



INCIDENT MANAGEMENT IN A SHARED SUPPLIER ENVIRONMENT »

White Paper

Written by Sue Bullock, Atos Origin, Professional Services

Contents

INTRODUCTION	3
1 THE ISSUE	4
2 HANDLING INCIDENTS IN A SHARED SUPPLIER ENVIRONMENT	5
3 DEVELOPING JOINT INCIDENT MANAGEMENT PROCESSES	6
3.1 A service definition blueprint	6
3.2 Assessment of key assumptions	7
4 IMPLEMENTING JOINT INCIDENT MANAGEMENT PROCESSES	8
5 A MAJOR INCIDENT MANAGEMENT PROCESS	9
5.1 The key steps of shared Major Incident support	10
CONCLUSION	11

Introduction

MANY ORGANISATIONS DEPENDING HEAVILY UPON THEIR IT HAVE SUCCESSFULLY FORMULATED A SERVICE MANAGEMENT STRATEGY THAT DEFINES THE QUALITY OF IT SUPPORT AND SERVICE FOR THE BUSINESS. OVER TIME, THIS CAN LEAD TO VARIOUS IT SERVICE CONTRACTS BEING SUPPLIED BY DIFFERENT (AND OFTEN COMPETING) SPECIALIST IT OUTSOURCERS. THE RESULT IS FRAGMENTED, NON-COHESIVE IT SUPPORT FOR THE PEOPLE WHO USE THE SERVICES, ALONG WITH THE ADDED BURDEN ON MANAGEMENT TEAMS OF COORDINATING AN END-TO-END SERVICE FOR A NON-CORE BUT BUSINESS CRITICAL AREA.

Most service delivery strategies are based on the CCTA IT Infrastructure Library (ITIL), which is now recognised as the standard for service management. But that fact comes with a crucial caveat. The interpretations and subsequent development of the guidelines provided by ITIL into support and delivery processes can differ widely between providers, even where the end result – for example a resolved Incident – may be the same.

This situation raises an important question. How can such inconsistent and varied ITIL-based services be jointly applied to meet an organisation's strategic needs and effectively support genuinely mission-critical IT systems?

Answering this question, through the implementation of practical measures, is particularly complicated when more than one supplier organisation is involved, and where each agreement in place has its own service levels, recording systems, processes, responsibilities and communication methods. Not only may down-time incur significant costs, but can a business be confident that its existing processes are capable of productively engaging with suppliers to resolve Incidents in the right way, and as efficiently as possible, in such a high-pressure environment?

This White Paper looks at the change of approach needed to effectively manage both Incidents and Major Incidents in a shared supplier environment. The Paper uses a real case study to highlight examples of effective end-to-end service management in a shared supplier contract that comprises two competitor IT outsourcers.

1 The issue

In any large organisation, how many mission-critical IT services are dependent on more than one supplier but are not covered by a single support contract? It is likely to be a significant number, in this Paper we will look at the special processes needed to deal with Incident Management across a shared supplier base, in order to ensure seamless support for IT services.

The processes are based on ITIL principles throughout, but they have been extended to deal with the special requirements of shared suppliers' service alignment. We will be using examples from the case study to demonstrate how new processes have been developed in a shared support, and multi-location, environment.



2 Handling Incidents in a shared supplier environment

What happens when an Incident such as an IT systems outage occurs? Almost certainly a Help Desk (or Service Desk, which is the term used in this Paper) will receive details of the Incident, usually by phone. The Service Desk will attempt to pass on the Incident details to a technical resolution group (a phrase from ITIL terminology).

In a shared supplier organisation, it is vital that the Service Desk has been notified of each and every change to the IT support system, as changes occur. Otherwise, the Service Desk may be presented with logging details of an Incident they know nothing about – what information to capture, who to assign it to, how critical that Incident is – and at the very first hurdle, the Incident resolution process breaks down.

Assuming the Service Desk is able to pass on sufficient details to the correct technical resolution group, they will then assess the Incident and try to resolve it according to the service level in place. This is a perfectly reasonable response by the group – but it begs a question.

How will this process stand up in a mission-critical environment when the following is taking place?

- > There are alternative Service Desks to call, depending on the nature of the Incident (has each Service Desk that needs to be updated been notified about all relevant IT changes?)
- > More than one Service Level Agreement (SLA) applies
- > Each Service Desk is swamped by calls from a large number of angry business users who are complaining about the huge impact the Incident is having, whilst demanding to know when the service will return to normal?

Not only are such Incidents very stressful, they're also infectious. And once infection sets in, service management processes tend to be forgotten in the panic that ensues, which may result in unnecessary delays and the wrong people being involved, adding to the confusion and, ultimately, the cost of resolving the Incident.

3 Developing joint Incident Management processes

The implications of successfully dealing with an Incident in the example in section 2 are such that IT services delivered by more than one supplier require special consideration – whether an Incident be run-of-the-mill or a major event.

Simple Incidents often only relate to a single service, and hence a single supplier of that service. But major or complex Incidents, which have an impact on a larger range of linked IT services, often require direct involvement from more than one support area. They will need input from each organisation that delivers a service. Incidents involving more than one supplier therefore need all the parties involved to work together to achieve rapid response, effective and timely escalation, and excellent shared communications. That's the necessary solution-mix for avoiding the 'bouncing call' syndrome.

Our experience suggests that the normal service management processes (which relate to a single service provider) are simply not good enough for managing such shared services. The company in our case study recognised that the special nature of the interfaces and close working required to resolve Incidents means that new processes must be developed. Processes capable of dealing with the way in which different service providers interface and work together in order to ensure there is no impact (or minimum impact) upon their shared customer when an Incident occurs.

A key customer requirement is for suppliers to collectively develop a cohesive one-stop-shop Incident Management process for the end-user community. This demands that two requirements are met. The first is a single-point-of-contact for all Incidents. The second is a single recording mechanism for Incidents, from which reports can accurately and comparatively be extracted for each of a suppliers' services.

In the case study, a single Service Desk was established with one supplier for all IT Incidents. The desk comprises the necessary tooling and associated reporting capability and is staffed by first-line support analysts trained in the initial assessment of calls for each of the suppliers' services. Analyst training is further refined by question and answer scripts provided and maintained by each supplier's own technical specialists.

For cohesive working it is clearly important to understand each supplier's language and service touch points, from initial notification of an Incident to how a supplier then engages in Incident resolution and completes a Service Desk phone call. An initial service management framework was therefore established so that any areas of conflict and inconsistency in customer service could be identified and captured. For that to be achieved, it was necessary to share information on the following services in order to form a service definition blueprint.

3.1 A SERVICE DEFINITION BLUEPRINT

Description

- > Title and brief description of the overall service provided by a contributing supplier
- > Dates: start, end, review
- > Scope of the service; what is covered and what is excluded
- > Responsibilities of external contributors to the service (touch points).

Service hours

- > The hours that the service is normally provided (e.g. 24x7, Monday to Friday 08:00 – 18:00)
- > Arrangement for requesting service extensions, including required notice periods (e.g. request must be made to the Service Desk by 12 noon for an evening extension, by 12 noon on Thursday for a weekend extension)
- > Special hours (e.g. public holidays)
- > Service calendar.

Availability

- > Availability targets for the service within agreed hours, normally expressed as percentages
- > Measurement period and method for calculating availability (this may be expressed for the overall service, underpinning services and critical components, or all three)
- > Service 'unavailability' measures, in terms of the customer's inability to carry out its business activities.

Support

- > Support hours (where these are not the same as service hours)
- > Arrangement for requesting support extensions, including required notice periods (e.g. request must be made to the Service Desk by 12 noon for an evening extension, by 12 noon on Thursday for a weekend extension)
- > Special hours (e.g. public holidays)
- > Target time to respond to Incidents, either physically or by other method (e.g. telephone contact, email)
- > Target time to resolve Incidents, within each Incident priority – targets vary depending upon Incident priorities
- > Contact details to log Incidents, and scope of Incident Support provided for this service.

Change

- > Processes to apply and targets for approving, handling and implementing Requests for Change, usually based upon the category or urgency/priority of the change
- > Any Change Control function such as a Change Advisory Board, including the make-up of the Board and areas of responsibility.

IT service continuity and security

- > A brief mention of IT Service Continuity Plans and how to invoke them, and coverage of any security issues, particularly any responsibilities of the customer (e.g. back-up of freestanding PCs, password changes)
- > Details of any diminished or amended service targets should a disaster situation occur (if no separate SLA exists for such a situation).

Service reporting and reviewing

- > The content, frequency and distribution of service reports, and the frequency of service review meetings.

3.2 ASSESSMENT OF KEY ASSUMPTIONS

As already noted, suppliers need to share information in order to create and sustain a cohesive Incident response and resolution service. But this also needs to be achieved without compromising each supplier's commercial confidentiality. The solution is to look at each supplier's key assumptions and Incident Management interfaces and then compare them for consistency.

For the case study company, some of these assumptions were relatively simple to agree, and these formed the core of the initial shared Incident Management process. Others required a more detailed study before they could be integrated at a later date.

The key interfaces together with an assessment of how difficult they were to agree is summarised in Figure 1 below.

FIGURE 1: KEY INTERFACES AND ASSESSMENT OF DIFFICULTY

ASSUMPTION	AGREEMENT DIFFICULTY	ACTION
Single-point-of-contact for any Incident will be enabled and supported for end-users, and a subsequent single contact point provided by each supplier	Quick win	Single number allocated and Incident Manager role allocated within each supplier organisation
Communication of the status and progress of Incidents will be supported between the Service Desk, suppliers and the user community	Quick win	Develop a shared comms strategy
The content of any form of message issued by the Service Desk will be precise and 100% accurate to avoid loss of respect by the user community	Medium	Service Desk messages would require authorisation from relevant supplier's Service Manager
The Service Desk will need to learn much more about each supplier's services and any jargon they use if it is to be taken seriously by the user community	High	Re-engineer Service Desk role, resources and supplier-specific training
All automated monitoring systems for events, alerts and Incidents will have a notification interface point to Lead Supplier systems for initiating the Incident process, logging details in Service Desk tooling and ensuring the end-to-end management and progression of the Incident to Incident closure	High	Integrate systems monitoring tooling alerts into central 'Manager of Managers' system and link to Service Desk tooling
Agreement on membership and scope of any shared Boards (Change Advisory Board, Major Incident Team)	Quick win	Agree terms of reference and scope of responsibility for members of Process Board

4 Implementing joint Incident Management processes

The transition of the Incident Management service from multiple suppliers to a shared supplier environment is experienced as a benefit by the user community because they now have a single contact point providing comprehensive expertise. Previously, users had to self-manage multiple numbers or people to contact for a wide range of possible Incidents. For the supplier community, effective communication with first-line support is the key to successfully providing user support. But for a comprehensive and fully-integrated Incident Management service, cross-training between specialists and the Service Desk is also needed. The training fulfils three important and linked criteria:

- > It provides an understanding of the needs to be met by all parties during initial contact by users
- > It ensures that the Service Desk understands, and can ask for and deliver, the information required by second or third-line support specialists to resolve an Incident
- > And it also ensures that second and third-line staff understand how the Service Desk tooling works.

This last point includes items such as which fields are mandatory and how they need to be used, how SLA time monitoring is applied through automation, and how to populate tickets with further information gathered during the lifecycle of an Incident.

Once this knowledge sharing is completed, there needs to be a clear mechanism in place to maintain the new relationship, including regular knowledge updates, to facilitate ongoing development and promote qualitative service improvement.

Joint service reporting and a unified service management review function will ensure that the cohesiveness of the service is maintained. Training for staff in the joint processes and any shared tooling, with a focus on the interfaces and communications between suppliers, is a key deliverable of the implementation phase.



5 A Major Incident Management process

Major Incidents often impact more than one area of technology within IT – causing the biggest headaches when trying to coordinate solutions, especially for the users suffering the IT outage. The principal area of difficulty is the effective coordination of communication and technical team interfaces, because problems quickly escalate in a high pressure situation.

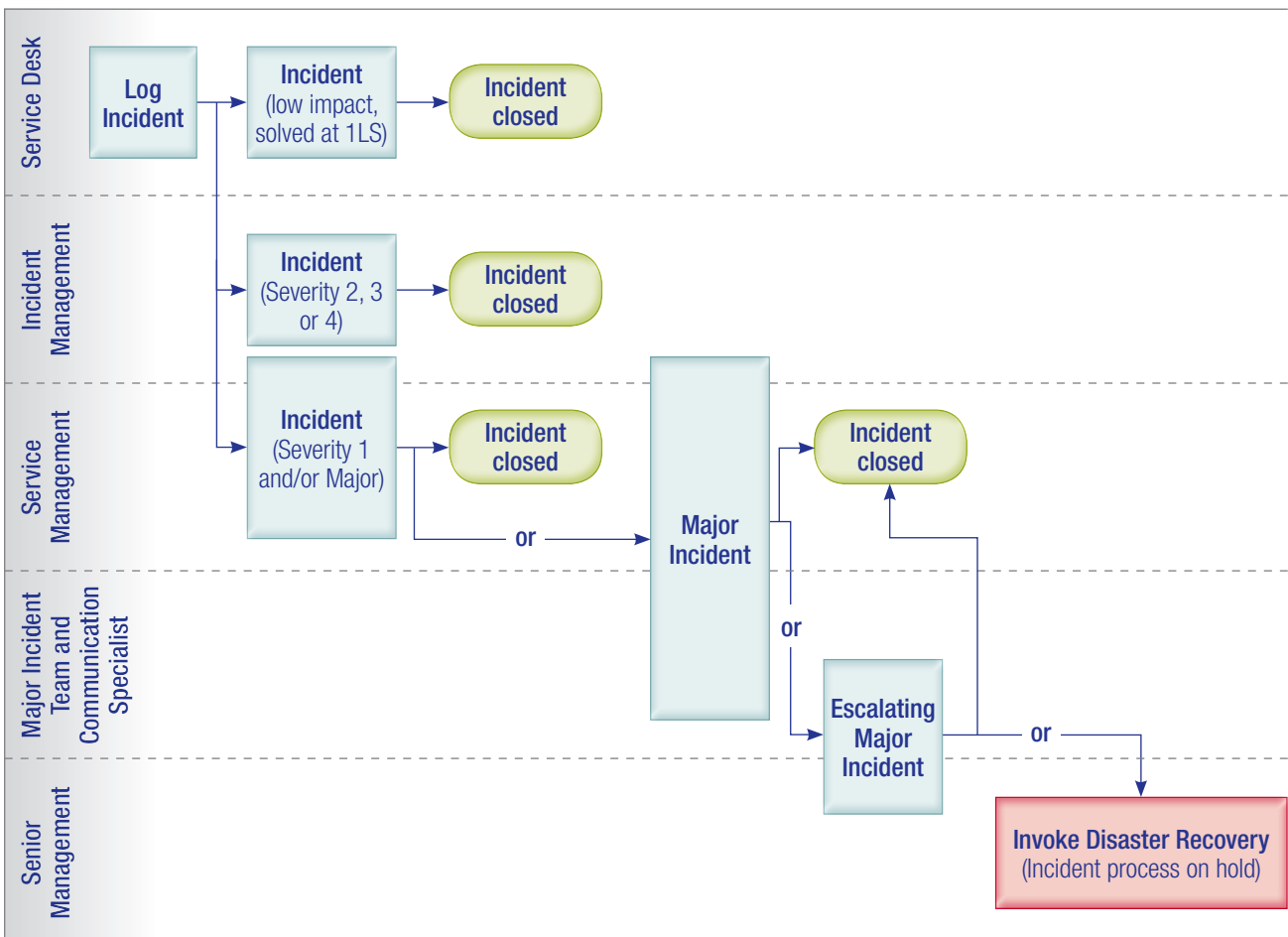
An Incident can start as a simple matter, able to be directly addressed by first-line support. But it may also be the first indication of a larger evolving problem that develops rapidly into a major organisational issue. The diagram below shows the route taken by an escalating Incident through the organisational structure, from an Incident closed at first call to an extreme case scenario in which initial logging of the Incident escalates to invoking Disaster Recovery for the service.

Major Incident Management plays a pivotal role in successfully managing escalating Incidents across supplier organisations. Its purpose is to:

- > Coordinate the solution process across the organisations as necessary
- > Streamline communications to the impacted customer/s via a single-point-of-contact
- > Streamline communications within the support organisation, where a lot of teams are involved and all staff need to know who is doing what and how Incident resolution is progressing
- > Act as a focal point for the customer to instigate Major Incident Management, by contacting Senior Management at the Lead Supplier.

FIGURE 2: INCIDENT TYPES AND EVOLUTION OF A MAJOR INCIDENT

Accountable role is the lower of the rows involved in a particular Incident type
Responsible role is the row above the Accountable role



A Major Incident Team

The purpose of establishing a Major Incident Team is two-fold:

- > To minimise the time it takes to resolve an Incident by getting representatives of all applicable competencies together, and thereby facilitating coordinated decision-making and management of the solution process. Representatives must have a sufficient level of authority to both decide and enact on behalf of their business
- > To give the customer and support organisations the opportunity to prevent or minimise business losses as early as possible; the main factor being good communication between all relevant parties regarding the resolution process and its anticipated duration.

5.1 THE KEY STEPS OF SHARED MAJOR INCIDENT SUPPORT

Shared supplier organisations need to adopt a strategy that puts a Major Incident Team in place, ready to be 'activated' as soon as a Major Incident occurs. Overall, there are four steps or phases. The first is:

1. Appoint Major Incident Team Personnel

The Lead Supplier Service Delivery Manager, in agreement with the service directors for the supplier organisations, decides who should be involved in the Major Incident Team. The decision is based on which stakeholders need to be kept informed, their contractual knowledge of the services and any additional information provided at the time. The single cross-supplier Major Incident Team Manager and the Major Incident Team will be appointed and convene to agree next steps and shared strategy. Each supplier and the customer organisation are represented within this team, by members authorised to provide sufficient resources, as required, to resolve an Incident. When an Incident actually occurs, there are then two phases to be managed by the Major Incident Team:

2. Oversee communications and resolution activity

During this phase, the Major Incident Team will manage both communications and Incident resolution for all suppliers. Communications activity includes planning communications, deciding who needs to receive what level of messages, and delivering to the plan so that all stakeholders are informed appropriately. In the meantime, the Major Incident Team will be utilising any necessary resources at its disposal – human and technological – to ensure a rapid and effective solution is found and applied for any given Incident.

3. Closedown of Major Incident

This phase includes performing final communications and handing over control of any outstanding activities to Incident Management. In this phase it will also be decided how the post-Major Incident review should be managed, either using Problem Management processes, or by an independent review. The Major Incident Team will then be disbanded – allowing them to return to their normal activities – until they are required to manage the next Major Incident.

Finally, the last phase is:

4. Post-Major Incident review and wash-up

This is where lessons learned are gathered, reviewed, captured and shared for future reference.

Conclusion

The challenge of maintaining a high-performance partner and supplier network is not limited to organisations or situations with special IT requirements; it's a challenge that must be addressed and solved by businesses in every area of industry and commerce as well as the Public Sector. In fact, most organisations have numerous supplier relationships, some of which are likely to be better managed than others from a risk and Business Continuity perspective.

A key requirement for suppliers to work together is an agreed agenda based on information that is common to all parties. The core elements of this approach are a shared document management system and a set of associated workflow processes. Every supplier, and the customer, must work in mutual consultation to agree the parameters and procedures for successful joint Incident response and resolution. Once agreed, everyone then works from the same approved documents and through the same workflow processes.

The philosophy that underpins this approach applies to both Incident and Major Incident resolution. The purpose is to make sure that errors are not duplicated across different areas of responsibility. A traditional service management approach will not solve the error duplication problem. Truly effective solutions must be based on a philosophy and practice of open and understood joint-working.

Key areas that need to be developed are the role of the Service Desk and the processes for handling shared Changes, Incidents and Major Incidents. Rigorous Problem Management and excellence in communications with the customer require time to mature – but they must be strived for if IT is to be held in high regard by the business.

The case study company benefited significantly from such processes; service users are more satisfied with the support they receive, the consistency of support across suppliers is apparently seamless and the availability of key systems has improved.

For any business, the true test of excellence in service management is how well the organisation responds when that unexpected but inevitable service change, or end-user difficulty, comes along. In a shared supplier IT environment, putting the right joint working, single contact response and resolution processes in place is the foundation for achieving and sustaining excellence that brings real benefits to everyone utilising the IT services.

ABOUT ATOS ORIGIN

Atos Origin is an international information technology services company. Its business is turning client vision into results through the application of consulting, systems integration and managed operations. The company's annual revenues are EUR 5.8 billion and it employs over 50,000 people in 40 countries. Atos Origin is the Worldwide Information Technology Partner for the Olympic Games and has a client base of international blue-chip companies across all sectors. Atos Origin is quoted on the Paris Eurolist Market and trades as Atos Origin, Atos Worldline and Atos Consulting™.

Atos Origin
4 Triton Square
Regent's Place
London NW1 3HG
Tel: +44 (0)20 7830 4444

Advance with Atos Origin - for business and IT in harmony

www.atosorigin.co.uk