Project co-funded by the
CIVIL JUSTICE PROGRAMME
of the EUROPEAN UNION

iSupport
cross-border recovery
of maintenance obligations
pour le recouvrement
transfrontière des
obligations alimentaires

iSupport Tender, Maintenance and Governance Working Group (5)
Monday 16 February 2015, 15h00 UTC (16h00 ECT)

General description of the iSupport Maintenance services
Working paper

This Working Paper provides a governance model for the services relating to the maintenance of the iSupport system (*e.g.*, helpdesk, incident management, changes).

All descriptions and terminology in the document are based on Information Technology Infrastructure Library (ITIL) v2011 (which is the last ITIL version). This document provides a general description of the main ITIL processes.

A diagram showing the process steps is included at the end of the document.

The tenderer is welcome to bring their own procedures which will provide detailed procedures including their own templates for Service documents such as Service Level reports.

Contents

Incident and problem management

Incident

1. The objective of Incident Management is to restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price.

2. The definition of an incident is: An unplanned interruption to an IT Service or a reduction in the Quality of an IT Service. For example, an incident can refer to a malfunction, or another helpdesk request when the user cannot use the system properly which results in a reduction of the Quality. The incident can be reported by the user or by technical staff. In addition, some States may use an automatic monitoring tool which may report an incident, although the preference is for such reporting to come to the Helpdesk from the State technical staff.

Determine priority

3. Impact — Impact is the measure of the extent of the Incident and of the potential damage caused by the Incident before it can be resolved.
   - High — All iSupport users of all States are involved.
   - High — All iSupport users in one State are involved.
   - Medium — Some (not all) users of one or some (not all) iSupport systems are involved.
   - Low — One user of one iSupport system is involved.
4. Urgency — Urgency is a measure of how quickly a resolution of the Incident is required.
   - High — The user cannot use the system at all.
   - Medium — The user cannot use the main part[1] of the system, or can view all parts but cannot edit.
   - Low — The user cannot use another part of the system other than the main part.
5. Priority — Priority is a calculation based on impact and urgency. Priority 1 = highest priority.
   - 1 — eCAB (Escalation Change Advisory Board team) meets by phone.
   - 2 — eCAB is informed by e-mail, the eCAB decides whether a meeting is needed
   - 3 — The SP (Service Provider) resolves the incident.
   - 4 — The SP resolves the incident.
   - 5 — The SP resolves the incident.
6. Table Priority

Priority		Impact		
		High	Medium	Low
Urgency	High	1	2	3
	Medium	2	3	4
	Low	3	4	5

[1] What constitutes the “main part” of iSupport will be defined once iSupport is developed.

Service level requirements for incidents

Average time to implement a solution

7. Table Average time to implement a solution

Timelines **in total**; during working hours / days[2].	Priority				
	1	2	3	4	5
Confirm registration of the incident to the reporter (priority 1 and 2 also to eCAB)	10 minutes	1 hour	4 hours	4 hours	4 hours
Initial documentation is added to the Incident record in the Incident list	2 hours	3 hours	8 hours	3 days	5 days
Meeting of the Emergency CAB	4 hours (by telephone)	8 hours (if applicable)	-	-	-
The incident is analysed, analysis is added to the Incident record	8 hours	2 days	3 days	5 days	3 weeks
Solution available [3](permanent solution or work around)	2 days	3 days	4 days	1,5 week	4 weeks
Documentation added to Knowledge database	2 days	3,5 day	4,5 day	2 weeks	4,5 weeks

Examples:

- A priority 4 incident has to be solved within 1.5 weeks, of which the first 5 days can be spent on the analysis.
- A priority 2 incident has to be analysed within 2 days: if the incident is reported on Monday 15:15h CET, the analysis has to be completed by Wednesday 15:14h CET.

[2] To be defined at a later stage once the participating States are known (*e.g.*, the working hours / days of the jurisdictions operating iSupport).

[3] The moment of implementation depends on the incident: can it wait until the next release, does it have to be available for every State or one State only, etc.

8. Table Service Provider Requirements

Accomplished average % of the number of incidents in one year; others with a maximum margin of 25% of the Service Level	Priority				
	1	2	3	4	5
Confirm registration of the incident to reporter (priority 1 and 2 also to eCAB) by e-mail	90%	90%	75%	75%	75%
First documentation saved in Incident record in Incident list	90%	90%	75%	75%	75%
Analysis completed and saved as Incident record in Incident list	90%	90%	75%	75%	75%
Solution implemented (permanent solution or work around)	90%	90%	75%	75%	75%
Documentation added to Knowledge database	90%	90%	75%	75%	75%

Example:
The registration of 90% of the Priority 1 incidents has to be confirmed within the timelines as mentioned in table 'Service level requirements for incidents'. The remaining 10% may not exceed 25% of the Service level, therefore 10 minutes + 25% = 12,5 minutes maximum.

Workaround

9. The 'workaround' solution reduces or eliminates the impact of an incident or problem where a full resolution is not yet available. A workaround can be a technical solution or a procedural solution, which partly or completely provides a solution for the users. The workaround is not a final solution, e.g. because an extra computer is put into service, or the users perform the task manually.

Problem

10. A problem is the unknown cause of one or more incidents, often identified as a result of multiple similar incidents.
11. The objective of Problem Management is to minimize the impact of problems on the organisation. Problem management plays an important role in the detection and providing solutions to problems (workarounds and known errors) and prevents their reoccurrence.
12. A known error is an identified root cause of a problem. A know error can still be present even where there is a work around in place. Known errors are documented as such.

Change management and release management

Change

13. A change is an addition, modification or removal of anything that could have an effect on IT Services. The scope should include all IT Services, Configuration Items, processes, handbooks, help-screens etc.

14. The goal of change management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change-related incidents upon service quality, and consequently to improve the day-to-day operation of the organisation.

Request for Change (RfC)

15. All changes are described in a Request for Change (RfC). A RfC is an official request for a change either made by the SP or a user. Each RfC is prioritized by the SP based on an assessment taking into account impact, risk analysis, advantages and costs of the change and the business justification. RfCs regarding normal changes are discussed in the CAB. When approved, the RfC is processed (e.g. a programmer changes the source in the development environment and the change is tested in the test environment) and scheduled for a certain release.

Change Advisory Board (CAB)

16. The CAB meets on regular basis. The CAB discusses the RfCs and assigns the priority of the RfCs. More general topics such as the impact of updates on hardware and database systems to the iSupport system can be discussed in these meetings. These topics can be introduced by any member of the Governing Body.
17. Members of the CAB are:
    - One or more States members of the Governing Body[4], ensuring a geographical representation of users
    - At least one representative of the Permanent Bureau (HCCH)
    - At least one representative of the Service Provider

Types of changes

18. The SP determines the type of change:

- Service request

A service request is a change which is approved in advance, has a low risk and it appears on a regular basis. The change can be executed in a short time frame. It will be implemented outside the regular release calendar and does not have to be handled by the CAB. An example of a service request is a small update like a spelling change in the handbook or a local change (see Changes by States).

- Emergency change (e-Change)

An emergency change is handled by the Emergency CAB.

- Normal

All other changes.

[4] Depending on the size of the Governing Body.

Changes by States

19. It is expected that in some cases, States will be permitted, further to the approval of the SP, to make changes to the Source code.

Local changes are described in detail in a RfC document, including the proposed Source code changes. The RfC document is sent to the SP.

20. The RfC is handled as a service request if:

(1) there is no impact on the global iSupport system,

(2) there is no impact to the functionality of iSupport in other States,

(3) there is no impact on the maintenance of the global iSupport system: If this is the case, there should be no requirement for the SP to manage the impact of this change when developing other changes, releasing new releases or handling incidents.

21. A State will always have to wait for approval by the SP before implementing the change. Testing and documentation of local changes are handled by the State.
22. Otherwise, the RfC is not a local change and is handled like a normal change: it has to be approved by the CAB. It is handled by the SP, not the State.
23. Local changes are shown as such in the Knowledge database and are available to all States. If a State want to use a local change from another State, the service request procedure is in place. States can ask to include a local change from another State into the global iSupport system by starting the normal change procedure.

Emergency CAB (eCAB)

24. The eCAB team handles emergency incidents.

Participants of the eCAB team are:

- One or more States members of the Governing Body[5], ensuring a geographical representation of users (which position can change *e.g.*, each month so that all States have an opportunity to be part of the eCAB)
- At least one representative of the Permanent Bureau (HCCH)
- At least one representative of the Service Provider

PIR (post implementation review)

25. Each change is closed after an evaluation of the change including the evaluation of the tests, acceptance, check on cost, time and effort, a check on the achievement of the objective of the change, and lessons learned.

Release

26. A release is a cluster of new and/or updated items, which are tested and approved, and will be implemented in the iSupport system. Regular releases contain changes and all solutions for incidents and problems which have arisen since the last regular release, and include security solutions. Other types of releases will include solutions to incidents or problem.

[5] Depending on the size of the Governing Body.

Release and Deployment management

27. ITIL Release and Deployment Management govern the plan, schedule and control of the movement of releases to test and the live environments. The primary goal of Release Management and Deployment Management is to ensure that the integrity of the live environment is protected and that the correct components are released.

Release calendar

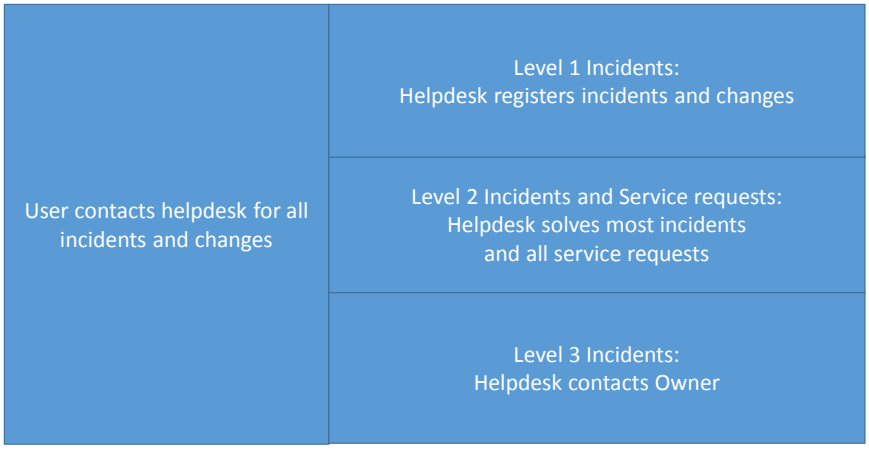
28. Each release consists of a set of changes. Each release is scheduled on a release calendar. Regularly scheduled iSupport versions are expected to be released twice per year, although more may be required in the first year. In between the primary version releases, secondary versions can be released in order to resolve an incident or problem. Unless the version requires otherwise, States are must install regular releases within three months of the release date.

Helpdesk

29. The Helpdesk is provided by the Service Provider. It is available for all iSupport users during the office hours of the iSupport users ('follow the sun'), and provides support for iSupport products only.
30. The iSupport Helpdesk is considered a level 2 service.

There are 3 levels:

- Level 1 = A call centre, with unskilled employees.
- Level 2 = A helpdesk with employees who can deal with most incidents and can take care of the Service Requests.
- Level 3 = Service Desk which can handle all incidents. For specialised incidents regarding the implementation of the Regulation, Convention and iSupport incidents on specialist level, the Helpdesk contacts the Owner. The Helpdesk in this situation remains the 'SPOC' (single point of contact) for the user: the user calls the Helpdesk, then the Helpdesk contacts the Owner, finally the Helpdesk responds back to the user.



Service Level Management

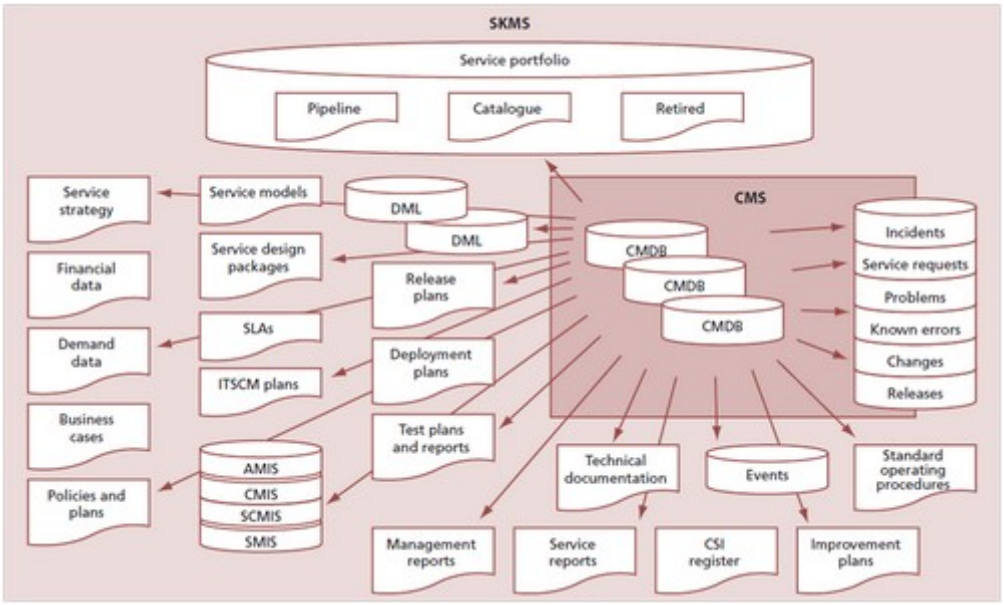
31. Service Level Management (SLM) is the process that forms the Service link between the Service Provider and the iSupport users, the Governing Body and the Owner. The main aim of SLM is to ensure the quality of the IT services provided, at a cost acceptable to the iSupport users. The goal for SLM is to maintain and improve on service quality through a constant cycle of agreeing, monitoring, reporting and improving the current levels of service. It is focused on the operation of iSupport and maintaining the alignment between the iSupport users and the Service Provider.
32. The Service Provider provides Service reports to the owner (HCCH) and the Governing Body on a regular basis. The Service Provider will use the default report templates which contain quantity and quality information.
33. In a meeting at least once per year, the Service Level Manager presents the results, and negotiates the Service Levels for the upcoming period if applicable, with the Governing Body and the Owner.

Service Asset and Configuration management

34. Service Asset and Configuration management (SACM) ensures that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available. A CMS, the Configuration management system, manages all CIs (Configuration Items) in the CMDB(s) (Configuration Management DataBase) of the iSupport system. All incidents, problems, changes, releases and service levels are based on one or more CIs. CIs are not stored in the CMDB, only the reference to the CIs. The SKMS (Service Knowledge Management System) is a set of tools and databases that are used to manage knowledge, information and data.

Knowledge management

35. The primary role of Knowledge Management is to improve the quality of decision making by ensuring that accurate, reliable and trustworthy information is available throughout the Service Lifecycle.
36. The usage is knowledge that is provided by the Service Knowledge Management System (SKMS). The SKMS contains links to all types of knowledge: all incidents and problems (pending and closed), known errors, service requests, changes and release information, SLAs, documentation like test-plans, management reports etc.

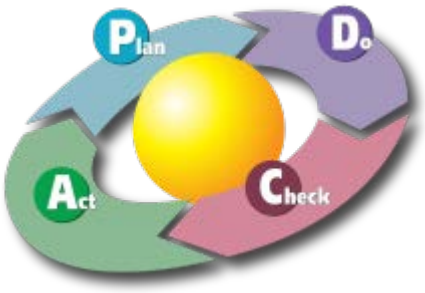


37. Examples of the usage of the SKMS:

- Users can view the status of a reported incident and look for pending incidents and known errors (and solutions) before they report an incident. They can view procedures and handbooks.
- Governing Body members and the Owner can view reports like financial reports and service level management reports.
- The CAB can view reported RfCs and the Release Calendar.

Continual service improvement (CSI)

38. The Continual Service Improvement (CSI) process uses methods from quality management in order to learn from past successes and failures. The CSI process goal is to continually improve the effectiveness and efficiency of IT processes and services, in line with the concept of continual improvement adopted in ISO 20000.

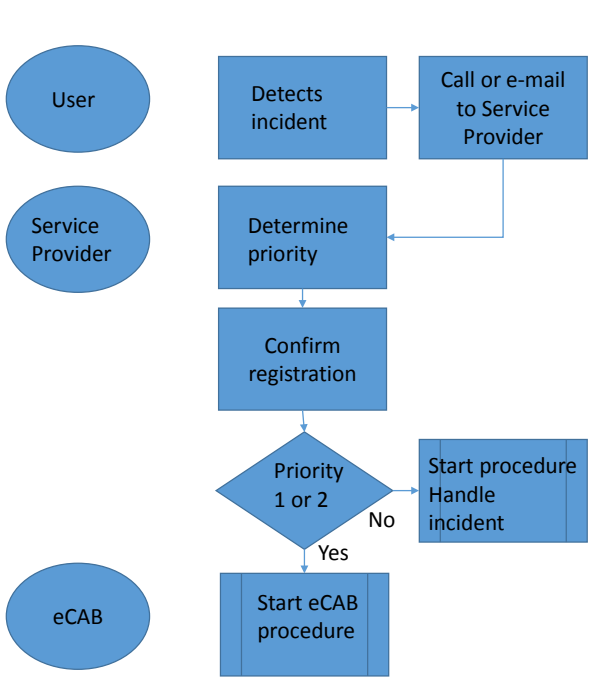


39. The Deming Cycle (PDCA cyclus, created by Edward Deming) is used in the CSI process.

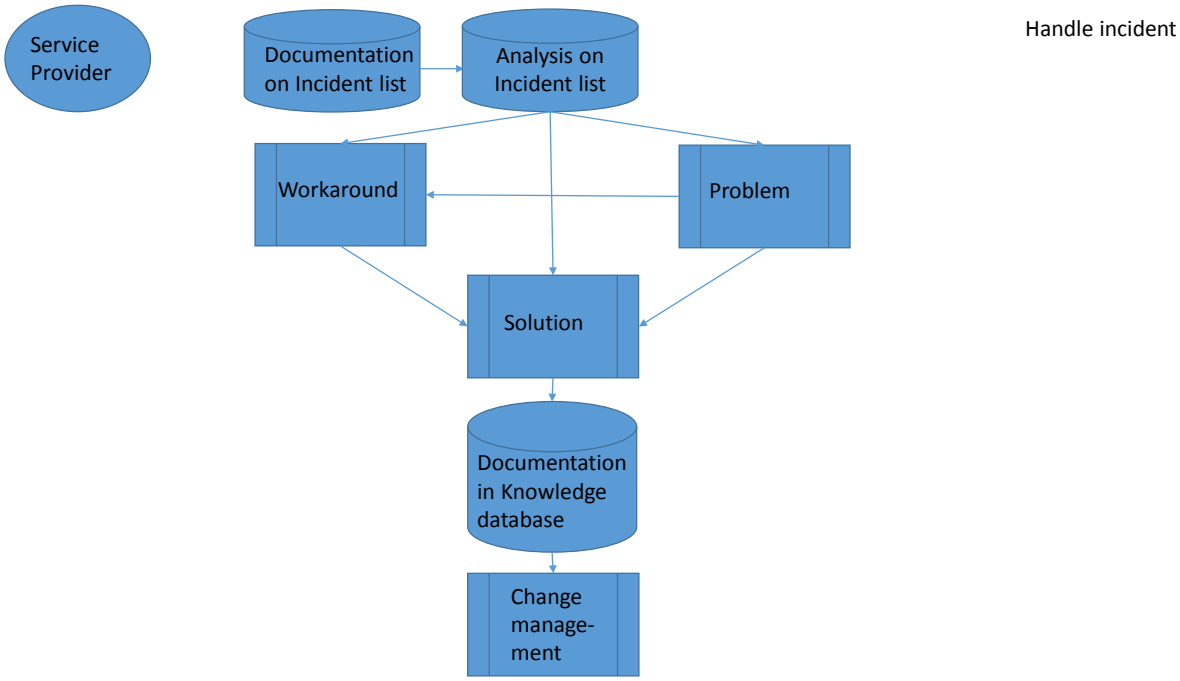
The Owner identifies a CSI manager within the HCCH organisation. The CSI manager works, together with the SP and the Governing Body, on the service improvement process.

Process steps diagram

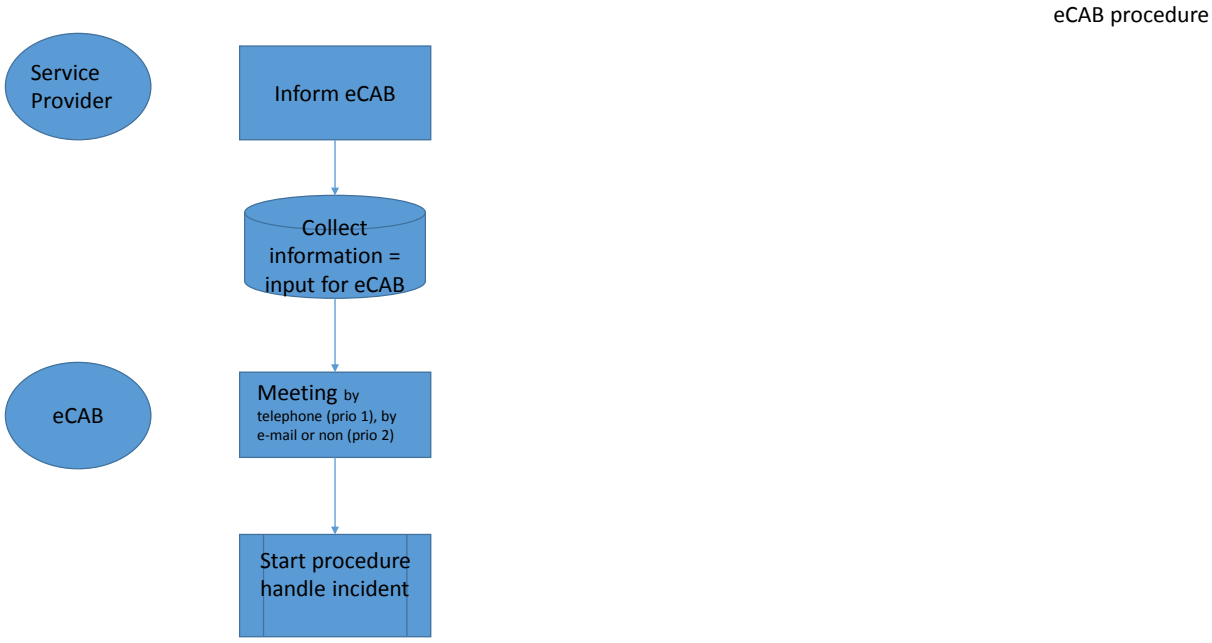
40. Diagram: Incident management – start an incident



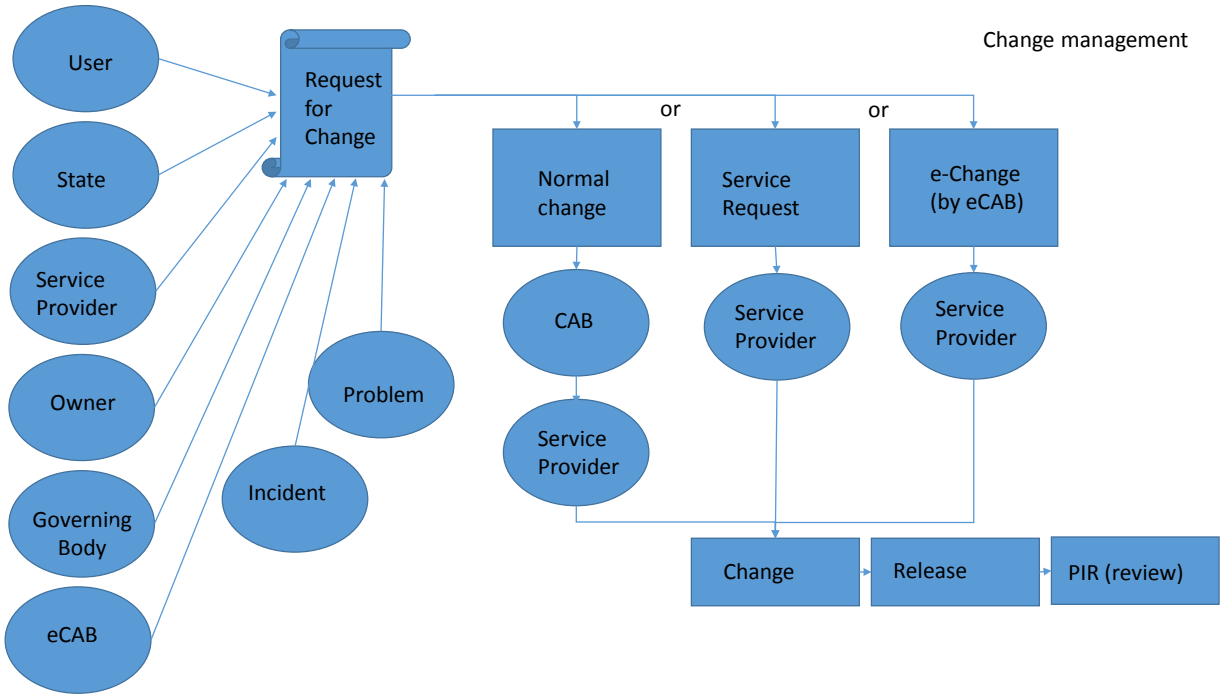
41. Diagram: Handle incident



42. Diagram: eCAB procedure



43. Diagram: Change management



44. Diagram: Local change