

Technology Service Incident Classification and Communication Standard

Abstract

This document defines how providers of technology services should communicate with their BBC customer stakeholders in the event of any major disruption to the normal delivery of their services.

This standard is applicable to both internal and external service providers.



<i>Reference</i>	SA2 -1001 DQ main_05
<i>Version</i>	1.0
<i>Status</i>	Approved
<i>Date</i>	01/04/2011

Change History

Ver	Date	Change	Author
0.1	26/11/2010	Initial draft	Roger Shakeshaft
0.2	07/12/2010	<p>7. Definitions added for Problem and Known Error</p> <p>11.1: Consultation with BBC Duty Manager added prior to issuing of Incident Alert</p> <p>11.1 Known Error statement added to Incident Alert</p> <p>11.4 Consultation with BBC Duty Manager added prior to issuing Service Restoration Notice</p> <p>A.1 Abbreviated TFC service names used instead of CSR codes</p> <p>E.1.1 Incident Alert SMS template changed</p> <p>E.2.1 Service Restoration Notice SMS template changed</p>	Roger Shakeshaft
0.3	15/12/2010	<p>Sections 1, 2, 3 and 4 restructured</p> <p>2.1 Major Incident definition revised and cascade down to Provider-specific guidelines added</p> <p>4. Service Warning product added to Incident Lifecycle</p> <p>5.1 Service Warning requirements added</p>	Roger Shakeshaft
0.4	16/10/2010	Annexes E to H re-sequenced	Roger Shakeshaft
0.5	17/10/2010	<p>Annex E Renamed to Communication Modes</p> <p>Annex F Distribution list added for Service Warning</p> <p>Annex G Renamed to Format Specifications</p> <p>Annex H Renamed to Communication Examples</p>	Roger Shakeshaft
0.6	05/01/2011	<p>Typographic errors in cross-references corrected</p> <p>2.3 Exclusions redefined</p> <p>5.2 to 5.6 Incident reference number added to all Incident Communication Products</p> <p>5.6 Post Incident Report requirements redefined</p> <p>5.8 Problem Closure Report requirements redefined</p> <p>Annex G This annex (formerly Format Specifications) removed as Communication Product templates now held and maintained separately by Service Assurance</p>	Roger Shakeshaft
0.7	27/01/2011	<p>4 Criteria changed for when an Incident Briefing is issued</p> <p>5.5 Service Restoration Notice requirements redefined</p> <p>5.6 Post Incident Report requirements redefined</p> <p>5.8 Problem Closure Report requirements redefined</p>	Roger Shakeshaft
0.8	22/02/2011	<p>4 Updated lifecycle to include Incident Closure product</p> <p>5.1 – 5.8 Added “distributed to” requirement to Communication Products</p> <p>5.5 Added requirement to briefly outline what was done to restore service</p> <p>5.2 Added requirement to name incident</p> <p>5.4 Updated “Affect on Service Level Agreements (none; unknown; breached; impacted)”</p> <p>5.5 Updated “advise whether the Service was restored by fix, workaround, self-restore, other</p> <p>5.6 Added new Incident Closure product and re-numbered</p> <p>Annex B Updated to present P1 and P2 in red font</p> <p>Annex C Deleted 2 codes</p> <p>Annex D Added 2 area codes</p>	D Organ

		Annex G Updated all templates	
0.9	24/02/2011	Contents Updated page number references Annex D Added "International" affected area code	
1.0	01/04/2011		

Foreword

This document is owned, reviewed and maintained by the Incident Management Forum.

This forum is chaired by BBC Service Assurance and is comprised of stakeholders from both service providers and service recipients.

This edition cancels and replaces all prior versions of the standard.

This is a controlled document. It can be referenced, but not reproduced, in other documents and its terms may be used for contractual definitions.

This page intentionally blank

Contents

	Page
1 Introduction	8
1.1 Background	9
1.2 Application	9
1.3 Terms and Definitions	10
1.4 Conventions	10
1.5 Normative References	10
2 Scope	12
2.1 Major Incident Definition	12
2.2 Major Incident Guidelines	13
2.3 Exclusions	13
3 Incident Classification	14
4 Incident Lifecycle Model	14
5 Communication Products	16
5.1 Service Warning	16
5.2 Incident Alert	17
5.3 Incident Update	17
5.4 Incident Briefing	18
5.5 Service Restoration Notice	18
5.6 Post Incident Report	19
5.7 Problem Update	21
5.8 Problem Closure Report	21
6 Management Responsibilities	23
Annex A - Service Codes	25
Annex B - Severity Codes	26
Annex C - Impact Type Codes	27
Annex D - Affected Area Codes	28
Annex E - Communication Modes	29
Annex F - Service Stakeholders	30
Annex G - Communication Product Examples	30

This page intentionally blank

1 Introduction

This standard defines an information interface between the BBC customers and users of technology services (**Service Stakeholders**) and the service providers (**Providers**).

This interface has been standardised in order to ensure Providers communicate effectively with their Service Stakeholders in the event of that any major disruption occurs in the delivery of their service or services.

This standard is built around a notional **Incident Lifecycle Model** to enable the BBC's information requirements (expressed as Communication Products) to be mapped onto the Provider's existing incident and problem management processes (see below).

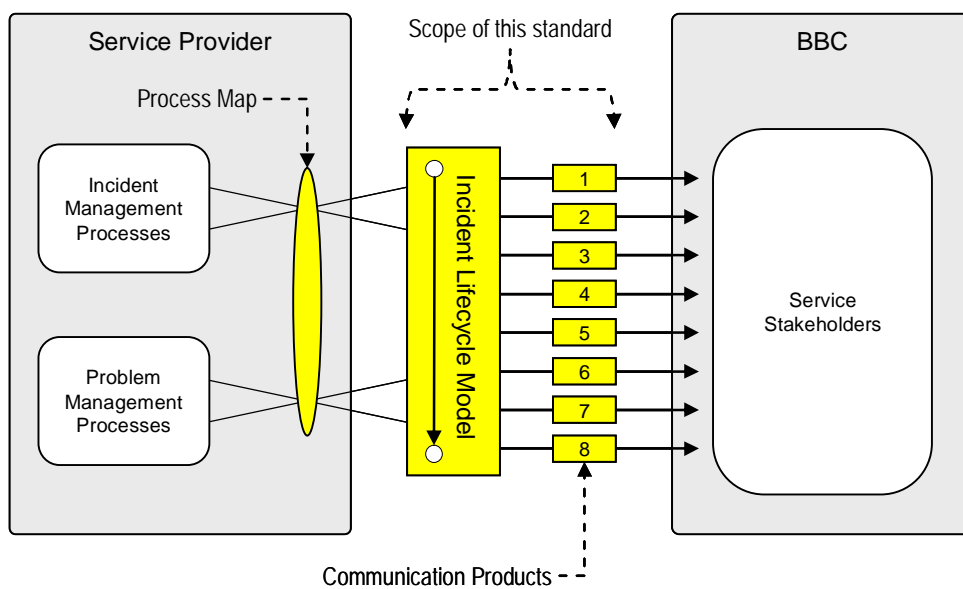


Fig 1 - Mapping BBC information requirements onto Provider processes

The standard is intended to benefit the BBC by:-

- reducing the impact of major incidents through effective communication
- reducing the risk of major incidents through better visibility of problem management
- enabling incident-related performance benchmarking across dissimilar services through standardised coding and classification
- standardising business-critical communications across multiple providers
- providing the basis for continuous improvement

The standard is intended to benefit the Provider by:-

- reducing ad-hoc demands for information from Service Stakeholders during major incidents and enabling resolver resources to focus on service restoration
- minimising the impact that service disruptions have on valued customers

1.1 Background

The BBC relies upon a diverse range of technology services, from both internal and external providers, in order to operate effectively and fulfil its Public Purposes.

This reliance means that the BBC's operation, output, staff and partners can experience business impact should any significant disruption (major incident) occur to these services.

The level of business impact experienced during such disruptions can be greatly affected (positively or negatively) by the quality of stakeholder communication during the service restoration (incident management) process.

Service Stakeholders will include those charged with the responsibility of maintaining business continuity throughout service disruptions and the quality of the decisions they make will directly link to the quality of information they receive from the Provider who is working to restore normal service.

For example, if continuity stakeholders are aware that the provider is confident that service will be restored soon then they may elect to take no action and simply wait for restoration thus avoiding the cost and further disruption that could be incurred by invoking disaster recovery plans.

Conversely, if continuity stakeholders are aware that the provider is not confident of a speedy service recovery then they may avoid wasting valuable time by invoking disaster recovery plans sooner rather than later.

The requirements defined in this standard are intended to minimise the impact that major technology service disruptions have on the BBC by improving the effectiveness of service provider communications during such events.

1.2 Application

This standard shall be applied to the operational interface between the BBC and any Provider (internal or external) where there is a risk that any disruption to normal service delivery may significantly impact upon the Corporation's ability to function.

Once conformity with this standard has been attained, then the Provider shall maintain compliance until Provider's tenure as a service provider ends or until formal dispensation is granted by the BBC, whichever is the sooner.

1.3 Terms and Definitions

BBC Duty Manager:	BBC post with ultimate responsibility for the operational aspects of a business area e.g. News Duty Broadcast Duty Manager (BDM), Operations Manager (DOM), Duty Facilities Manager (DFM), etc.
Incident:	See definition of Major Incident in Scope (see 2.1)
Problem:	The unknown underlying cause of one or more Incidents
Known Error:	A Problem that has been successfully diagnosed and for which a workaround is in place Note: A workaround may provide a long term solution to a Known Error in the event that a permanent resolution is deemed economically unviable Note: Incidents caused by Known Errors should be specifically tracked as this information may inform the case for investing in permanent solutions to Problems
Service Client:	The person/s acting on behalf of the BBC as formal customer of the Provider's service or services
Service User:	Any party who makes use of the Provider's service and who is competent to determine when it has been restored to normal operation following an Incident
TFC:	The (Siemens) Framework Contract

1.4 Conventions

The following conventions have been used throughout this document to aid readability.

All references to:-

- "Incident" should be read as "Major Incident"
- "Problem" should be read as "Major Problem"
- "Service" should be read as "Service or Services"

The terms "Major Service Disruption" and "Major Incident" are used interchangeably.

1.5 Normative References

This document makes reference to content within the following associated sources.

Source	Owner
Business Continuity Architectural Characteristics	Architecture Council
TSI Communication Distribution Lists	Service Assurance
TSI Communication Templates	Service Assurance

This page intentionally blank

2 Scope

This standard defines the BBC's requirements for:-

- incident and problem information in the form of Communication Products
- the format, delivery modes and recipients of Communication Products
- the classification and coding of major incidents
- specific management responsibilities within the Provider's organisation

This standard is only applicable to Major Incidents.

2.1 Major Incident Definition

A **Major Incident** is defined as:-

“an instance where a service disruption impacts the BBC's operation to such an extent as to warrant the application of all reasonable endeavours to restore normal service and to ensure that the BBC is not impacted again by subsequent disruptions with a common root cause.”

Note: To comply with this definition a Provider may respond to an Incident by identifying and eliminating its root cause or, where this is not viable, by putting in place arrangements that limit the impact on the BBC to the same extent as would be achieved by elimination of the root cause.

This definition of Major Incident is intended to map onto Provider-specific guidelines as shown below.

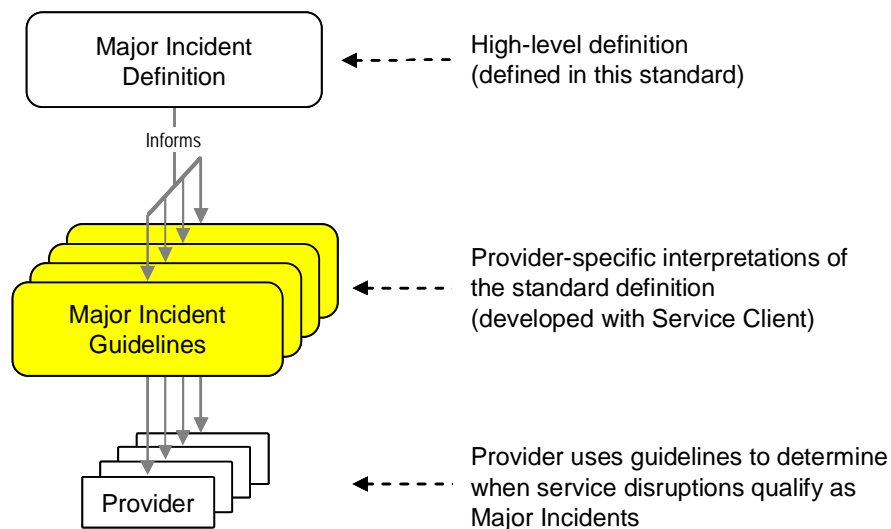


Fig 2 - Mapping the Major Incident definition onto Provider-specific guidelines

2.2 Major Incident Guidelines

The Provider shall develop and agree with the Service Client the Major Incident Guidelines that shall be used operationally to determine when service disruptions qualify as Incidents.

The Provider shall document and maintain these guidelines and shall review them with their Service Client on a regular basis to ensure their on-going effectiveness.

2.3 Exclusions

In the event that control of an Incident is appropriated by BBC management (such as a Silver or Gold Command Team in a business continuity scenario) then this standard may not apply.

In such circumstances the Provider shall seek and comply with BBC management instructions with regards to Incident communications.

3 Incident Classification

The Provider shall ensure that every Incident is classified in terms of:-

- the service that has been disrupted
- the severity of the impact on the BBC
- the type of impact experienced by the BBC or its audiences
- the BBC business areas and/or output channels that have been affected

Should an Incident be re-classified during its lifecycle then the Provider shall advise of the new classification (and the reasons for it) in the next communication that is issued.

Where the Incident impacts, or is at risk of impacting, areas within the operational remit of a BBC Duty Manager then the Provider shall immediately brief said manager and agree with them, how the incident shall be classified and described before the first communications are issued.

4 Incident Lifecycle Model

The Incident Lifecycle Model provides the structure for defining the BBC’s information requirements throughout the life of an Incident, from detection through service restoration and on to elimination of root cause.

The model takes the form of a series of key milestones within the Provider’s incident and problem management processes against which are defined the BBC’s information requirements in the form of Communication Products (see below).

Milestone	Milestone Definition	Communication Requirement
1	Tangible risk of major service disruption (Incident) occurring	The Provider shall issue a Service Warning as per requirements in 5.1
2	No longer a risk of major service disruption	The Provider shall issue a Stand Down notice as per requirements in 5.1
3	Major service disruption detected and confirmed (Incident opened)	The Provider shall issue an Incident Alert as per requirements in 5.3
4	Service not yet restored and update now due as stipulated in Incident Alert or previous Incident Update	The Provider shall issue Incident Updates as per requirements in 5.4
5	BBC management request that an Incident Briefing be issued	Provider shall issue an Incident Briefing as per requirements in 5.5
6	Service restored	Provider shall issue a Service Restoration Notice as per requirements in 5.6
7	Incident closed (following a period of monitoring for sustained normal operation)	Provider shall issue an Incident Closure Notice as per requirements in 5.6
8	Sufficient information has been gathered to produce conformant Post Incident Report (as per 5.8) or when required by applicable service levels, whichever is the sooner (Incident closed and Problem opened)	Provider shall issue a Post Incident Report as per requirements in 5.8
9	At weekly intervals while Problem remains open	Provider shall issue a Problem Update as per requirements in 5.9
10	Corrective and/or preventive actions completed and their effectiveness verified (Problem closed)	Provider shall issue Problem Closure Report as per requirements in 5.10

Fig 3 - Incident Lifecycle Model

5 Communication Products

Communication Products (Products) are the information messages that shall be issued by the Provider during the Incident lifecycle and at the milestones defined in Fig 3.

The requirements applicable to individual Products are defined below.

Email and Word document templates are available from Service Assurance for the Products defined below.

All communications templates issued for this Standard should conform to BBC confidentiality requirements.

Examples of each Product can be seen in Annex G.

5.1 Service Warning

The purpose of this Product is to provide designated Service Stakeholders with advance warning of potential Incidents.

The Provider shall issue a Service Warning as soon as a situation is detected that has significant potential to result in or develop into an Incident.

The **Service Warning** shall answer as many of the following questions as available information allows and as is possible without delaying the issuing of the Product.

- Why has the warning been issued?
- What business/audience areas are at risk and in what way?
- How many users are at risk?
- Is it a Known Error?
- What is being done to minimise the risk?
- Who is the provider and who is leading on their behalf?
- Who the Product has been distributed to?

Updates shall take the form of subsequent Service Warnings until such time as:-

- the risk materialises into an Incident, whereby an Incident Alert is issued
- the risk subsides, whereby a Stand Down is issued advising that the threat has passed

Service Warnings shall always specify when the next update will be issued?

5.2 Stand Down

The purpose of this Product is to provide designated Service Stakeholders with notice that there is no longer a threat of a potential Incident as previously indicated via a Service Warning.

The Provider shall issue a Service Warning as soon as a situation is detected that has significant potential to result in or develop into an Incident.

The **Stand Down notice** shall inform the Service Stakeholder:

- Why is there no longer a risk of service disruption

5.3 Incident Alert

The purpose of this Product is to alert designated Service Stakeholders to Incidents as quickly as possible.

The Provider shall issue an Incident Alert as soon as the service disruption has been detected and classified (as per requirements in 3).

The **Incident Alert** shall provide answer as many of the following questions as available information allows and as is possible without delaying the issuing of the Product.

- Incident name
- What happened?
- How has the service been affected
- What is the business/audience impact and how many people affected?
- Is it a Known Error?
- What is being done to restore normal service?
- Who is the Provider and who is leading on their behalf
- Who is leading on behalf of the BBC?
- When is service restoration expected and how reliable is this estimate?
- Who the Product has been distributed to?

All **Incident Alerts** shall contain a unique Incident reference number and shall specify when the next update will be issued.

5.4 Incident Update

The purpose of this Product is to provide designated Service Stakeholders with timely progress reports on the efforts being made to restore service.

The Provider shall issue an Incident Update at the date and time stipulated in the previously issued Product unless the service is restored in the meantime and a Service Restoration Notice has been issued as per 5.6.

The Provider may issue an Incident Update ahead of the previously stipulated date and time if there is something significant to report that would be of value or interest to the Service Stakeholders.

The **Incident Update** shall:-

- provide a brief update on what has happened or been learned since the last communication was issued
- aim to answer any Incident Alert questions that are still outstanding (see 5.3)
- provide an updated forecast as to when normal service will be restored
- include previously issued Incident Alert and Incident Updates to maintain a history of the Incident
- clearly date and time stamp the update to avoid confusion with earlier information
- Who the Product has been distributed to

All **Incident Updates** shall contain the Incident reference number and shall specify when the next update will be issued.

5.5 Incident Briefing

The purpose of this Product is to provide designated Service Stakeholders with Incident information that can be easily distributed to non-technical stakeholders within their own business areas.

This Product shall be written in a manner and language appropriate for a non-technical senior business management audience.

The **Incident Briefing** shall provide a succinct bullet-point style executive brief that answers the following questions:-

- What happened?
- What was the impact?
- Who is or was affected most?
- What is being or has been done to help those worst affected?
- Who is the Provider and who is leading on their behalf
- Who is leading on behalf of the BBC?
- What's the plan for restoring normal service?
- What's been done so far?
- When will the service be back to normal?
- What's the level of confidence in this forecast?
- Affect on Service Level Agreements (none; unknown; breached; impacted)
- When will the next briefing be issued?
- Who the Product has been distributed to

All **Incident Briefings** shall contain the Incident reference number and shall specify when the next update will be issued.

5.6 Service Restoration Notice

The purpose of this Product is to alert designated Service Stakeholders to service restoration as quickly as possible.

The Provider shall issue a Service Restoration Notice as soon as possible after it has been confirmed (see below) that the Service has been restored to normal operation.

This Product shall **not** be issued until service restoration has been independently confirmed by consultation with an appropriate BBC Duty Manager, or an appropriate Service User if there is no duty manager for the affected area, and an auditable record has been made of this consultation.

The **Service Restoration Notice** shall:-

- advise the date and time that the Service was restored
- advise which Service User confirmed service restoration
- advise briefly what was done to restore the service
- advise whether or not there is any outstanding risk to on-going service (e.g. loss of resilience etc.)
- advise whether the Service was restored by fix, workaround, self-restore, other
- advise if the server will be monitored and for how long before Incident Closure
- provide advice, where possible, that may benefit Service Users who have been impacted by the disruption. (For example: "If any data was lost as a result of this incident then contact Service Desk to see what can be restored from backups")

- include previously issued Incident Alert and Incident Updates to maintain a history of the Incident
- State who the Product has been distributed to?

If the service has not been restored to normal, then a follow-up Service Restoration Notice shall be issued when normal service has been restored.

Should service quality degrade after a Service Restoration Notice has been issued, then the Incident Lifecycle shall reset to Milestone 2 and an Incident Update shall be issued.

All **Service Restoration Notices** shall contain the Incident reference number and shall specify when the **Incident Closure Notice** (see 5.8) will be issued.

5.7 Incident Closure

The purpose of this Product is to alert designated Service Stakeholders to incident closure, usually after a period of monitoring following service restoration.

The Provider shall issue an Incident Closure Notice as soon as possible after it has been confirmed (see below) that the Service has sustained normal operation.

This Product shall **not** be issued until sustained normal operation has been independently confirmed by consultation with an appropriate BBC Duty Manager, or an appropriate Service User if there is no duty manager for the affected area, and an auditable record has been made of this consultation.

The **Incident Closure Notice** shall:-

- advise the date and time that the Incident was closed
- advise which Service User confirmed sustained normal operation
- provide advice, where possible, that may benefit Service Users who have been impacted by the disruption. (For example: "If any data was lost as a result of this incident then contact Service Desk to see what can be restored from backups")
- include previously issued Incident Alert and Incident Updates to maintain a history of the Incident
- State who the Product has been distributed to?

Should service quality degrade after an Incident Closure Notice has been issued, then the Incident Lifecycle shall reset to Milestone 2 and an Incident Update shall be issued.

All **Incident Closure Notices** shall contain the Incident reference number and shall specify when the **Post Incident Report** (see 5.7) will be issued.

5.8 Post Incident Report

The purpose of this Product is to provide designated Service Stakeholders with technical details about how the service was restored.

The Provider shall issue a Post Incident Report as quickly as practically possible after service restoration has been confirmed or within applicable service levels, whichever is the sooner.

The **Post Incident Report** shall confirm:-

- the date and time that service disruption was first detected
- the date and time that service was restored
- the total duration of the Incident in hours and minutes

- the date that the Incident was closed
- why the Incident was closed, from one of the following reasons:-
 - Ê Service restored by elimination of root cause
 - Ê Service restored by workaround
 - Ê Service restored by other means
 - Ê Incident closed for another reason (specifying the reason)

The **Post Incident Report** shall also provide:-

- a high-level summary of the Incident, confirming:-
 - Ê which services were impacted, how and to what extent
 - Ê which business/audience areas were impacted, how and to what extent
- a detailed chronology of events, which shall:-
 - Ê confirm who first discovered the service disruption and how
 - Ê confirm who restored the Service and how (describing workaround/s if used)
- a legend identifying any individuals, groups or organisations identified by their initials in descriptions
- the reference number of any Known Error identified as causing the Incident
- the reference number of Problem record/s to which this Incident is linked
- the name of the Provider's head of Incident management
- the author's name and the report's version number
- Who the Product has been distributed to?

All **Post Incident Reports** shall contain the Incident reference number and shall specify when the first **Problem Update** (see 5.9) will be issued.

5.9 Problem Update

The purpose of this Product is to provide designated Service Stakeholders with timely progress reports on the efforts being made to avoid similar incidents recurring.

The Provider shall issue a Problem Update at each of the following key milestones during the problem management process.

- a) At weekly intervals until the Problem Closure Report is issued (see 5.10)
- b) When the root cause of the Incident has been identified (or, in the event that root cause cannot be determined, a course of action has been identified that will equally reduce the risk of a similar Incident recurring)
- c) When corrective/preventive actions have been planned
- d) When corrective/preventive actions have been completed

Each **Problem Update** shall:-

- contain the Problem reference number
- include detail that is pertinent to the milestone (e.g. explanation of root cause, corrective/preventive action plan, etc.)
- Who the Product has been distributed to?

Problem Updates shall always specify when the next update will be issued.

5.10 Problem Closure Report

The purpose of this Product is to provide designated Service Stakeholders with technical details about what has been done to avoid similar incidents recurring.

The Provider shall issue a Problem Closure Report as quickly as practically possible after the root cause of the Incident has been eliminated or the risk a recurrence has been substantially reduced.

The **Problem Closure Report** shall confirm:-

- the Problem reference number along with the reference number and brief details of any Incidents or Known Errors to which this Problem has been linked
- the date the Problem record was opened
- the date the Problem record was closed
- the total duration of the Problem in days
- the date that the Incident was closed
- why the Problem was closed, from one of the following reasons:-
 - Ê Root cause identified and eliminated
 - Ê Known Error record created, describing workaround
 - Ê Problem closed for another reason (specifying the reason)

The **Problem Closure Report** shall also provide:-

- a high-level summary of the problem, outlining which services and business areas were impacted
- a description of what has been done to reduce the risk of the Problem causing further business impact, confirming:-
 - Ê whether or not the root cause was found and, if so, what it was
 - Ê whether or not the root cause was eliminated and, if so, how
 - Ê whether or not a workaround was identified and, if so, what it was
- a legend identifying any individuals, groups or organisations identified by their initials in descriptions
- the reference number of any Known Error identified as causing the Incident
- the reference number of Problem record/s to which this Incident is linked
- the name of the Provider's head of Incident management
- the author's name and the report's version number
- Who the Product has been distributed to?

6 Management Responsibilities

Management within the Provider's organisation shall ensure that:-

- their incident and problem management processes are mapped on to the milestones defined in the Incident Lifecycle (see Section 4) and that documentation is maintained to show how this mapping is done and how it produces Communication Products that comply with the requirements defined in Section 5
- auditable records are maintained so as to maintain the ability to prove conformity with this standard retrospectively and from the date on which the Provider first achieved compliance with this standard
- competent resources are maintained to sustain conformity with this standard
- compliance is not impacted or degraded by way of change within the Provider's organisation
- internal arrangements are altered as required to maintain conformity in the event that this standard is changed and that said alterations are completed within a duration as established by prior agreement with the Service Client
- during an Incident the priority shall be to restore normal service as quickly as possible while maintaining compliant Service Stakeholder communications
- following Incident closure, the priority shall be to eliminate the root cause of the disruption or reduce the risk of a recurrence to as low as practicably possible, while maintaining compliant Service Stakeholder communications
- all Incidents are classified using:-
 - Ê Service Codes as defined in Annex A
 - Ê Severity Codes as defined in Annex B
 - Ê Impact Type Codes as defined in Annex C
 - Ê Affected Area Codes as defined in Annex D
- the Communication Products are disseminated by way of the modes defined in Annex E
- the Communication Products are disseminated to the Service Stakeholders in accordance with the criteria and distribution lists specified in Annex F
- the format and style of Communication Products comply with the templates maintained by Service Assurance (see 1.5)

This page intentionally blank

Annex A - Service Codes

This annex contains the codes that shall be used in Communication Products to uniquely identify the services that have been disrupted by Incidents.

Where no code exists in this annex for a disrupted service then the Provider shall provide and use a name or reference that will be meaningful to the recipients of the Communication Products.

A.1 TFC Service Codes

The Provider shall use the codes defined in the table below in relation to any Incident impacting services delivered by way of The (Siemens) Framework Contract (**TFC**).

The codes shall be reproduced exactly as shown below (i.e. case is significant).

Code	Contracted Service
INTERNET	CSR 3 - Internet
DISTRIBUTION	CSR 4 - Distribution
NETWORK	CSR 5 - Circuits and Networks
DESKTOP	CSR 6 - Information Security CSR 7 - Application and Integration Infrastructure CSR 9 - Office Productivity Tools CSR 10 - Processing Platform CSR 11 - Storage
TELEPHONY	CSR12 - Telephony

Annex B - Severity Codes

The table below defines the codes that shall be used to classify the severity of the impact on the BBC arising from service disruptions.

For consistency across the organisation, these codes map directly on to the Resilience Classification tiers as defined in the Business Continuity Architectural Characteristics (**BCAC**) document (see Normative References for the version used in this standard).

The Resilience Classification interpretations have been reproduced below to aid readability however the reader is advised to consult the latest version of the BCAC document to ensure that the correct interpretations are used.

Note: All references in the original BCAC interpretation to “systems” have been replaced by the word “services”.

The codes shall be reproduced exactly as shown below (i.e. case and font colour is significant).

Code	BCAC Classification	Impact Definition
P1	Critical Plus	Crucial to maintaining BBC output. Failures result in international or nation-wide “priority” output interrupted (almost) instantaneously: e.g. BBC1; BBC News; R4; R5L; Local Radio (during civil emergencies etc.); BBC and/or News web front pages; iPlayer etc. Sometimes applies to services depended upon by many other (sometimes) less critical services: e.g. Raman; IP networking etc.
P2	Critical	Failures result in international or nation-wide non-“priority” output interrupted (almost) instantaneously. Will also have a major impact on the ability of the BBC to produce output. This includes contributions for live broadcast, loss of news feeds, live scheduling, etc. A failure in a Critical service may result in considerable staff disruption, even though it does not immediately impact audiences.
P3	Essential	Has a significant financial impact or loss of productivity. Failure would have an imminent (but not immediate) impact on the ability of the BBC to produce output or result in the loss of a portion of a service. Can only be without the service for a few hours
P4	Important	Has significant financial impact, loss of productivity. The business can continue for a day without major issues.
P5	Supportive	Has financial impact, loss of productivity. The business can continue for two days without major issues

In the event that an Incident presents an impact severity that qualifies against more than one interpretation above, then the highest (most critical) code shall be used.

Annex C - Impact Type Codes

The table below defines the codes that shall be used to classify the type of impact experienced by the BBC as a result of service disruptions.

The codes shall be reproduced exactly as shown below (i.e. case is significant).

Code	Impact Definition
AUDIENCE	The disruption is impacting the audience's on-air or on-line experience
PRODUCTION	The disruption is impacting the BBC's ability to make programmes and/or communicate with the general public
BUSINESS	The disruption is impacting the BBC's ability to operate its business

In the event that an Incident presents an impact type that qualifies against more than one definition above, then the highest (most significant) code shall be used.

Annex D - Affected Area Codes

The table below defines the codes that shall be used to identify the business areas and generic output channels (i.e. TV, Radio, Web) impacted by service disruptions.

The codes shall be reproduced exactly as shown below (i.e. case is significant).

Code	Area Impacted
3rdP	Partner or other third party
A&M	Audio and Music
BBCM	BBC Monitoring
ER	English Regions (i.e. all Regions)
FM&T	Future Media and Technology
MC&A	Marketing, Communications and Audiences
Nations	All Nations
News	News
N-Ire	BBC Northern Ireland
Ops	Operations
Pan-BBC	All Areas
Radio	Radio
Scot	BBC Scotland
Sport	Sport
TV	TV
UNK	Area not known
Vision	Vision
Wales	BBC Wales
Web	Web
WW	BBC Worldwide
W12	London W12
W1	London W1
International	International bureaux

In the event that an Incident impacts multiple business areas or generic output channels, then each affected area shall be identified in the communications.

Annex E - Communication Modes

The table below defines the modes that shall be used to disseminate Communication Products to Service Stakeholders.

Communication Product	Communication Mode
Service Warning	SMS Text Message and Email
Stand Down	SMS Text Message and Email
Incident Alert	SMS Text Message and Email
Incident Update	Email
Incident Briefing	Email
Service Restoration Notice	SMS Text Message and Email
Incident Closure	Email
Post Incident Report	Email with attached report in a Word document
Problem Update	Email
Problem Closure Report	Email with attached report in a Word document

Annex F - Service Stakeholders

Communication Products shall be issued to Service Stakeholders in accordance with the criteria and distribution lists defined in the table below.

Criteria	Distribution List
Where Communication Product is: <ul style="list-style-type: none"> • Service Warning 	SIEMENS SERVICE WARNINGS
Where Communication Product is: <ul style="list-style-type: none"> • Incident Alert • Incident Update • Service Restoration Notice • Incident Closure 	SIEMENS INCIDENT ALERTS
Where Communication Product is: <ul style="list-style-type: none"> • Incident Briefing 	SIEMENS INCIDENT BRIEFINGS
Where Communication Product is: <ul style="list-style-type: none"> • Post Incident Report 	SIEMENS POST INCIDENT REPORTS
Where Communication Product is: <ul style="list-style-type: none"> • Problem Update • Problem Closure Report 	SIEMENS PROBLEM MANAGEMENT REPORTS

See **TSI Communication Distribution Lists** in Normative References (2.1) to identify source of above distribution lists.

Annex G - Communication Product Examples

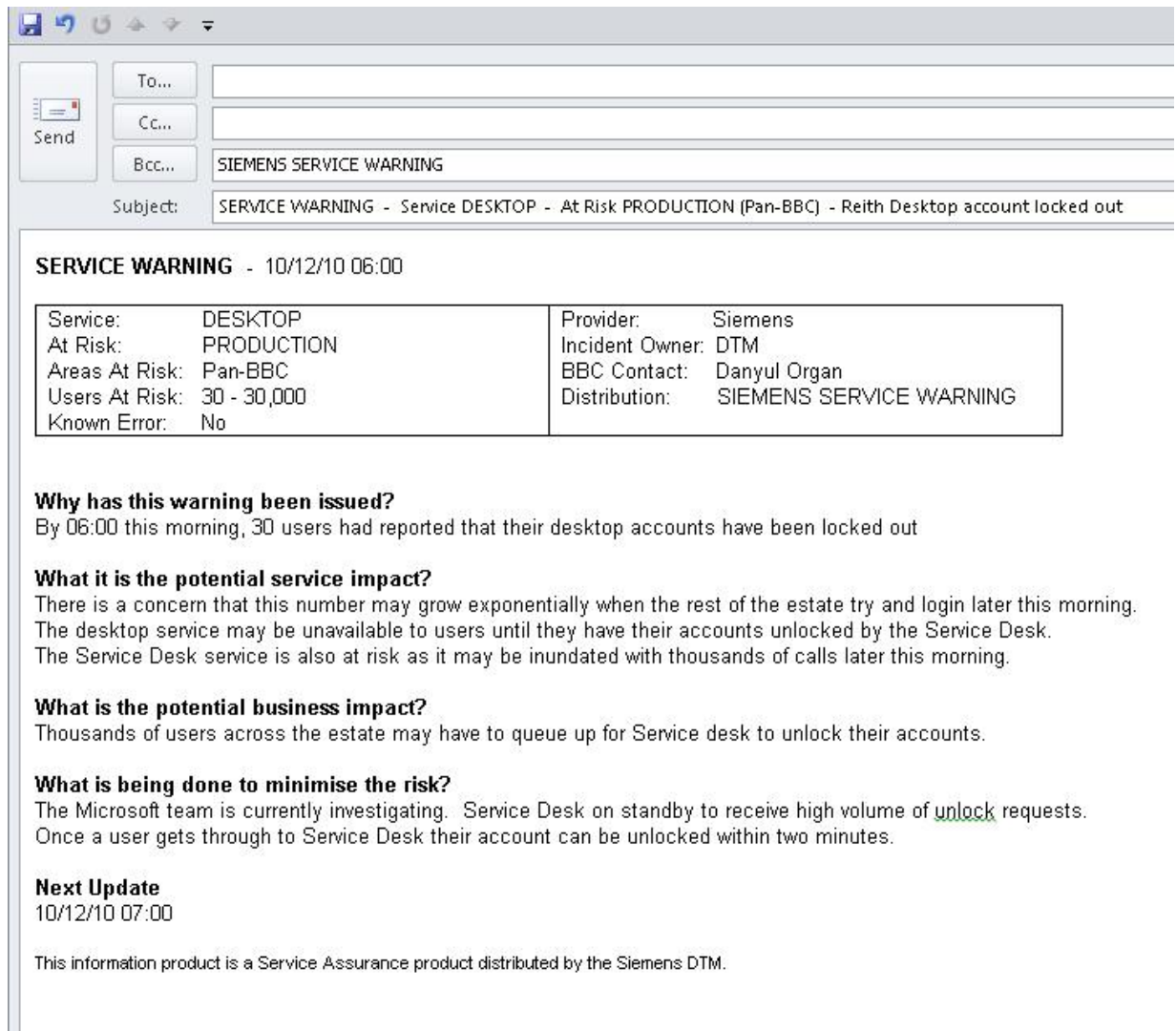
This annex contains example Communication Products for guidance and information only.

Email and Word document templates for Communication Products are available from Service Assurance

G.1 Service Warning / Stand Down - SMS Text Message



G.2 Service Warning – Email



SERVICE WARNING - 10/12/10 06:00

Service:	DESKTOP	Provider:	Siemens
At Risk:	PRODUCTION	Incident Owner:	DTM
Areas At Risk:	Pan-BBC	BBC Contact:	Danyul Organ
Users At Risk:	30 - 30,000	Distribution:	SIEMENS SERVICE WARNING
Known Error:	No		

Why has this warning been issued?
By 06:00 this morning, 30 users had reported that their desktop accounts have been locked out

What it is the potential service impact?
There is a concern that this number may grow exponentially when the rest of the estate try and login later this morning. The desktop service may be unavailable to users until they have their accounts unlocked by the Service Desk. The Service Desk service is also at risk as it may be inundated with thousands of calls later this morning.

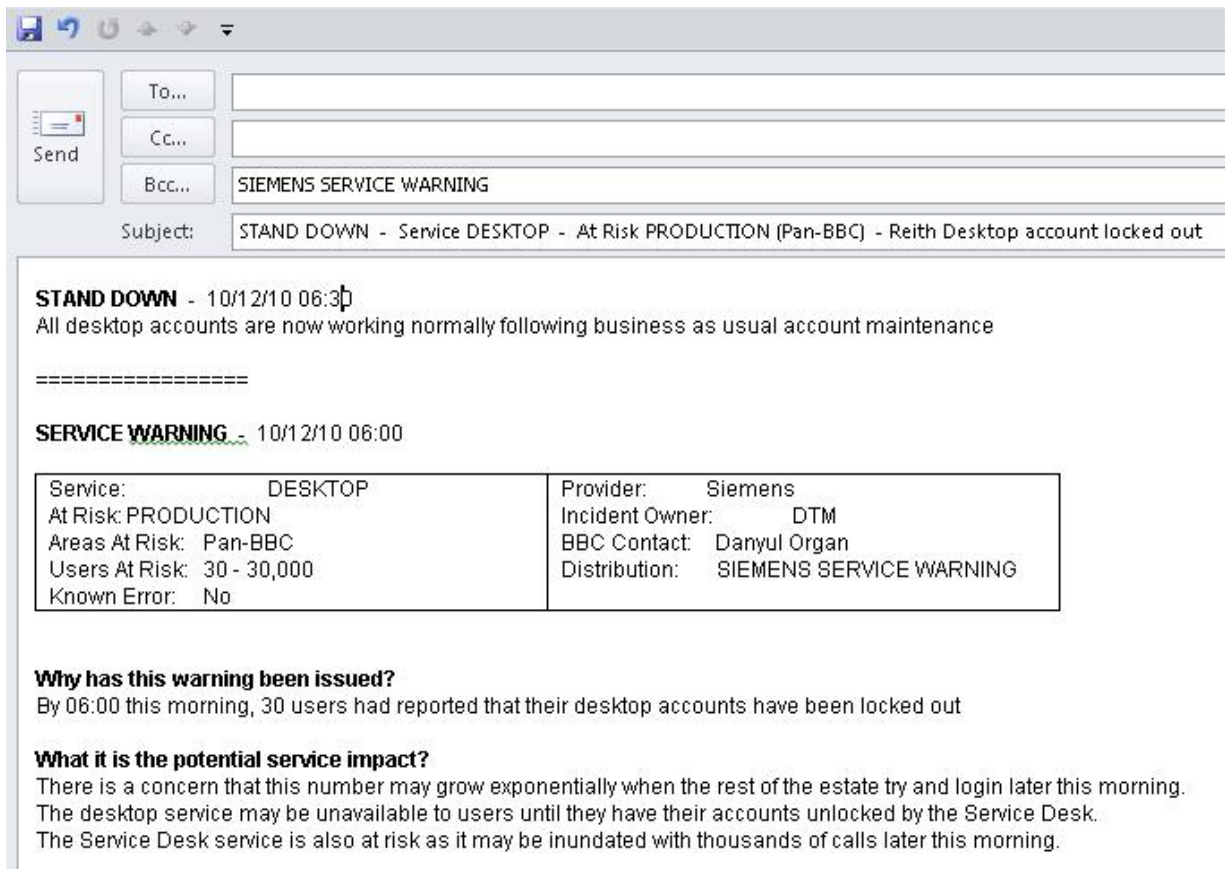
What is the potential business impact?
Thousands of users across the estate may have to queue up for Service desk to unlock their accounts.

What is being done to minimise the risk?
The Microsoft team is currently investigating. Service Desk on standby to receive high volume of [unlock](#) requests. Once a user gets through to Service Desk their account can be unlocked within two minutes.

Next Update
10/12/10 07:00

This information product is a Service Assurance product distributed by the Siemens DTM.

G.3 Stand Down – Email



G.4 Incident Alert - SMS Text Message



G.5 Incident Alert – Email

INCIDENT ALERT TSI1234 - 09/08/10 22:40

Ref:	TSI1234	Provider:	Siemens
Severity:	P4-DESKTOP	Incident Owner:	DTM
Impacting:	PRODUCTION	BBC Contact:	John Smith
Areas Affected:	News, ER	Next Update:	10/08/20 00:40
Users Affected:	1,000 to 2,000	Distribution:	SIEMENS INCIDENT ALERT
Known Error:	No		

What happened?
File server NEWSMBRD01 in [Millbank](#) failed due to a hardware failure

How has the service been affected?
None of the files on the affected server can be accessed

What is the business impact?
1,000 to 2,000 users at [Millbank](#) will not be able to access files, which may impact preparations for the upcoming party conferences

What is being done to restore normal service?
Data is being restored from the latest backup onto a standby server

When is service restoration expected?
10/08/2010 00:40

How reliable is this estimate?
High

This information product is a Service Assurance product distributed by the Siemens DTM.

G.6 Incident Update – Email

The screenshot shows an email client interface with the following details:

- To...**: [Empty]
- Cc...**: [Empty]
- Bcc...**: SIEMENS INCIDENT ALERT
- Subject:** INCIDENT UPDATE #2 TSI1234 - P4 DESKTOP - Affecting PRODUCTION (News, ER) - File server in Millbank failed

INCIDENT UPDATE #2 10/08/10 09:02

What has happened or been learned since the last communication?
Data restore completed without incident
Final testing underway before standby server put into service
Number of affected users now known to be 980

When is service restoration expected?
10/08/2010 09:30

How reliable is this estimate?
High

Next Update
10/08/20 09:30

INCIDENT UPDATE #1 10/08/10 07:55

What has happened or been learned since the last communication?
Data restore progressing as expected

When is service restoration expected?
10/08/2010 00:40

How reliable is this estimate?
High

Next Update
10/08/20 09:00

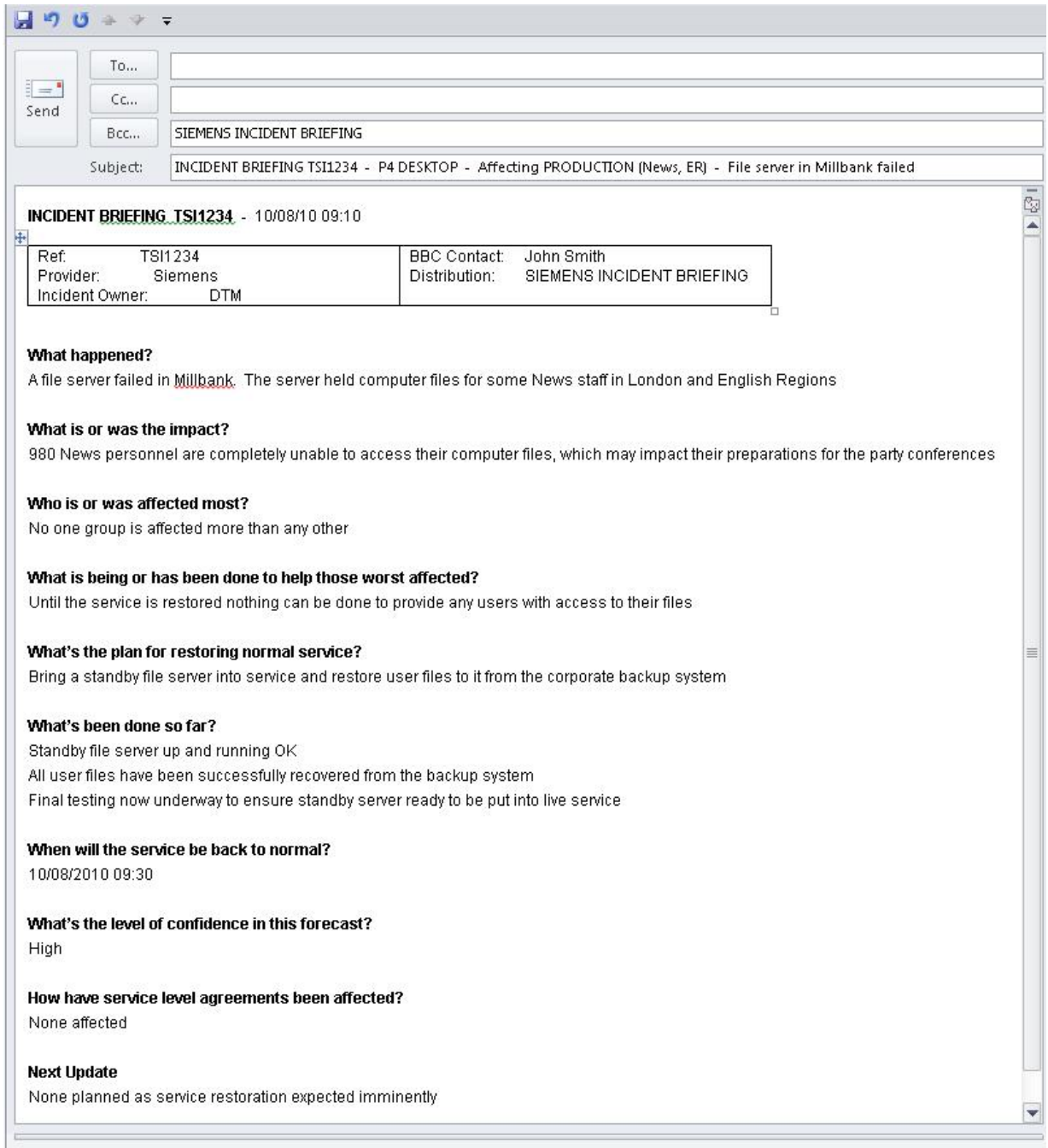
INCIDENT ALERT TSI1234 - 10/08/10 07:25

Ref:	TSI1234	Provider:	Siemens
Severity:	P4-DESKTOP	Incident Owner:	DTM
Impacting:	PRODUCTION	BBC Contact:	John Smith
Areas Affected:	News, ER	Next Update:	10/08/20 00:40
Users Affected:	1,000 to 2,000	Distribution:	SIEMENS INCIDENT ALERT

Two yellow callout boxes with red arrows pointing to the email content:

- Subsequent updates**: Points to the 'INCIDENT UPDATE #2' section.
- Original alert**: Points to the 'INCIDENT ALERT TSI1234' section.

G.7 Incident Briefing – Email



G.8 Service Restoration Notice – SMS Text Message



G.9 Service Restoration Notice – Email

Send

To...

Cc...

Bcc... SIEMENS INCIDENT ALERT

Subject: SERVICE RESTORED TSI1234 - P4 DESKTOP - Affecting PRODUCTION (News, ER) - File server in Millbank failed

SERVICE RESTORED TSI1234 ! 10/08/10 09:25

Repair: FIX	PIR Due: 15/08/20
Service Quality: NORMAL	Distribution: SIEMENS INCIDENT ALERT
Confirmed By: John Smith	

What was done to restore the service?
Data was permanently restored to an alternative server.

What advice is there for those who may have been impacted by this incident?
If any data was lost as a result of this incident then contact the Service Desk (0440) to find out what can be restored from backups

Next Update
None

INCIDENT UPDATE #2 10/08/10 09:02

What has happened or been learned since the last communication?
Data restore completed without incident
Final testing underway before standby server put into service
Number of affected users now known to be 980

When is service restoration expected?
10/08/2010 09:30

How reliable is this estimate?
High

Next Update
10/08/20 09:30

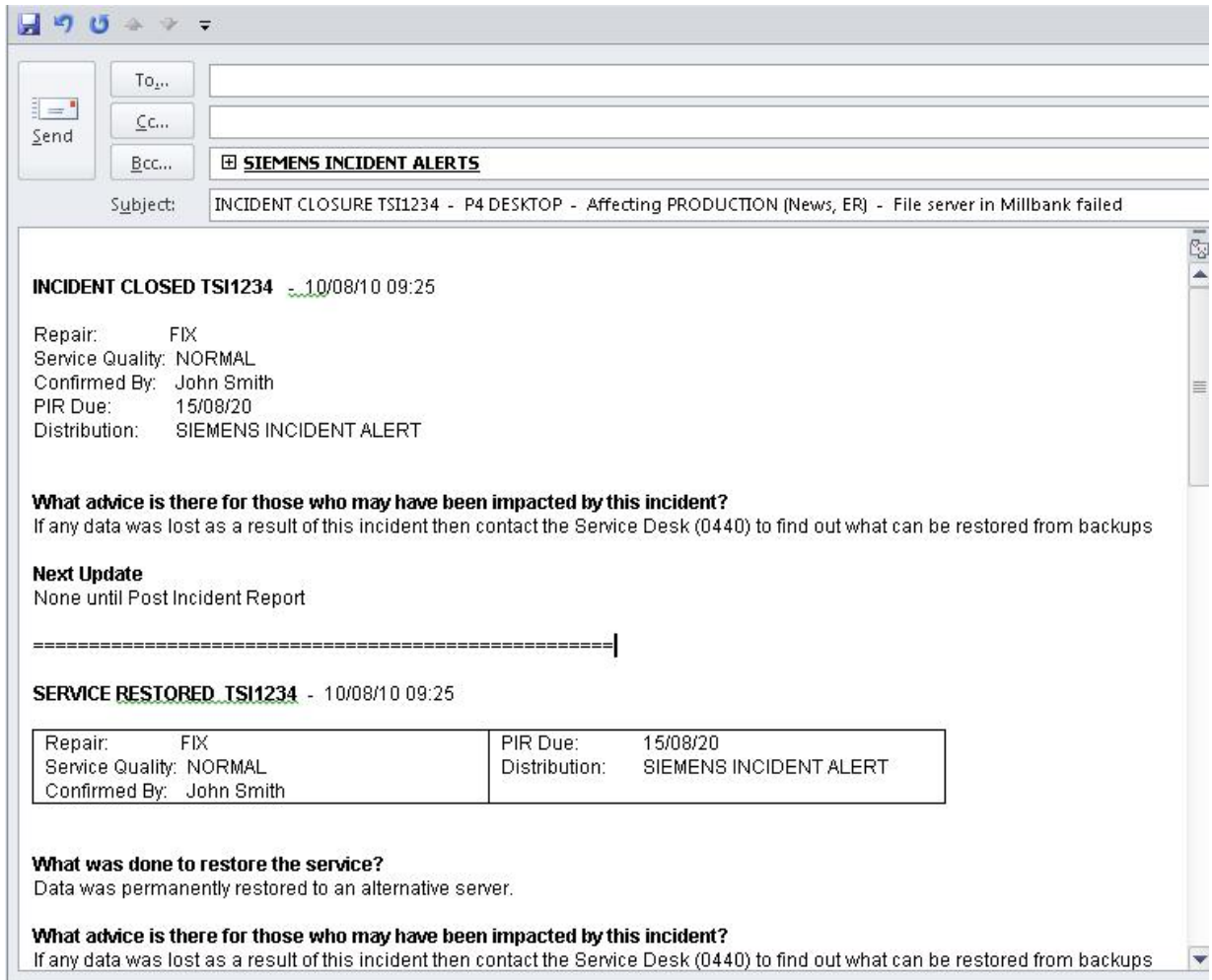
INCIDENT UPDATE #1 10/08/10 07:55

What has happened or been learned since the last communication?
Data restore progressing as expected

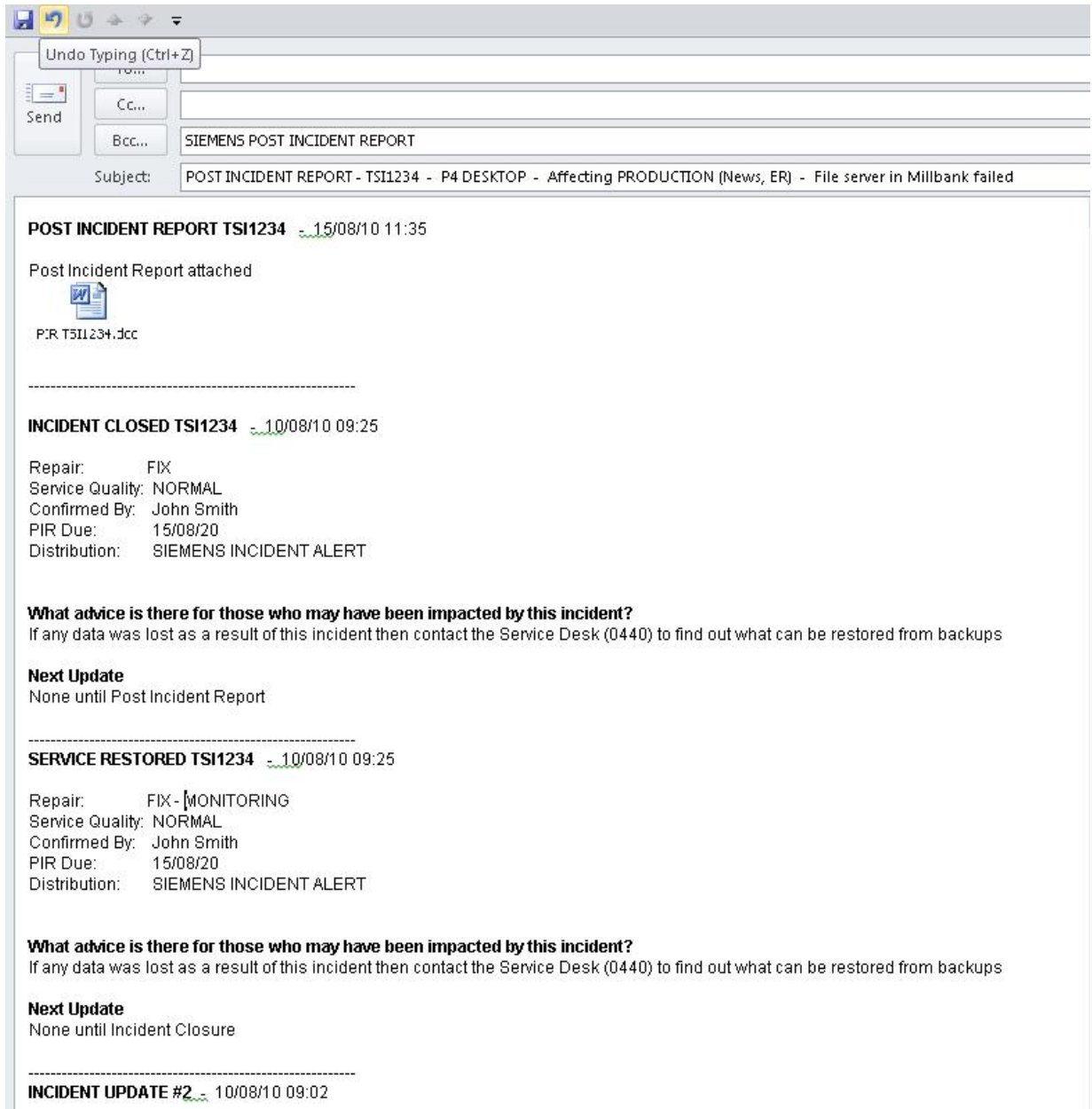
When is service restoration expected?
10/08/2010 00:40

How reliable is this estimate?
High

G.10 Incident Closure – Email



G.11 Post Incident Report – Email



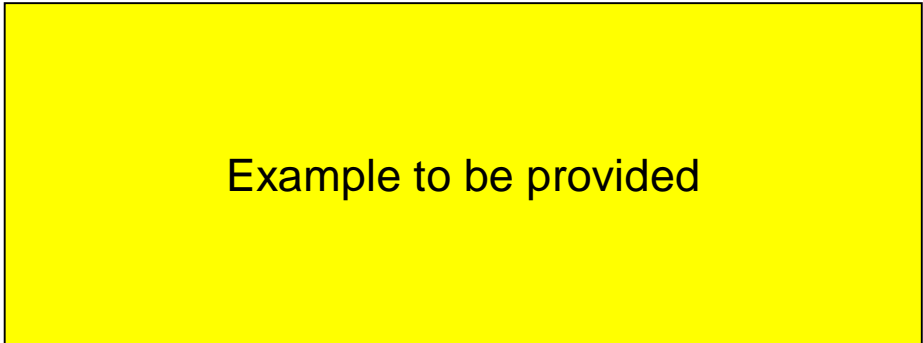
G.12 Post Incident Report – Word Document

INCIDENT SUMMARY	
Service Provider	
Incident Reference	
Incident Name	
Service/s Affected	<i>Summarise what happened, confirming which services affected, how and to what extent</i>
Area/s Impacted	<i>Confirm which business areas were impacted, how and to what extent</i>
Incident Detected	<i>dd/mm/yyyy hh:mm</i>
Service Restored	<i>dd/mm/yyyy hh:mm</i>
Incident Duration	<i>hh:mm between [Incident Detected] and [Service Restored]</i>

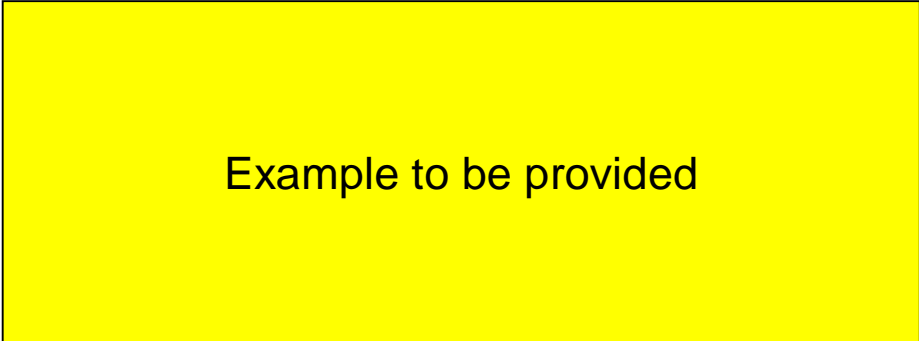
INCIDENT CHRONOLOGY			
Date	Time	Who	What
<i>dd/mm/yyyy</i>	<i>hh:mm</i>	<i>Initials</i>	<i>Delete this row and copy and paste others below as necessary to detail the chronology of events (from incident discovery to service restoration), including as a minimum:-</i> <ul style="list-style-type: none"> <i>confirmation of who first discovered the service disruption and how</i> <i>confirmation of who restored the service and how</i> <i>description of any workarounds that were used to restore the service</i>

INCIDENT RESOURCES			
Initials	Name	Company	Position
<i>Delete this row and add others below as necessary to identify all parties referenced in the chronology above.</i>			

G.13 Problem Update - Email



G.14 Problem Closure Report - Email



G.15 Problem Closure Report – Word Document

Problem Closure Report

PROBLEM SUMMARY	
Service Provider	
Problem Reference	
Problem Name	
Problem Description	<i>Briefly describe the problem, outlining the impact it caused to services and business areas</i>
Record Opened	<i>dd/mm/yyyy</i>
Record Closed	<i>dd/mm/yyyy</i>
Problem Duration	<i>Days between [Record Opened] and [Record Closed]</i>

PROBLEM RESOLUTION
<p><i>Overwrite this section with a description of what has been done to reduce the risk of the Problem causing further business impact, confirming:-</i></p> <ul style="list-style-type: none"> <i>whether or not the root cause was found and, if so, what it was</i> <i>whether or not the root cause was eliminated and, if so, how</i> <i>whether or not a workaround was identified and, if so, what it was</i> <p><i>Where initials are used to identify resources then these should be defined in the table below</i></p>



PROBLEM RESOURCES			
Initials	Name	Company	Position
<i>Delete this row and add others below as necessary to identify all parties referenced in the chronology above.</i>			