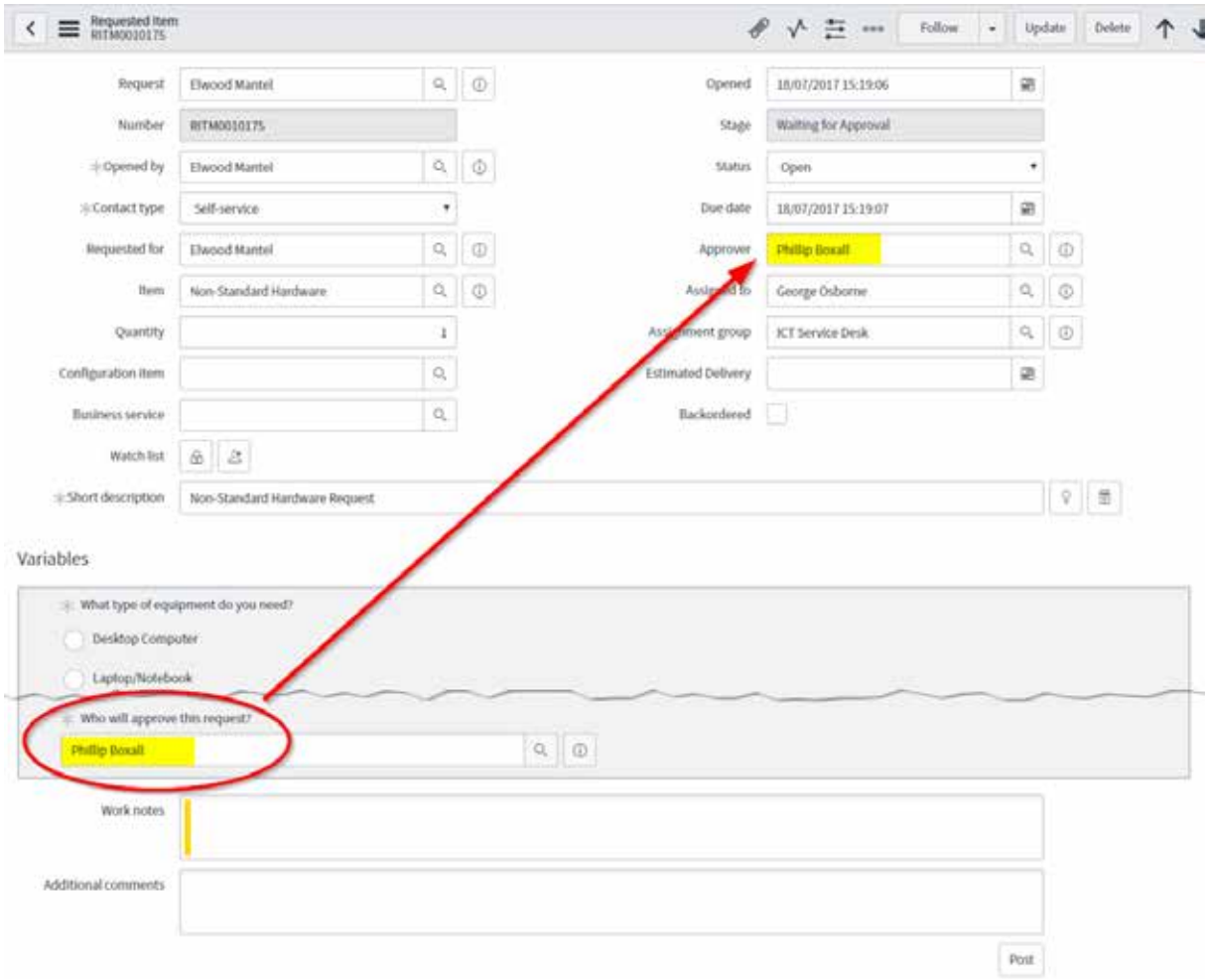


Figure 23: Mapping the approver for routing

Once updated, the requested item will be forwarded to the selected manager to approve or deny.

2.5. Service Level Agreements

Delivery of service catalogue items is being measured by SLAs. Service levels work in ServiceNow by cumulative times across a number of escalation points. There are three escalation points of low, medium and high, and a target escalation point when it becomes overdue having reached the total amount of time allowed. For the service catalogue, only one escalation point is being used at approximately the 75 percent point of the target time.

The service levels have been set as follows using these two escalation points:

SLA Name	Target	Escalation	Overdue
Urgent Request	1 hour	30 min	30 min
Standard Short	3 days	2 days	1 day
Standard Medium	5 days	4 days	1 day
Standard Long	20 days	15 days	5 days
Non-Standard	40 days	30 days	10 days

The service levels should be monitored and adjusted to ensure catalogue items are being managed appropriately. Each service level contains a list of the categories it applies to.

For the service catalogue, SLAs only work at the task level. These have been set by equating an execution plan task with the relevant SLA. When a request is made from the catalogue, the tasks in an execution plan are created as request tasks, so by having only one task per execution plan, the SLAs can be set as needed.

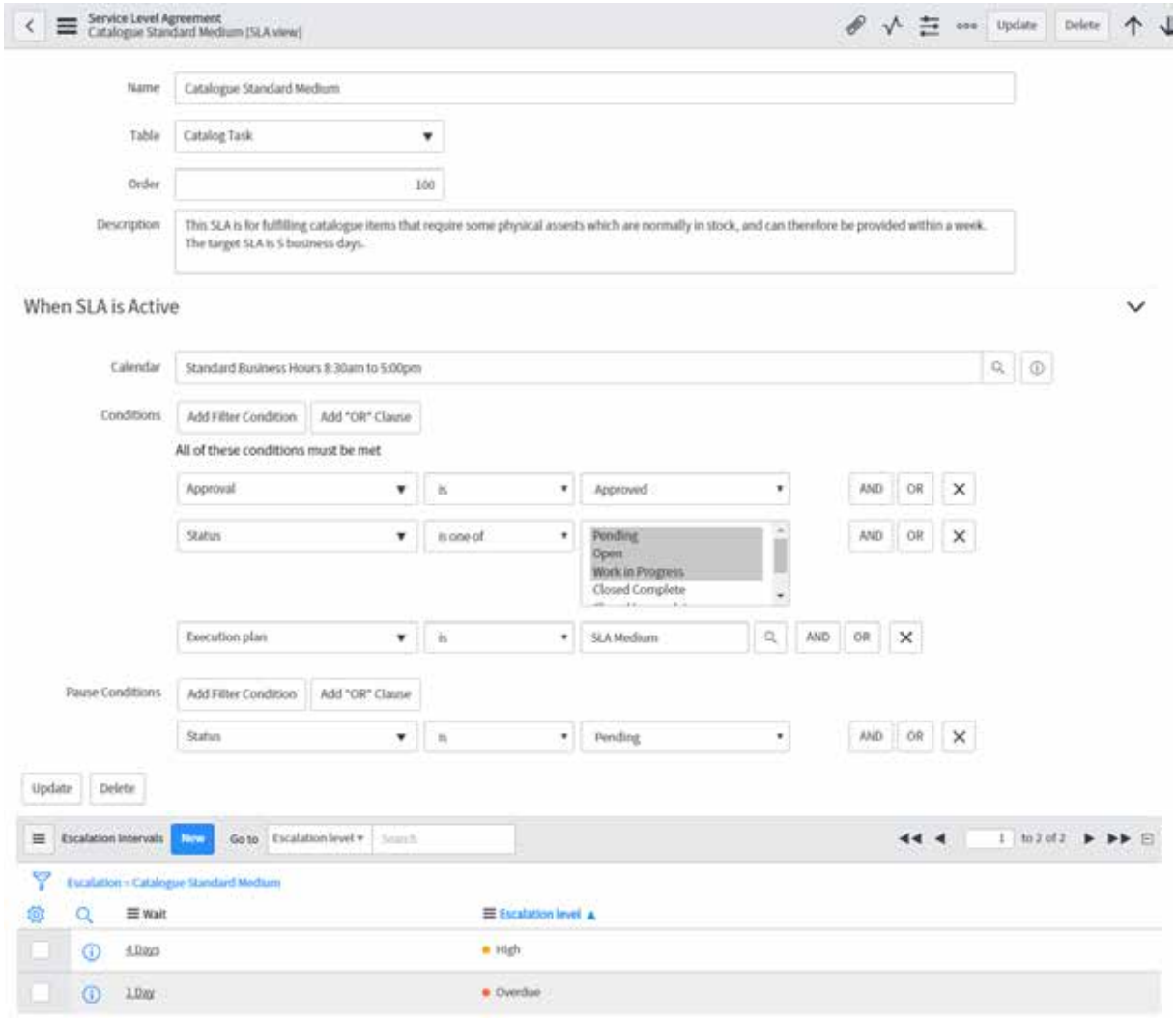


Figure 24: Setting up a Service Level Agreement

Figure 25: SLA escalation intervals

Field	Description
Name	The name of the SLA.
Table	For the service catalogue this should be **Catalog Task**.
Order	SLAs can be set to run concurrently or sequentially depending on the order specified. Currently, the order is not important.
Description	Enter a description of what the SLA is intended to measure, including the SLA target.
Calendar	Most SLAs will only measure across business hours so the Standard Business Hours calendar should be specified. Leave blank if the SLA operates on a 24x7 basis.
Conditions	The conditions under which the SLA operates need to include all states from start to finish, including any pause conditions For the service catalogue the standard conditions will be the SLA only starts once an item is approved and when requested items have the corresponding execution plan to the current SLA. Approval is Approved AND Status is one of Pending, Open, Work in Progress AND Exec Plan is SLA <name>
Pause Conditions	This is when the SLA stops measuring under certain conditions, such as waiting on customer feedback. Requested items should be set to Pending status to ensure the clock stops. Status is Pending
Escalation level	Select the escalation point you want to reference. For service catalogue items this will normally be the High and Overdue levels.
Wait	Enter the time to wait before the escalation triggers in days, hours, minutes and seconds. The amount of time for each escalation is cumulative. For example, if the SLA target is 4 days with one escalation point at approximately 75% of the target time, the following escalation points would be entered: High 3 days (0 h:m:s) *wait three days before escalating* Overdue 1 day *wait another day before breaching*

2.6. Notifications

Notifications for the approval or rejection of requests are defined in the ServiceNow core system. Notifications for requests created, assigned and completed are outlined in the Communications section (5.1).

3. Request Processing

3.1. Process Workflow

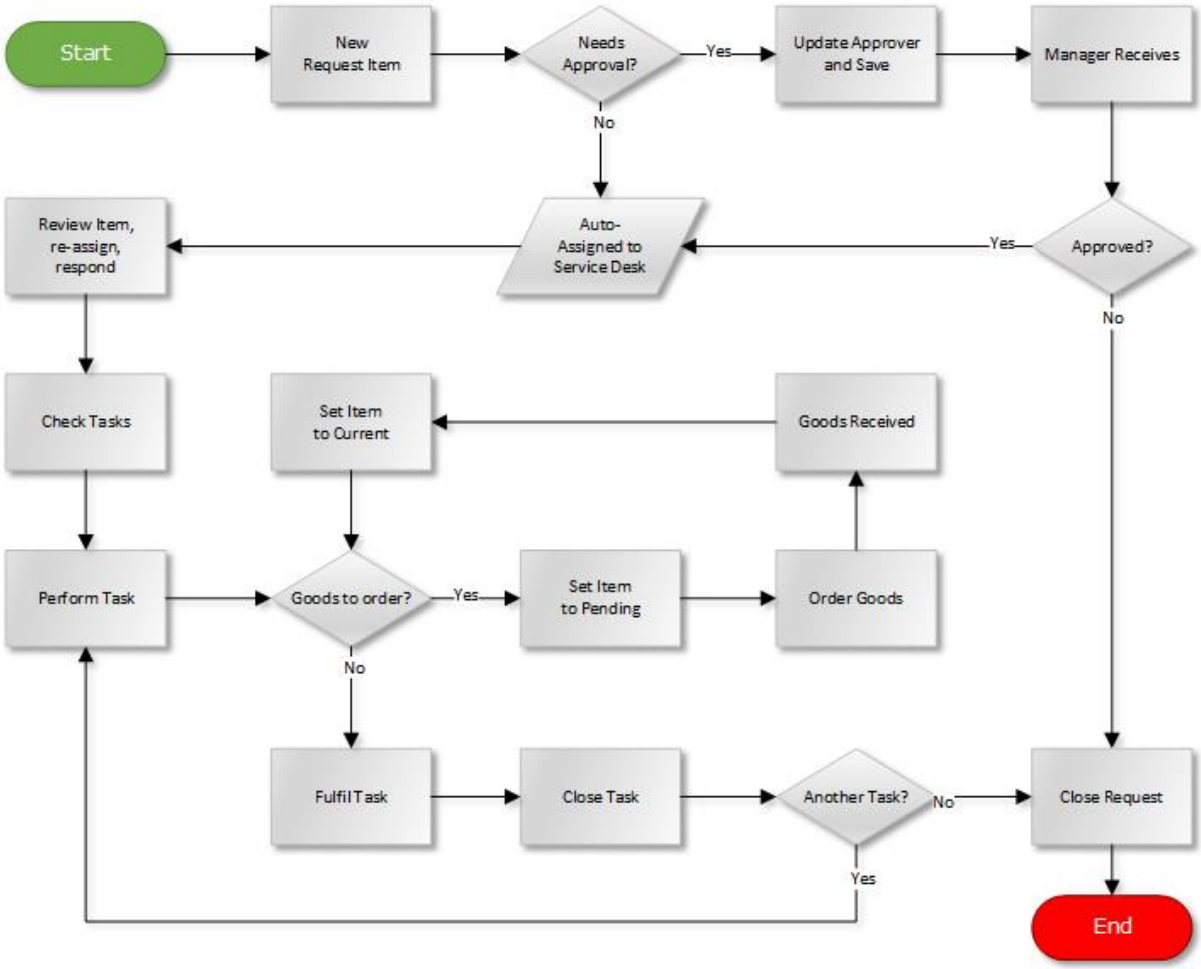


Figure 26: Service Catalogue Request Processing

3.2. Fulfilling Requests

End users generate requests when they select an item from the service catalogue, fill in the details on the relevant form and then click "order". The process to fulfil the requests is then as follows.

1. The Service Desk checks for any items requiring approval. If the item **Approval** is *Not Yet Requested*, the item needs to be pushed to the approval stage. This is where the **Approve** field needs to be populated with the name of the approver the requester has nominated in the Variables section (see section 2.4.3, Figure 23).
2. All items, whether auto-approved, or once they have been approved by the manager, are reviewed by the Service Desk to ensure there is sufficient information to provide the request. If not, follow up with the requester.
3. If the request needs to be assigned to another support group, change the Assignment Group in the requested item and the task.

4. If goods need to be ordered, the request should be put into Pending Status, while they are purchased and delivered. The Status should be reset once the goods are received.
5. Perform the work required to fulfil the request.
6. Add fulfilment details in the Additional Comments field and ensure the user is notified that the request has been fulfilled.
7. When completing a task, make sure the parent item is also completed.

4. Roles and Responsibilities

4.1. Service Catalogue Manager Responsibilities

It is the responsibility for the owner of the service catalogue to manage the catalogue for applicability and usability, and to provide meaningful metrics on its use. This includes:

- Setting up and maintaining catalogue categories to meet user needs.
- Establishing catalogue items with relevant variables to capture sufficient information to enable support groups to fulfil requests.
- Defining suitable execution plans in conjunction with support teams that provide enough information on progress of requests to end users.
- Setting up necessary approval rules to minimise manual handling for approvals.
- Defining notifications to keeps users and support groups informed of key stages of request fulfilment.
- Assigning appropriate service levels to requests such that they are fulfilled in a timely manner.
- Establishing security on categories and items where necessary to limit unnecessary access.
- Monitoring usage of the catalogue to ensure ongoing relevance of categories and items.
- Writing knowledge articles to assist end users finding and using the correct items.
- Writing knowledge articles to assist support groups fulfilling requests.
- Performing analysis of requests and providing metrics to management.

4.2. Service Desk Responsibilities

It is the responsibility of the Service Desk to fulfil requests made by users in the Service Catalogue. This includes:

- Monitoring requests that are made on a regular basis to ensure they are assigned and actioned within the relevant SLA.
- Ensuring items requiring manager approval are pushed through to the relevant manager quickly.
- Managing the fulfilment of requests in a timely manner.
- Reassigning requests to 2nd and 3rd level support groups where appropriate in a timely manner.
- Keeping users informed of progress.

- Contributing to refinement of the Service Catalogue with suggestions for additions and improvements.
- Writing knowledge articles to assist other Service Desk team members and other support groups in fulfilling requests.

5. Communications

Automatic email notifications can be generated in ServiceNow for targeted events, such as notifying a support group when a request has been created. Notifications are intended to keep all parties informed regarding activity on a request.

5.1. Notifications

The following table outlines the content of the automated notifications from ServiceNow. Each notification uses the AAD default format which includes a header and footer.

Name, Table & Conditions	To	Content
Request Opened on Behalf *Requested Item* New request	Creator & Requested for	Thank you for contacting the Australian Antarctic Division ICT Service Desk. We have received your request and will respond as soon as possible. To view your request click here: **${URI_REF}**. **Number:** ${URI_REF} **Short description:** ${short_description}
Approval Request *Approval* New request requiring approval	Creator & Approving Manager	**${URI_REF}** is awaiting approval. **Requested by:** ${sysapproval.opened_by.name} **Short description:** ${sysapproval.short_description} **Priority:** ${sysapproval.priority} **Category:** ${sysapproval.category} **Comments:** ${sysapproval.description} **Edit Request:** ${sysapproval.URI} **View & Comment Request:** ${URI} ${mailto:mailto.approval} ${mailto:mailto.rejection}
Request Approved *Requested Item* Approval is Approved and Approver is not empty	Creator & Requester	Dear ${request.requested_for.first_name}, Your request **${URI_REF}** has been approved and has progressed to the next stage. **Request Number:** ${URI_REF} **Short Description:** ${short_description}

Name, Table & Conditions	To	Content
Request Item Commented *Requested Item* Additional comments in Item are updated	Requester, Assignment group, Assigned to, Watch list	Dear ${request.requested_for.first_name}, Your request **${URI_REF}** has been updated. **Request Number:** ${URI_REF} **Item:** ${cat_item} **Short Description:** ${short_description} **Comments:** ${comments}
Request Task Commented to User *Catalogue Task* Additional comments in Task are updated	Requester, Assignment group, Assigned to, Watch list	Dear ${request.requested_for.first_name}, Your request has been updated. **Request Number:** ${request_item.number} **Item:** ${request_item.cat_item} **Short Description:** ${request_item.short_description} **Comments:** ${comments}
Request Completed *Requested Item* Active is false	Creator & Requester	Dear ${request.requested_for.first_name}, Your request **${URI_REF}** has been completed. Request Number: **${URI_REF}** Short Description: **${short_description}** Click me if you are happy! Click me if you are not happy

6. Reporting

The following reports will be available regarding the service catalogue and requests:

Description	Contents
Service Catalogue List	A list of items currently available in the service catalogue
List of Open requests	List of requests that are currently open
List of Pending requests	List of requests that are currently in a pending status
Approvals not yet requested	List of any requests where the approval has not yet been requested which need to be process by the Service Desk
Requests awaiting Approval	List of requests that are waiting for approval
Request SLAs	Aggregate of requests by SLA escalation points
Request Counts by Category	Aggregate of requests by category
Request Counts by Item	Aggregate of requests by item

Australian Government

Department of the Environment and Energy

Australian Antarctic Division

ICT Service Level Agreement

File [RM8] ref:	Responsible Officer: **ICT Change Manager**	Authorising Officer: **ICT Manager**	Authorisation Date:
Version: **1**			
Location of Master Copy:			Review Date: **October 2017**
Location of Hard Copies/Points of Use:			
Business Classification: **Unclassified**			

VERSION HISTORY

Revision number	Year of Operation	Authorisation Date	Date of Next Review
1	2017-2018		

AMENDMENT HISTORY

Revision Number	Location of amendment (i.e. page #, para #, etc)	Addition / Deletion / Update	Description of amendment	Data amended	Author
1	n/a	Update	New document		M Brook

Contents

Agreement Overview

This Agreement represents a Service Level Agreement ("SLA" or "Agreement") between the Information and Communication Technology (ICT) section and the Australian Antarctic Division for the provisioning of ICT Services required to support and sustain operations at Antarctic and sub-Antarctic stations and the Australian Antarctic Division in Kingston, Tasmania.

This Agreement remains valid until superseded by a revised agreement mutually endorsed by the stakeholders.

This Agreement outlines the parameters of all services covered as they are mutually understood by the stakeholders. This Agreement does not supersede current processes and procedures unless explicitly stated herein.

Objective & Goals

The objective of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent delivery of support services to the Australian Antarctic Division by ICT.

The goals of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to the end user.
- Match perceptions of expected service provision with actual service support & delivery.

Stakeholders

The following Service Provider(s) and End User(s) will be used as the basis of the Agreement and represent the stakeholders associated with this SLA:

Service Provider(s): ICT ("Provider")
End User(s): the Australian Antarctic Division ("Customer")

Periodic Review

This Agreement is valid from the **Effective Date** outlined herein and is valid until further notice. This Agreement should be reviewed at a minimum once per year; however, in lieu of a review during any period specified, the current Agreement will remain in effect.

The **ICT Change Manager** ("Responsible Officer") is responsible for facilitating regular reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties. The Responsible

Officer will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

Business Relationship Manager: ICT
Review Period: Yearly (12 months)
Previous Review Date: N/A
Next Review Date: 01/Nov/2017

Service Agreement

The following detailed service parameters are the responsibility of the Service Provider in the ongoing support of this Agreement.

Service Scope

The following Services are covered by this Agreement;

- Service Request Management
- Incident Management
- Problem Management

Customer Requirements

Customer responsibilities and/or requirements in support of this Agreement include:

- Reasonable availability of customer representative(s) when resolving an Incident, Problem or Request.

Service Provider Requirements

Service Provider responsibilities and/or requirements in support of this Agreement include:

- Meeting response times associated with service related incidents.
- Appropriate notification to Customer for all scheduled maintenance.

Service Assumptions

Assumptions related to in-scope services and/or components include:

- Changes to services will be communicated and documented to all stakeholders.

Service Management

Effective support of in-scope services is a result of maintaining consistent service levels. The following sections provide relevant details on service availability, monitoring of in-scope services and related components.

Service Availability

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

ICT Service Portal: http://servicedesk.aad.gov.au
Telephone support: XXXX
Email support: XXXX

Service Requests

In support of services outlined in this Agreement, the Service Provider will respond to service related incidents, problems and/or requests submitted by the Customer within the following time frames:

Incident SLA

PRIORTY	RESPOND	RESOLVE	TOTAL	WINDOW
(1) CRITICAL	0.5	4	4.5	24x7, 365 days
(2) HIGH	1	8	9	0830 – 1700, Mon – Fri
(3) MODERATE	4	38	42	0830 – 1700, Mon – Fri
(4) LOW	17	85	102	0830 – 1700, Mon – Fri

Key Points:

- Respond, Resolve and Time are displayed in hours.
- Total Response Time (Total) = Respond + Resolve.
- Time includes any escalations or activities that need to occur to bring the incident to resolution.

Problem SLA

PRIORTY	RESPOND	RESOLVE	TOTAL	WINDOW
(1) CRITICAL	1 Day	2 Days	3 Days	24x7, 365 days
(2) HIGH	4 Days	6 Days	2 Weeks	0830 – 1700, Mon – Fri
(3) MODERATE	10 Days	10 Days	1 Month	0830 – 1700, Mon – Fri
(4) LOW	20 Days	40 Days	3 Months	0830 – 1700, Mon – Fri

Key Points:

- Total Response Time (Total) = Respond + Resolve

- Time includes any escalations or activities that need to occur to bring the problem to closure.

Request SLA

SLA NAME	TARGET	ESCALATION	OVERDUE
URGENT REQUEST	1 hour	30 min	30 min
STANDARD SHORT	3 days	2 days	1 day
STANDARD MEDIUM	5 days	4 days	1 day
STANDARD LONG	20 days	15 days	5 days
NON-STANDARD	40 days	30 days	10 days

For more detailed information please see the respective process document for Incident, Problem and Service Request.