

MANUAL

DATA ACQUISITION & CONTROL ARCHITECTURE (DACA) – PROCEDURAL CONTROLS – INCIDENT MANAGEMENT

DEP 32.01.22.12-Gen.

March 2007
(DEP Circular 60/07 has been incorporated)

DESIGN AND ENGINEERING PRACTICE



This document is restricted. Neither the whole nor any part of this document may be disclosed to any third party without the prior written consent of Shell Global Solutions International B.V., The Netherlands. The copyright of this document is vested in this company. All rights reserved. Neither the whole nor any part of this document may be reproduced, stored in any retrieval system or transmitted in any form or by any means (electronic, mechanical, reprographic, recording or otherwise) without the prior written consent of the copyright owner.

PREFACE

DEPs (Design and Engineering Practice) publications reflect the views, at the time of publication, of:

Shell Global Solutions International B.V. (Shell GSI)

and/or

Shell International Exploration and Production B.V. (SIEP)

and/or

other Shell Service Companies.

They are based on the experience acquired during their involvement with the design, construction, operation and maintenance of processing units and facilities, and they are supplemented with the experience of Shell Operating Units. Where appropriate they are based on, or reference is made to, international, regional, national and industry standards.

The objective is to set the recommended standard for good design and engineering practice applied by Shell companies operating an oil refinery, gas handling installation, chemical plant, oil and gas production facility, or any other such facility, and thereby to achieve maximum technical and economic benefit from standardization.

The information set forth in these publications is provided to Shell companies for their consideration and decision to implement. This is of particular importance where DEPs may not cover every requirement or diversity of condition at each locality. The system of DEPs is expected to be sufficiently flexible to allow individual Operating Units to adapt the information set forth in DEPs to their own environment and requirements.

When Contractors or Manufacturers/Suppliers use DEPs they shall be solely responsible for the quality of work and the attainment of the required design and engineering standards. In particular, for those requirements not specifically covered, the Principal will expect them to follow those design and engineering practices which will achieve the same level of integrity as reflected in the DEPs. If in doubt, the Contractor or Manufacturer/Supplier shall, without detracting from his own responsibility, consult the Principal or its technical advisor.

The right to use DEPs is granted by Shell GSI, in most cases under Service Agreements primarily with Shell companies and other companies receiving technical advice and services from Shell GSI or another Shell Service Company. Consequently, three categories of users of DEPs can be distinguished:

- 1) Operating Units having a Service Agreement with Shell GSI or other Shell Service Company. The use of DEPs by these Operating Units is subject in all respects to the terms and conditions of the relevant Service Agreement.
- 2) Other parties who are authorized to use DEPs subject to appropriate contractual arrangements (whether as part of a Service Agreement or otherwise).
- 3) Contractors/subcontractors and Manufacturers/Suppliers under a contract with users referred to under 1) or 2) which requires that tenders for projects, materials supplied or - generally - work performed on behalf of the said users comply with the relevant standards.

Subject to any particular terms and conditions as may be set forth in specific agreements with users, Shell GSI disclaims any liability of whatsoever nature for any damage (including injury or death) suffered by any company or person whomsoever as a result of or in connection with the use, application or implementation of any DEP, combination of DEPs or any part thereof, even if it is wholly or partly caused by negligence on the part of Shell GSI or other Shell Service Company. The benefit of this disclaimer shall inure in all respects to Shell GSI and/or any Shell Service Company, or companies affiliated to these companies, that may issue DEPs or require the use of DEPs.

Without prejudice to any specific terms in respect of confidentiality under relevant contractual arrangements, DEPs shall not, without the prior written consent of Shell GSI, be disclosed by users to any company or person whomsoever and the DEPs shall be used exclusively for the purpose for which they have been provided to the user. They shall be returned after use, including any copies which shall only be made by users with the express prior written consent of Shell GSI. The copyright of DEPs vests in Shell GSI. Users shall arrange for DEPs to be held in safe custody and Shell GSI may at any time require information satisfactory to them in order to ascertain how users implement this requirement.

All administrative queries should be directed to the DEP Administrator in Shell GSI.

TABLE OF CONTENTS

1.	INTRODUCTION	4
1.1	SCOPE	4
1.2	DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS	4
1.3	DEFINITIONS	4
1.4	ABBREVIATIONS	5
1.5	CROSS-REFERENCES	5
1.6	COMMENTS ON THIS DEP	5
2.	INCIDENT MANAGEMENT	6
2.1	GENERAL	6
3.	CREATE INCIDENT MANAGEMENT PROCESS	7
3.1	CREATE A DACA INCIDENT MANAGEMENT PROCESS	7
3.2	SET PROCESS PERFORMANCE TARGETS	8
4.	CREATE A DACA INCIDENT RESPONSE TEAM	9
4.1	INCIDENT RESPONSE TEAM	9
5.	INCIDENT RESPONSE PROCESS	11
5.1	INCIDENT RESPONSE PLAN	11
5.2	COMMUNICATION DURING THE INCIDENT	17
6.	HIGH LEVEL WORKFLOW OF 'MANAGE INCIDENTS'	19
6.1	GENERAL	19
6.2	IDENTIFY AND LOG INCIDENT	20
6.3	CATEGORIZE, PRIORITIZE AND ALLOCATE INCIDENT	22
6.4	IDENTIFY RESOLUTION PLAN	23
6.5	RESOLVE INCIDENT	25
6.6	FOLLOW-UP INCIDENT	27
7.	REFERENCES	29

1. INTRODUCTION

1.1 SCOPE

This new DEP describes the Management Process for handling Information Security Incidents within the Process Control Domain (PCD); otherwise known as DACA Incident Management.

The purpose of this DEP is to guide Operating Units in implementing a robust incident management system. The establishment of these procedures and standards will ensure that the Operating Units are able to handle any interruption to a working service that disrupts access or use of Information Technology related services in the Process Control Domain.

This DEP will detail at a high level the various activities required to detect, assess, contain, document and analyse an information security incident. This DEP should be in addition to ITCI 051 and ITCI 052, any local incident management procedures, and any applicable regulations.

This DEP does not cover any specifics on how to identify or resolve any incidents, but will provide the framework to handle any DACA incidents.

The intended audience for this document is for PCD Administrators, C&A discipline and security focal points.

Where specific roles and responsibilities have been described in this DEP they have been based on DEP 32.01.21.10-Gen. In case of conflicts with any of the above-mentioned documents, this document will prevail.

1.2 DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS

Unless otherwise authorised by Shell GSI, the distribution of this DEP is confined to Shell companies and, where necessary, to Contractors and Manufacturers/Suppliers nominated by them.

This DEP is intended for use in major development projects and existing producing assets in exploration and production. However, it may be applied to other Business Groups at the discretion of the Principal.

When DEPs are applied, a Management of Change (MOC) process should be implemented; this is of particular importance when existing facilities are to be modified.

If national and/or local regulations exist in which some of the requirements may be more stringent than in this DEP, the Contractor shall determine by careful scrutiny which of the requirements are the more stringent and which combination of requirements will be acceptable with regards to the safety, environmental, economic and legal aspects. In all cases the Contractor shall inform the Principal of any deviation from the requirements of this DEP which is considered to be necessary in order to comply with national and/or local regulations. The Principal may then negotiate with the Authorities concerned, the objective being to obtain agreement to follow this DEP as closely as possible.

1.3 DEFINITIONS

1.3.1 General definitions

The **Contractor** is the party that carries out all or part of the design, engineering, procurement, construction, commissioning or management of a project or operation of a facility. The Principal may undertake all or part of the duties of the Contractor.

The **Manufacturer/Supplier** is the party that manufactures or supplies coating materials, equipment and services to perform the duties specified by the Contractor.

The **Principal** is the party that initiates the project and ultimately pays for its design and construction. The Principal will generally specify the technical requirements. The Principal may also include an agent or consultant authorised to act for, and on behalf of, the Principal.

The word **shall** indicates a requirement.

The word **should** indicates a recommendation.

1.4 ABBREVIATIONS

Term	Definition
C&A	Control & Automation engineering discipline
CCR	Central Control Room
DACA	Data Acquisition & Control Architecture
HSE	Health, Safety and Environment
ISIM	Information Security Information Manager
PCAD	Process Control Access Domain
PCD	Process Control Domain
PCDP	Process Control Domain Portal
RAM	Standard Shell Risk Assessment Matrix in accordance with EP2005/EP95000 methodology

1.5 CROSS-REFERENCES

Where cross-references to other parts of this DEP are made, the referenced section number is shown in brackets. Other documents referenced by this DEP are listed in (7.).

1.6 COMMENTS ON THIS DEP

Comments on this DEP may be sent to the DEP Administrator at standards@shell.com. Shell staff may also post comments on this DEP on the Surface Global Network (SGN) under the Standards folder.

2. INCIDENT MANAGEMENT

Definition of "PCD information security incident": any event that disrupts the expected standard operation of any PCD service, facility or system and causes disruption of or denial of operation to the PCD, or inappropriate access to or use of data.

An incident can also be caused by system failure or human error.

In this document the word 'incident' refers to 'PCD information security incident'.

2.1 GENERAL

Each Operating Unit shall have a DACA Incident Management Plan. This should be incorporated into any existing incident management plans. The plan should set out how a team is able to respond to and resolve a security incident in the Process Control Domain.

Incident Management is part of EP.24.04.05:

- Develop and execute an Information Security Improvement Programme, including implementation and testing of Business Continuity Plans (BCP) and Disaster Recovery Plan (DRP).
- Deal with information security incidents as and when they arise.

Ref DEP 32.01.21.10-Gen (DACA Roles and Responsibilities): The Operating Unit IT Service Delivery Manager and the OU DACA Security Focal Point are responsible for the Incident Management process. The Operating Unit Engineering Manager is accountable. The GITI DACA Service Manager and Group Security (ITCI) provides additional support. The ISIM should be involved in the creation of a DACA Incident Management Plan.

3. CREATE INCIDENT MANAGEMENT PROCESS

Key activities in this part of the management process are:

- Create a DACA Incident Management Plan
- Create a DACA Incident Response Team
- Set targets and KPIs

3.1 CREATE A DACA INCIDENT MANAGEMENT PROCESS

3.1.1 General

A regional/Operating Unit DACA incident management process should be available. The process should be about creating and maintaining an incident management plan. The incident management plan details how the organisation is able to respond to and resolve an Information Security incident in the Process Control Domain. There should be an owner for the plan, process and procedures.

- Identify key processes as identified in this document, and create local procedures for handling any incidents.
- Map the process activities, assign responsibility and identify involved parties.
- Identify the technology used. Optimise the design of the process, taking into account opportunities offered by technology.
- Assess process improvements from audits and reviews
- Identify process improvement options, evaluate and assess impact on existing organisation.
- Create an owner of the DACA incident management process.
- Ensure that the Asset Manager(s) provide input into the process development
- Ensure that this DACA incident management process is aligned with other incident management processes.

3.1.2 Incident management process documentation

A person should be assigned to upkeep and maintain the incident response process documentation and ensure that they are kept up to date. This person does not necessarily have to be involved in any of the incidents

If support is required outside normal working hours, the appropriate procedures and processes should be put in place and communicated.

The team should keep an up to date contact list of external support personnel; e.g. SecOps, GITI, Vendors etc

3.1.3 Responsibilities of the 'process owner'

- Maintain a register of stakeholder and legislation issues associated with the incident management process
- Identify threats to business objectives associated with the incident management process
- Propose KPIs to monitor risk controls, to be agreed by the Engineering/Asset Manager
- Identify any regulations that may need to be complied with
- Identify stakeholders
- Develop and maintain database for hazards, control measures and responsibilities
- Produce accountability and responsibility statements with contractors and third parties

- Maintain an integrated audit programme on the incident management process
- Define training needs for the people involved in the incident management process
- Co-ordinate performance review
- Communicate / report performance to stakeholders
- Monitor changes in external environment that affect the probability and consequence of threats to the business
- The OU DACA security focal point may be the process owner
- Monitor performance
- Identify areas to improve
- Update plan

3.1.4 Asset Manager Input

- Agree criteria for business risks associated with the incident management process
- Agree KPIs for the incident management process
- Agree control measures and responsibilities associated with the incident management process
- Ensure adequate resources and skills to effectively execute the incident management process
- Identify deviations from normal practice which affect probability and consequence, requiring additional controls

3.2 SET PROCESS PERFORMANCE TARGETS

The incident management process owner, Asset Manager and the Engineering Manager should set a number of KPIs for incident management.

These KPIs should not reflect the number of incidents or resolution time, as these vary from one incident to another.

The KPI should be based on improving the incident response, reducing the risk of the incident occurring again and incident reporting. Some examples are:

- Completing the security incident form and getting it signed off within a set period.
- Completing a post incident review shortly after the incident occurring
- Applying any actions after the post incident review
- Adding the security incident into a centrally managed system

The KPIs should be monitored and applied in the standard format within the facility/OU.

4. CREATE A DACA INCIDENT RESPONSE TEAM

This Section provides an extract and further details of the roles and responsibilities described in DEP 32.01.21.10-Gen. In any case, any local amendments to that DEP shall prevail.

4.1 INCIDENT RESPONSE TEAM

4.1.1 General

The incident response team will be responsible for investigating, resolving and owning any problem. The team should be fully aware about the C&A and IT functionality within the asset. The team should be comprised of at least the following people:

- Incident Investigator – responsible for resolving the incident and collating evidence.
- Incident Owner – responsible for co-ordinating the response and communication flow.
- Incident Support – C&A, IT, ISIM, Maintenance, Operations, Vendors etc
- Service Desk – a single point of contact for reporting incidents

A single person could take on more than one role, and several people can be involved in a single role.

4.1.2 DACA security focal point

The OU's DACA security focal point is responsible to the business for investigating, resolving and owning any data for any IT security incident within the PCD. The main responsibilities are:

- Investigating and reporting the cause behind any incident (Post Incident Review)
- The contact point for the business and affected asset managers
- Handling any escalations as required

4.1.3 Incident owner

The Incident Owner is the individual most responsible for the affected service and/or the source of the problem. The Incident Owner is responsible for working with the Incident Coordinator to ensure that communication to affected users and managers is maintained. The Incident Owner is also responsible for ensuring adequate and appropriate resources are assigned to the incident response team. Specifically, the incident owner is responsible for:

- Invoking the need for the incident response team.
- Keeping IT and Engineering management and the incident investigator informed of incident status.
- Ensuring appropriate resources are assigned.
- Ensuring that the work of the incident management team is coordinated.
- Escalating the problem as outlined in the escalation process.
- Sending problem notification and communicating status.
- Investigating and reporting on the cause of the incident (with the OU DACA security focal point.
- Ensuring appropriate legal and HR approvals are in place for people-related security incidents

The incident owner is not the same role as the incident process owner.

4.1.4 Incident response team's responsibilities

The incident response team can be composed of people from various departments. The incident response team is responsible for:

- Working together as a team to identify the problem using the technical expertise of all individuals to investigate all potential sources of a given problem.
- Working with the incident owner to identify resources needed to resolve the problem.
- Discussing ideas and suggestions for the possible source(s) of the problem.

ITCI 117 Section 3.4.13: *An investigation shall be performed into the source of the incident.*

- Agreeing on an action plan for researching the issue.
- Recommending specific assessment, investigation, and mitigation steps to the Incident Owner.
- Making recommendations to the incident owner such as a need for escalation, communication, etc.

NOTE: For the duration of the incident, members of the incident response team are directed by and responsible to the incident owner

- Once the issue is identified, the group agrees on an action plan and carries it out.

4.1.5 24x7 PCD support desk

The 24x7 PCD Support Desk is responsible for:

- Communicating the problem via company-wide mechanisms as specified in the Incident Response Process and Communication Guidelines.
- Providing feedback to the Incident Owner regarding user inquiries.
- Providing feedback to the problem reporter(s) (if not part of Incident Team)
- Recording the incident as a trouble ticket, and closing the ticket when the incident is closed.

4.1.6 IT staff

If a service is quickly restored before the incident response process has been invoked, the OU DACA Security Focal Point and PCD Administrator should still be informed, and they will bring these incidents to the Operations Meeting for discussion and post-incident reviews as necessary.

4.1.7 Incident response training

The incident response team(s) should meet on a regular (approximately 3-monthly) basis to review the procedures and processes and update them where necessary.

If an incident has not occurred in the previous 6 months, then a dry run of an incident should be enacted. Where possible, this should be linked into the OU Emergency Response Management system.

To ensure that the incident management plan succeeds, all personnel shall be trained. The following is a minimum standard:

- All staff and contractors in the PCD should be trained to identify an incident.
- All support personnel should be trained to identify an incident.
- All staff and contractors in the PCD should be informed of how to report an incident.
- All support personnel should be aware of how to respond to a reported incident.
- All response personnel shall be trained to appropriately respond to an incident.

A training plan should be made for each role to onboard new members of the team.

5. INCIDENT RESPONSE PROCESS

ITCI 117 Section 3.4.1: *The following responsibilities and procedures shall be developed and documented to enable timely management of any security incident within the PCD and/or PCAD.*

- *Incident management plan* (see note below)
- *Incident response training*
- *Incident alarm/detection process*
- *Incident response ownership*
- *Incident response plan*
- *Incident communication plan*
- *Incident investigation plan*
- *Incident close-out process, including remediation.*

NOTE: The above is a direct extract from ITCI-117 but it is strictly not accurate. In the context of this DEP, the term incident management plan as used above should be considered to mean incident response plan.

The incident response plan will form the core of the incident management process. The key activities in the incident response process are:

5.1 INCIDENT RESPONSE PLAN

5.1.1 Incident detection

5.1.1.1 General

Detecting an incident is the responsibility of all personnel within the PCD, and in some parts GITI and/or the local IT support teams. It is not always easy to detect when an incident is occurring, but some of the signs are uncharacteristic system behaviour, slow responses or process failures.

5.1.1.2 Systems Management

Systems within the PCD should be enabled to help detect and log when an incident is occurring. Mechanisms shall be in place to detect and log as a minimum:

- Account Login Failures
- Discovery of an infected file
- Uncharacteristic system behaviour
- Shutdown/Restart of equipment
- New unauthorised devices on the network
- Rejected connection attempts into or out of the PCD and PCAD
- Change to configuration of network devices (switches, routers, firewalls)
- Change to event logging configuration of any device
- Sharp, sustained network bandwidth utilisation changes

5.1.1.3 Logfiles

Logfiles can be used to report an incident, for incident investigation and for the post incident review. Configuring and using logfiles and their tools are described elsewhere.

5.1.1.4 Archiving of logfiles

ITCI 117 Section 3.4.5: *The logfiles shall be protected against unauthorised access.*

ITCI 117 Section 3.4.6: *The logfiles shall be archived for a minimum of one year or for the minimum legal requirements.*

5.1.2 Incident reporting

5.1.2.1 Incident reporter

It is the responsibility of anyone detecting an incident, or believing that an incident is occurring, to report the incident. Once an incident has been, or is thought to have been identified this should be reported to the service desk in a timely manner. To help with the investigation the incident reporter should provide as much information as possible to the service desk, such as:

- Date and time of the incident, and if the incident appears to have finished, the duration of the incident.
- Location(s), where you are and where the incident is occurring
- Details of the devices, applications etc. affected
- Symptoms

5.1.2.2 Service desk

When the Service Desk (or 24x7 function that receives the problem report) receives an incident notification they should complete the following:

- Retrieve as much information from the reporter and use an Incident Reporting Form for recording the information.
- Correlate all the incidents together, to check if there is a common cause.
- Record the time, duration and location of the incident.
- Assign a initial categorisation and priority
- Inform the PCD administrator
- Inform the ISIM
- Determine who should be notified internally
- Determine who should be notified externally

5.1.3 Incident assessment and investigation

5.1.3.1 Incident assessment

Once a security incident has been identified then it should be categorised and prioritised and the appropriate actions taken. The Service Desk conducts an initial assessment; the incident owner should change the assigned categories and prioritisation if required.

5.1.3.1.1 Categorisation

Each asset should have an incident categorisation and prioritisation guideline. The following is a guideline that can be used or adapted to existing procedures; also ITCI 052 can be used for guidance:

- **Category 1 – Cyber security incident when the PCD IT infrastructure is the target**

This category typically includes intrusions into the IT infrastructure, Denial of Service attacks and incidents resulting from “malware” [viruses, worms, spam and PUPs (Potentially Unwanted Programs, e.g. adware and spyware, etc.)].

- **Category 2: Information security incidents where elements of the IT infrastructures or applications are misused**

This category includes fraud, where IT infrastructure or applications is used, theft of IT components and anything else that contravenes rules on the acceptable use of company IT facilities, e.g.: chain e-mail; use of games and unlicensed software; use of IT facilities for storage and dissemination of unacceptable material, pornography, hate mail, etc.

- **Category 3: Information security incidents where no IT components play a role**

This category includes theft, loss or unauthorised disclosure of (classified) information, and external threats to information posed by activities such as illegal information brokering.

- **Category 4: Investigations by others**

This special category includes the management of those incidents where a Shell Company is required to support the external investigation of our systems and the information contained on them.

5.1.3.1.2 Prioritisation

Prioritisation should dictate how much effort and urgency is required to resolve the incident. A Corrective Maintenance Prioritization Tool (CMPT) has been designed and globally approved for use in Shell E&P to ensure the correct level of priority can be assigned to maintenance corrective work. The CMPT has origins with the HSE RAM.

The tool is used to assess the robustness of the temporary mitigation that is implemented when a failure or an incident occurs.

In the CMPT, seven types of priorities are defined, based on the severity of the potential consequences if the corrective actions are not completed, together with the likelihood of those consequences actually occurring before completion.

Table 1 Corrective Maintenance Schedule Prioritisation

Corrective Maintenance Schedule Prioritisation		
	Priority Setting	Latest Allowed Finish Date
7	Routine Priority	12 Months
6	Routine Priority	6 Months
5	Routine Priority	8 Weeks
4	Routine Priority	4 Weeks
3	Routine Priority	2 Weeks
2	Urgent Response Priority	Immediate
1	Emergency Priority	Immediate

High priority jobs are always escalated to the OU Asset Manager for further review, mitigation and risk reduction.

5.1.3.2 Incident Investigation

When an incident occurs, then the fault needs to be investigated, contained and resolved.

ITCI 117 Section 3.4.11: *An investigation shall be performed within a month to identify any risks to the integrity of the safety and production systems.*

ITCI 117 Section 3.4.16: *Any troubleshooting tools utilised on the PCD shall be approved by the PCD administrator (or relevant designated authority) each time they are used.*

The first priority is to identify what type of incident is occurring (or has occurred); there are many types of incidents that can occur. Procedures should be put in place to ensure operators, maintenance personnel and others are able to help identify incidents.

Descriptions of incidents include:

- User account compromise
- Behavioural vulnerability
- Corruption of Data / Information
- Denial of Service
- Disclosure (Misuse) of Data / Information
- Network compromise
- Password compromise
- Physical security
- Probes
- Process vulnerability
- Administrator account compromise
- Software vulnerability
- Theft – Data
- Theft – Physical
- Unauthorised Access and/or Use
- Virus

Once the type of incident has been identified, then the extent of the incident shall be clarified as follows:

- Determine the extent of damage or penetration
- Determine all devices, services, processes that are affected
- Perform a business impact analysis

Data can be gathered from the following sources:

- Visual – LEDs, Alarms, monitoring software
- Logs – Systems CPU I/O, network logs, application, firewall
- Analysis Software – Sniffers, Performance Management tools

The Incident Team shall record all information about the data gathering, incident resolution attempts and actions taken during the investigation. This information will be used in the Post Incident Review.

5.1.3.3 Incident Containment and Resolution

Because an information security incident can affect other devices within the PCD, the incident should be contained as soon as possible to ensure it does not escalate.

Whilst the incident is occurring decisions need to be made about containing the incident. The Incident Owner shall decide whether the incident will impact HSE and production if it spreads to other hosts.

If the incident spreads from the current source (e.g. Virus) to other devices, then a decision about removing that device from the Network shall be made as quickly as possible.

ITCI 117 Section 3.4.12: *The device(s) that are affected by the security incident should be isolated from other systems if possible.*

The following are some examples on how to isolate systems:

- Disconnect from the network

- Review system access rights
- Stop processes running on the system
- Introduce new passwords within the system

Once the incident has been identified, assessed and if required contained, then the incident needs to be resolved and a course of action planned out. If the system has been contained, then the Incident Owner may reduce or increase the priority as required. The intention is for the PCD to be returned to a fully working environment.

When the incident may have been caused by malware or suspicious activity, it shall be investigated whether any data has been modified, deleted or copied. If there is the possibility that there is a virus, Trojan etc., especially if it allows remote access to the device, then the total system must be restored from the backups. It is essential that system and data backups are completed, and that the restore procedures are complete and tested.

5.1.4 Resolution

Once the service has been restored then all data that would assist in the incident investigation should be gathered from the systems.

If a device was disconnected from the network during the incident, ensure that the operators are aware when it will be reconnected.

If a device has been or is suspected to have been infected by malware (virus, Trojan etc.) then a full updated virus scan, security patch update, firewall ruleset change and/or any other appropriate mitigating steps shall be implemented before the device is connected back to the network.

ITCI 117 Section 3.4.14: *Once the device(s) have been restored, the integrity of the system shall be verified before the system is placed back into operation.*

When the system is connected, check that the symptoms are not occurring again.

Once the incident owner is satisfied with the resolution, then he/she should inform the service desk, who in turn should close the ticket and inform the incident reporters. The incident owner, with the OU DACA Security Focal Point, should then complete a post incident review, and the security incident form. The incident should not be closed until the end user or customer has acknowledged that the service is running without problems.

5.1.5 Incident escalation

Procedures should be created for escalating an incident within the organisation and to external sources, such as vendors and maintenance contractors.

ITCI 117 Section 3.4.10: *A documented security incident escalation process shall be maintained to ensure appropriate escalation to other relevant parties of the incident.*

All persons involved and senior management should be aware of these procedures.

The escalation procedures should be linked to the severity and priority of the incident.

In the initial assessment, each incident is communicated and resources are assigned. Whenever additional information is discovered, the initial decisions about resources and communications may need to be modified.

Only the incident owner or OU DACA Security Focal Point may only invoke escalation of an incident. Escalation can include, but is not limited to:

- Change in incident owner
- Substantial change in incident team
- Change in scope (e.g. user impact)
- Security implications
- Change in required resources (including outside vendors)
- Releasing personnel so they can be part of the incident team

5.1.6 Handling incident response data

5.1.6.1 General

During the investigation, restoration and operation of the incident, as much information as possible should be gathered, stored and analysed. The data should then be kept for the standard incident investigation and any possible asset, partner and/or legal investigation.

5.1.6.2 Gathering data

There are a number of ways in which the data can be obtained that needs to be analysed and used for the post incident report:

- Interviewing witnesses or relevant parties.
- Performing crime scene analysis.
- Gathering supporting evidence.
- Gathering staff evidence. For example, Human Resources records, permits to work.
- Retrieving the incident data from the incident team.
- Creating a forensic backup of relevant data or systems. For example, imaging of computer systems.
- Identifying what records or logs exist for the incident
- Identifying other evidence. For example, witnesses, CCTV, manual systems, system connectivity.

Where relevant the Chief Ethics and Compliance Officer shall be contacted to advise on the Shell General Business Principles regarding data gathering techniques used in the event of possible litigation.

5.1.6.3 Analysing incident data

Analysing the data can be time consuming, but is required to efficiently learn from the event. The following are some of the steps that can be used:

- If an attempt was unsuccessful, establish why it failed
- Establish which systems were directly and indirectly involved
- Establish the value and relevance of evidence
- Establish if other systems could be involved which have not been investigated

5.1.6.4 Storing incident data

All data that is recovered during the incident should be stored in a secure environment.

5.1.7 Post incident report

ITCI 117 Section 3.4.9: *A process shall be implemented to enable collection and reporting of all security incidents.*

5.1.7.1 Incident Report

An incident review team comprising of the incident owner, engineers, vendors and other interested parties should be formed to complete the report. This team should be led by someone outside the respective discipline of the incident and not actually involved in the incident.

A post incident report should be used to assist the investigation team to assist in reviewing the incident. The post incident report should use data from the data analysis of the incident and include:

- The sequence of events
- A list of systems directly and indirectly involved
- Related history and background

- Establish the root cause
- The resolution and, if required, all the actions that occurred to get to the resolution.
- Lessons learned including opportunities for future improvement of processes, procedures and/or service.

5.1.7.2 Incident Final Reporting

ITCI 117 Section 3.4.2: *PCD incidents shall not be reported via the Global Incident Management System (Fountain).*

The Incident Report should be filed and stored in accordance with the local, regional or central procedures.

Any recommendations that are made by the incident review team should be implemented in a timely manner. If the recommendations are not to be implemented, then a risk assessment must be made and the discipline head or the asset manager should make the final decision.

5.1.7.3 Incident Close Out

ITCI 117 Section 3.4.15: *All high-priority remediation actions that the investigation finds shall be completed within a defined period of time after reporting.*

- Review the Post Incident Report
- Distribute the Post Incident Report to local teams and the Central DACA Team
- Ask "should we disclose to statutory bodies?"
- Review assessment and countermeasures
- Determine whether the attack was internal or external
- Address disciplinary issues
- Consider legal proceedings
- Address contractual issues

5.2 COMMUNICATION DURING THE INCIDENT

5.2.1 Notification

Most of the following steps are covered by the previous steps, but a formal communication plan should be used, to ensure that all personnel are aware. The stakeholders in the first four stages of the incident response process (6.1) shall be notified as follows:

- Notify first-tier support at the PCD service desk
- Assign a service desk ticket with an initial assignment to the incident owner. The service desk reports the ticket number to the incident owner.
- Update online "alerts and status" pages
- Notify Information operators and/or operators as appropriate
- Notify all I&IT staff of high-priority or high-visibility incidents. The incident owner may need to rely on individual managers to notify respective staff.
- Notify Resolution of Incident to all affected bodies
- Notify people about the Post Incident Report
- If required, notify Public Affairs
- If required, notify Authorities / Governing Bodies

Notification may include a description of the problem, identification of affected users, attempted mitigation, and estimated restoration of service.

5.2.2 Methods of communication

Methods of communication shall be electronic as follows:

- Communications between the service desk and incident owner must be acknowledged; a plan must be made in case the incident owner is not contactable, on how to communicate with each other.
- In the event of an expected short-term (less than 3-hour) outage, e-mail to those groups listed on the incident communications flow chart
- In the event of an expected long-term outage with high impact, e-mail to key groups.
- If e-mail and/or the network are affected by the incident, rendering electronic methods of notification impossible or unreliable, voice mail shall be used in addition to, or instead of, e-mail.
- In the event of an expected short-term (less than 3-hour) outage, voice mail notification and a distribution list should be used.

An approved procedure shall be put in place for dealing with any news media. At no time during or after the incident shall any member of staff talk directly to the news media about any incident without the prior express approval and direction of the designated authority.

6. HIGH LEVEL WORKFLOW OF 'MANAGE INCIDENTS'

Objective	Ensure that a Security Incident affecting the PCD is effectively managed and the incident resolved as safely and as quickly as possible. Ensure that records are kept of the steps taken to investigate and resolve each incident.
------------------	--

6.1 GENERAL

The following process map represents the high level activities of managing incidents.

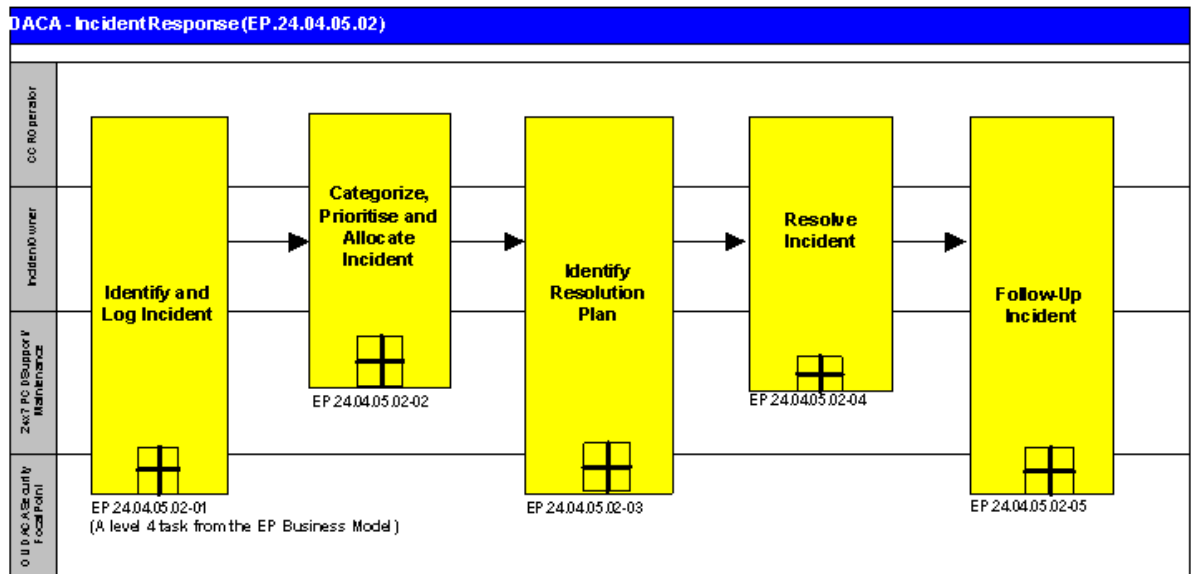


Figure 1 Manage incidents process map

The OU IT service delivery manager shall ensure that an appropriate and effective Manage Incidents procedure is in place. The 24x7 PCD support/maintenance team (a centralised help desk) shall be responsible for the day-to-day management of incidents. The level of participation for each key role is described in the following table:

Table 2 The level of participation for each key

Roles Vs Activities	24x7 PCD Support/Maint.	PCD Admin.	PCAD Admin.	CCR Operator	2 nd Line Support/ 3 rd Party	DACA Security Focal Point
Identify & Log Incident	Execute	Initiate/ Informed	Initiate/ Informed	Initiate/ Informed	Initiate	Initiate/ Informed
Categorize, Prioritise and Allocate Incident	Initiate/ Support	Execute/ Informed	Informed	Informed	Execute	Informed
Identify Resolution Plan	Support	Initiate/ Support	Initiate/ Support	Initiate/ Support	Initiate/ Support	Escalation
Resolve Incident	Support	Initiate/ Support	Initiate/ Support	Initiate/ Support	Initiate/ Support	Escalation
Follow-Up Incident		Initiate/ Execute	Support	Support	Support	Informed

6.2 IDENTIFY AND LOG INCIDENT

6.2.1 General

Objective	To provide a mechanism where all Security Incidents that are identified are reported to a central help desk, which will log the details, notify all interested parties and ensure that all incidents are addressed according to their assigned priority and SLA.
Pre-conditions	None
Considerations & decision points	When logging an incident, consideration should be given to the possibility that the incident has already been notified and logged by a different person. In this case, it would be preferable to link the 2 reports rather than create a separate incident. As soon as possible after an incident has been identified, consideration should be given as to whether or not the block manager should be activated. This decision is covered in a separate workflow ("manage block manager activation").
Tools	The applications and tools that support this process are: • E-mail • Telephone • Incident Logging and Management application (e.g. PCD Service Desk) • Block Manager functionality within the PCDP

6.2.2 Input and providers

Input data & Information	Mechanism: report, database or model	Provider(s)
Details about the incident (e.g. date/time first noticed, symptoms, impact, location, etc.).	Telephone call or e-mail	Incident Reporter
Details of other existing incidents	Data base	Incident Logging and Management application (e.g. PCD Service Desk)
Notification points	Database	Standing data within centralised help desk

6.2.3 Process map: Identify and log incident

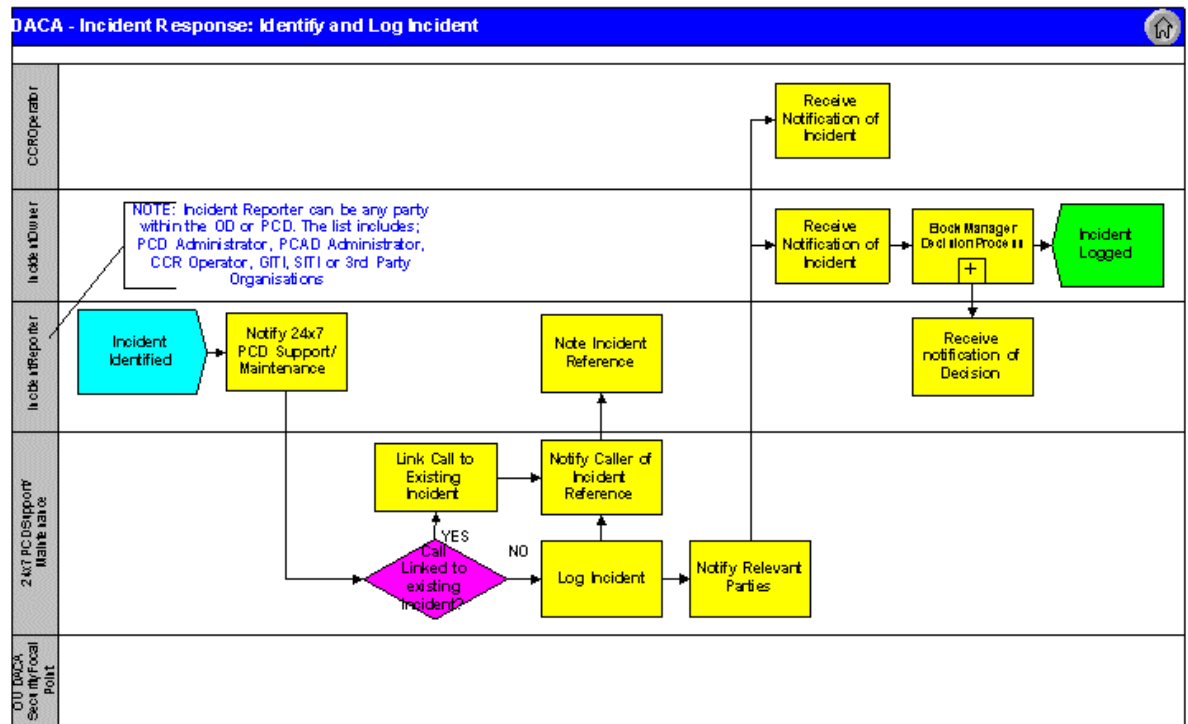


Figure 2 Identify and log incident

Comments:

- o The decision regarding the activation of the Block-Manager shall be made by the PCAD Administrator if he/she is on shift and available. If, for any reason, the PCAD Administrator is unavailable, the responsibility for making the decision shall lie with the CCR Operator.
- o When processing new Incidents, the 24x7 PCD Support/Maintenance personnel will attempt to link the call to an existing incident where appropriate. However, unless there is a high probability that the call is linked, a new incident should be created.

6.2.4 Output and customers

Output data & Information	Mechanism: report, database, model, application	Target Customer or Activity
Incident record created.	Database	24x7 PCD Support/Maintenance
Notification of Incident	E-mail	Incident Owner and CCR Operator

6.3 CATEGORIZE, PRIORITIZE AND ALLOCATE INCIDENT

6.3.1 General

Objective	To ensure that all Incidents are given an appropriate category and priority and are then allocated to the most appropriate person/team to investigate and resolve the Incident. Where possible, the incident should be contained to minimise the impact.
Pre-conditions	An Incident must have been identified and logged. There must be sufficient information to allow the Incident to be correctly allocated.
Considerations & decision points	The main consideration here is the availability of the PCD Administrator. As this role is not available at all times (i.e. not covered by a number of people working shifts) then there needs to be cover provided elsewhere when the PCD Administrator is not working. This cover must have sufficient expertise to provide this back-up role.
Tools	The applications and tools that support this process are: • E-mail • Telephone • Incident Logging and Management application (e.g. PCD Service Desk)

6.3.2 Input and providers

Input data & Information	Mechanism: report, data base or model	Provider(s)
Incident details	Database	Incident Logging and Management application (e.g. PCD Service Desk)
Technical Details re: Hardware & Software affected	CMDB (Configuration Management Database) Hardware & Software documentation Sets	PCD Administrator Hardware/Software Supplier
Support details	Standing data	Support knowledge base

6.3.3 Process map: Categorize, prioritise and allocate incident

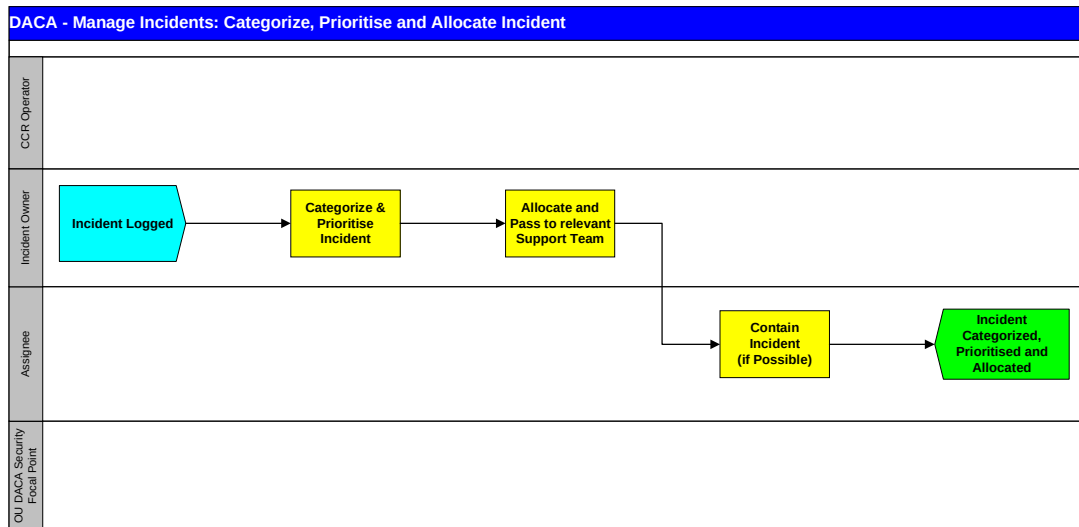


Figure 3 Categorize, prioritise and allocate incident

6.3.4 Output and customers

Output data & Information	Mechanism: report, data base, model, application	Target Customer or Activity
Updated Incident Record	Database	Incident Logging and Management application (e.g. PCD Service Desk) Assignee (Role appears in next workflow)

6.4 IDENTIFY RESOLUTION PLAN

6.4.1 General

Objective	To ensure that a method of resolving the Incident and restoring normal service is identified and planned.
Pre-conditions	An Incident must have been identified and allocated to an individual or team for resolution.
Considerations & decision points	This can be quite a complex process where Incident ownership passes from team to team as more information is gathered and the underlying cause becomes clearer. It can also require significant co-operation between teams where the cause is complex. At any one time during this process there can only be one person/team owning the resolution process (the Assignee). However, he will be able to call upon the assistance of any relevant 'Other Team' required (e.g. Vendor, SIT1, GIT1, STO, etc.).
Tools	The applications and tools that support this process are: • E-mail • Telephone • Incident Logging and Management application (e.g. PCD Service Desk)

6.4.2 Input and providers

Input data & Information	Mechanism: report, data base or model	Provider(s)
Incident details	Database	Incident Logging and Management application (E.g. PCD Service Desk)
Technical Details re: Hardware & Software affected	CMDB (Configuration Management Database) Hardware & Software documentation Sets	PCD Administrator Hardware/Software Supplier

6.4.3 Process map: Identify resolution plan

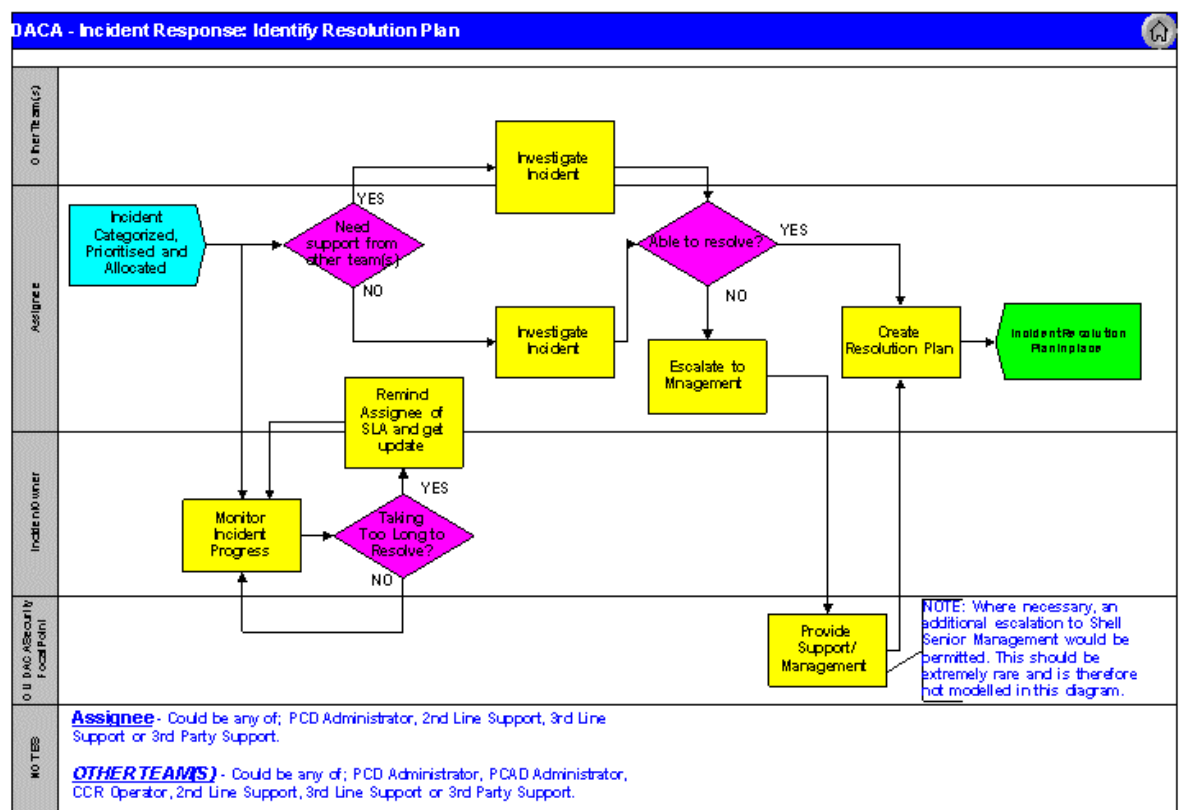


Figure 4 Identify resolution plan

Comments:

- o Consider use of 'block manager' facility as part of the restoration plan. For instance, detailed planning could be required to ensure that incorrect set points are not acted upon when the connection is restored and historical data 'catch-up' is taking place.
- o Where SLAs are about to be breached or other concerns are raised, a senior management escalation point shall be available at all times.
- o All key decisions and actions (especially changes in Incident ownership) shall be notified to the 24x7 PCD Support/Maintenance team to ensure that the central Incident Management database is kept up to date.

6.4.4 Output and customers

Output data & Information	Mechanism: report, data base, model, application	Target Customer or Activity
Detailed Restoration plan	Report	Assignee
Updated Incident Record	Database	Incident Logging and Management application (e.g. PCD Service Desk) Assignee

6.5 RESOLVE INCIDENT

6.5.1 General

Objective	To carry out the finalised resolution plan to restore normal operation of the PCD and PCAD.
Pre-conditions	A fully detailed resolution plan must have been created and agreed.
Considerations & decision points	Before an Incident can be considered closed, it shall be confirmed with one or more of the original Incident reporters that the issue has, in fact, been resolved. Where the number of reporters is small, all should be contacted. However, if the number is large – a sample check is acceptable.
Tools	The applications and tools that support this process are: • E-mail • Telephone • Incident Logging and Management application (e.g. PCD Service Desk) • Various IT tools and techniques

6.5.2 Input and providers

Input data & Information	Mechanism: report, data base or model	Provider(s)
Detailed Restoration Plan	Report	Assignee

6.5.3 Process map: Resolve incident

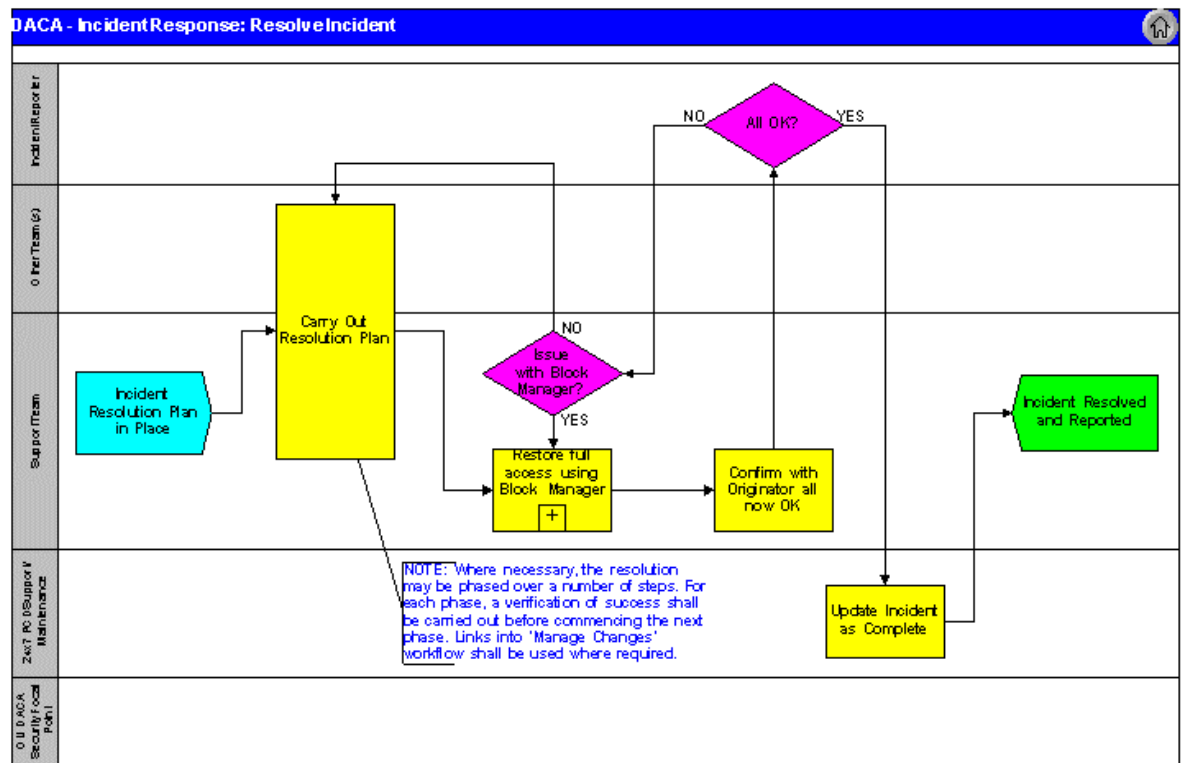


Figure 5 Resolve Incident

Comments:

- o In reality, the 'Restore full Access using Block Manager' activity may be embedded within the 'Carry Out Restoration Plan' activity, as there may be restoration activities either side of the action to restore access. However, it is shown here as a separate task to ensure that the use of Block Manager is considered within the overall workflow rather than to show it happening at a definite stage within the procedure.
- o All key decisions and actions (especially confirmations that all is now OK) shall be notified to the 24x7 PCD Support/Maintenance team to ensure that the central Incident Management database is kept up to date.

6.5.4 Output and customers

Output data & Information	Mechanism: report, data base, model, application	Target Customer or Activity
All systems operating as normal.	Database	Incident Logging and Management application (e.g. PCD Service Desk)

6.6 FOLLOW-UP INCIDENT

6.6.1 General

Objective	To review certain incidents to see if any follow-up activity (i.e. Lessons Learned exercise, HSSE Reporting or IT Security Incident Reporting) is required and to carry out such activity
Pre-conditions	An incident has occurred and been resolved. All appropriate details pertaining to the incident (e.g. the investigations carried out, the resolution/mitigation actions taken, etc.) are available.
Considerations & decision points	High-impact incidents and a sample of all other Incidents shall be reviewed to see what (if any) lessons can be learned to either prevent a recurrence or to handle a future occurrence more efficiently. Where this lessons learned activity identifies a potential mitigation activity, this could be linked to the "manage changes" workflow.
Tools	The applications and tools that support this process are: • E-mail • Telephone • Incident Logging and Management application (e.g. PCD Service Desk) • Various IT tools and techniques

6.6.2 Input and providers

Input data & Information	Mechanism: report, data base or model	Provider(s)
Incident details	Database	Incident Logging and Management application (e.g. PCD Service Desk)

6.6.3 Process map: Follow up incident

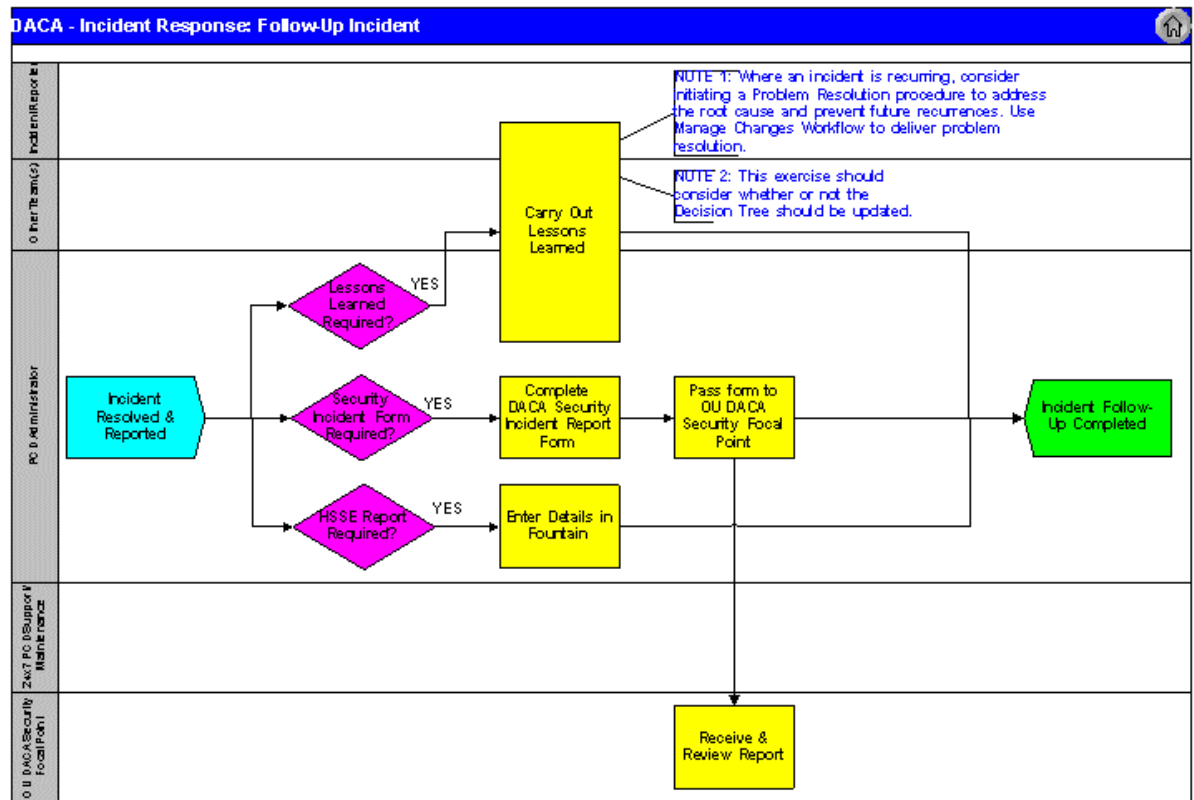


Figure 6 Resolve Incident

Comments:

- o The "lessons learned" exercise may result in other follow-up actions not modelled here because they will be carried out by means of the "manage changes" workflow.
- o Follow-up actions taken by the OU DACA Security Focal Point are not modelled here because they are likely to be the result of reviewing a number of incident reports rather than resulting from a single incident. In any case, the follow-up actions should be initiated by means of the Manage Changes workflow.

6.6.4 Output and customers

Output data & Information	Mechanism: report, data base, model, application	Target Customer or Activity
Lessons Learned Report	Report	PCD Administrator
HSSE incident report	Fountain	HSSE
Security Incident Report	Form	OU DACA Security Focal Point

7. REFERENCES

In this DEP, reference is made to the following publications:

- NOTES:
1. Unless specifically designated by date, the latest edition of each publication shall be used, together with any amendments/supplements/revisions thereto.
 2. The DEPs and most referenced external standards are available to Shell staff on the SWW (Shell Wide Web) at <http://sww05.europe.shell.com/standards/>.

Amended per
Circular 60/07

SHELL STANDARDS

DACA - Roles & Responsibilities	DEP 32.01.21.10-Gen
IT4S Incident Management Policy	ITCI 051
IT4S Incident Management Standard	ITCI 052
Information Security Standard For PCADs & PCDs	ITCI 117