Consequence Requirements Specification for the Policy-Based Security for the Crisis Management Test Bed

WP5 Policy Based Security for the Crisis Management Test Bed

December 2008
Version 3.0

Consequence

Context-aware data-centric information sharing

FP7-ICT-2007-1
ICT-2007.1.4. Secure, dependable and trusted Infrastructures
Grant Agreement 214859

Consequence Deliverable D5.1: Page 1 of 80
LEGAL NOTICE

The following organizations are members of the Consequence Consortium:
Europäisches Microsoft Innovations Center GmbH,
BAE SYSTEMS (Operations) Limited,
Hewlett-Packard Italiana,
Imperial College of Science, Technology and Medicine,
The Science and Technology Facilities Council,
Consiglio Nazionale delle Ricerche,
Centre for Research and Telecommunication for Networked Communities.

This document is © Copyright 2008 the members of the Consequence Consortium (membership defined above)

The information in this document is provided 'as is', and no guarantee or warranty is given that the information is fit for any particular purpose. All warranties and conditions, express or implied, concerning the information, are excluded. The user uses the information at its sole risk and liability. Neither the Consequence Consortium, nor any member organization nor any person acting on behalf of those organizations is responsible for the use that might be made of the information in this document.

The views expressed in this document are the sole responsibility of the authors and do not necessarily reflect the views of the European Commission or the member organizations of the Consequence Consortium.

This document is for general guidance only. All reasonable care and skill has been used in the compilation of this document. Although the authors have attempted to provide accurate information in this document, the Consequence Consortium assumes no responsibility for the accuracy of the information.

Information is subject to change without notice.

Mention of products or services from vendors is for information purposes only and constitutes neither an endorsement nor a recommendation.

Reproduction of this document is authorized provided the source is acknowledged. However if any information in this document is marked as confidential then such information may not be published and may be used only for information purposes by European Community Institutions to whom the Commission has supplied it.

Microsoft is a trademark of Microsoft Corporation in the United States, other countries or both.

HP is a trademark of Hewlett-Packard Company in the United States, other countries or both.

Other company, product and service names may be trademarks, or service marks of others. All third-party trademarks are hereby acknowledged.
Project acronym: Consequence
Project full title: Context-aware data-centric information sharing

Work Package: 5

Document title: Name of the deliverable
Version: 3.0
Official delivery date: 31 Dec 2008
Actual publication date: 19 December 2008
Type of document: Report
Nature: Public

Authors: D. Golby, S. Barker, F. Lockwood, A.G. Davies
Approved by: S. Crompton, A. Orlov, D. Starostin

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Sections Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>July 2008</td>
<td>All sections. Intended for discussions of overall doc structure.</td>
</tr>
<tr>
<td>1.1</td>
<td>Aug 2008</td>
<td>Final version of scenario storyboard. First version of Scenario requirements. Rest of document to be completed.</td>
</tr>
<tr>
<td>2.0</td>
<td>Nov 2008</td>
<td>Updated version incorporating results from end-user interviews and scenario policies</td>
</tr>
<tr>
<td>2.1</td>
<td>Nov 25 2008</td>
<td>Version for review</td>
</tr>
<tr>
<td>3.0</td>
<td>Dec 2008</td>
<td>Final version incorporating changes suggested by the reviewers</td>
</tr>
</tbody>
</table>
Table of contents

1. INTRODUCTION 6

2. INFORMATION SHARING BETWEEN AGENCIES 6
   2.1. Relevant UK Legislation 7
   2.2. Information sharing: current practice 8
   2.3. Other sources 12
   2.4. Implications for Consequence 12

3. SCENARIO 13
   3.1. Introduction 13
   3.2. The OASIS-fp6 Project 13
   3.3. Scenario Description 15
   3.4. TSO Threat Analysis 23
   3.5. Scenario Phases 23

4. REQUIREMENTS ARISING FROM THE SCENARIO 36
   4.1. Business Requirements (BR) 36
   4.2. Administration Requirements (AR) 37
   4.3. Policy Implementation Requirements 38
   4.4. System Procurement Requirements (SR) 38

5. TESTING AND EVALUATION 39
   5.1. Experimental Methodology 39
   5.2. Evaluation Tests 43

6. CONCLUSIONS 47

7. REFERENCES 48

APPENDIX 1. GLOSSARY 50

APPENDIX 2. RESPONDER ORGANIZATIONS 50
APPENDIX 3.  TSO STRUCTURE  52
APPENDIX 4.  UK LEGISLATION  57
APPENDIX 5.  APPLICATION ARCHITECTURE  64
APPENDIX 6.  STUDIES AND TRIALS INTO INTER-AGENCY DATA SHARING  68
APPENDIX 7.  RESPONDER INFRASTRUCTURE PROFILES  75
APPENDIX 8.  FURTHER EVALUATION METHODOLOGIES & TECHNIQUES  79
1. Introduction

This report identifies the requirements for the Consequence Framework from the point of view of Crisis Management.

As the scale and impact of disasters (both natural and man-made) become more marked it is important that different agencies can work together and share information and resources to contain the crisis in a timely fashion. The resources and information that are shared may be subject to different security requirements across many different organisations, possibly even different jurisdictions. Examples of this kind of data include personal data (ie, data that can identify an individual), commercially sensitive data or in the most extreme cases data that has implications for national security. Therefore, it is essential that this kind of information is restricted to the people who need it for making key decisions without any disruption to their ability to deal with the incident.

The approach taken in this report is to identify the key top-level requirements by means of application scenarios. The requirements presented here emphasise the functional requirements and are intended to avoid prescribing architectural elements that are identified in the Architecture/Framework development activity in Consequence.

Before the scenarios are presented, the next section presents some of the background to this work, characterising the current practices for sharing information. This is based on interviews and surveys from previous studies. The interviews were conducted with representatives from the Police, Ambulance and Fire services in the UK and capture some aspects of the current state of the art, defining what information is typically shared between the agencies when they deal with an emergency.

Section 3 presents the scenario including the story line, the actors/stakeholders involved and different use cases. It also describes the underlying assumptions, background information (including legislation) and characterises the general systems and infrastructure that is involved. A basic application architecture is also presented.

The main requirements for the Crisis Management Test Bed are summarised in Section 4. These are intended to be used as the top-level requirements for the Consequence framework, to be developed further in the remainder of the project.

An important aspect of the work in WP5 is to evaluate the results of the project in order to a) confirm that the Consequence toolkit performs as expected, and also b) to refine and discover new requirements from the prototyping exercise. Section 5 describes the evaluation tests that are currently planned for evaluating Consequence. It also defines the criteria for assessing whether the framework meets its critical requirements.

2. Information Sharing Between Agencies

Generally, in England and Wales, emergencies are managed on a ‘multi-agency’ command system. This means that all agencies involved in responding to the emergency are able to do so in a coordinated way. The agencies involved provide on ‘Gold,’ ‘Silver,’ and ‘Bronze’ command centres, which are as follows:

- **Gold** command sets the strategic policy and considers next day, next week, next year issues.
- **Silver** manages the tactical deployment of resources at the incident site
• **Bronze** delivers the operational plan within the site of the incident.

Equivalent role classifications found in the literature are ‘strategic’, ‘operational’ and ‘tactical’.

The organisations that participate in an incident depend on the ‘scale’ of the incident (Appendix 3). The basic doctrine is to react at local level and only escalate (ie, involve other organisations) as required. If an emergency is of such a large scale that there are serious implications for national security, resilience, international relations and has a high level of media interest, then UK central Government will be involved via COBR (Cabinet Office Briefing Rooms, sometimes referred to as COBRA).

### 2.1. Relevant UK Legislation

In the UK, the relevant legislation for emergency response includes:

1. Civil Contingencies Act 2004 (CCA 04)
2. Data Protection Act 1998 (DPA 98)

CCA 04 places statutory obligations on organisations to manage emergencies and incidents. The act defines two main categories of organisations who are obliged to plan, respond and manage major crises that threaten life, property or economic prosperity on a large scale. These are the so-called Category 1 and Category 2 responders (for a more detailed list, see Appendix 2).

The Category 1 organisations include:

- Emergency Services
- Local Authorities
- Health Bodies
- Environment Agency

Category 2 organisations include:

- Utilities
- Transport
- Strategic Health Authorities
- Health and Safety Executive

The act also acknowledges that other types of organizations may be called upon to help in an emergency. It should also be noted that some of these responders dealing with the incident may be public agencies and some may be commercial organisations. For example, infrastructure/utility companies are privately owned in the UK and in other EU countries.

In the UK, these responder organisations may be members of a local Regional Resilience Forum [11]. The forum is a body for ensuring that the agencies are ready and prepared to deal with an incident. It co-ordinates the activities concerned with risk assessment, emergency response planning, business continuity management and public communications.

Further information on CCA 04 and the other UK legislation is presented in Appendix 4.
2.2. **Information sharing: current practice**

To understand information needs and existing sharing policies, a number of interviews with Category 1 responders were conducted. The interviews with Police, Fire & Rescue and Ambulance service representatives indicate that there are currently no formalised arrangements between agencies and sharing practices depend upon the individuals involved. The implication of this is that, at this time at least, there are no formal data sharing policies.

The information shared between Category 1 responders broadly falls into three categories:

- **Background** — information on features and conditions in the local area of relevance to incident management, for example:
  - Temporary road closures
  - Flooding
  - Wind direction
  - Marked addresses

  This information is usually delivered via *text-based media*, such as fax or email, and is not integrated into control room systems unless manually entered by operators where the system allows for this.

- **Co-ordination** — information on individual services or the co-ordinated response to an incident, for example:
  - Status of each service’s response
  - Rendezvous point
  - Evacuation details

  This information is currently not provided at all or delivered *verbally* via telephone or radio directly from the agency in question or through staff on scene.

- **Incident** — information particular to incidents, for example:
  - Location
  - Type of incident- a commonly understood term shared between the responders
  - Casualties

  This type of information is currently obtained directly from a caller on the emergency telephone line or passed on by another service. This information is used by each service to identify an appropriate response to the incident. In this category the information requirements for each service differ widely. Services do not have systems in place to identify and record information from the initial call which can satisfy all other services.

Table 1 provides an overview of current information sharing practices within and between each of the Category 1 responders. It should be noted that these are the findings from specific regions of each agency and do not necessarily represent the experience of UK wide forces.

What is clear is that information sharing is not standardised and what one agency expects and needs from another agency does not necessarily correspond to what they actually receive. This suggests a lack of understanding with regard to information sharing requirements. Other sources confirm these views. For example the following quote taken from a Lessons Learnt report after a Regional Resilience Exercise states that information flow was “determined to be key by everyone taking part in the exercise” (GOSE, 2004:25

```
### 2.2.1. Overview of what information is shared.

Prior to implementing data sharing and security policies the information access requirements need to be identified. The following table provides an overview of what the Police, Ambulance and Fire & Rescue services share internally, what each provides to other services, and what each expects to receive.

<table>
<thead>
<tr>
<th>POLICE</th>
<th>AMBULANCE</th>
<th>FIRE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Only</td>
<td>Ambulance provide to Police</td>
<td>Fire provide to Police</td>
</tr>
<tr>
<td>• Not all events can be seen by all police officers</td>
<td>• Number of resources</td>
<td>• Information on chemical-related incidents, for officers safety</td>
</tr>
<tr>
<td>• Calls can be secured internally</td>
<td>• Type of incident</td>
<td>• Information from FireMET (Police may not have access to this)</td>
</tr>
<tr>
<td></td>
<td>• Loading position</td>
<td>• Severity of incident</td>
</tr>
<tr>
<td></td>
<td>• Parking positions</td>
<td>• Type of incident</td>
</tr>
<tr>
<td></td>
<td>• Casualty clearing point</td>
<td>• Registration number of vehicles involved</td>
</tr>
<tr>
<td></td>
<td>• CBRN information</td>
<td>• Number of vehicles involved</td>
</tr>
<tr>
<td></td>
<td>• Informant details so they can call back (if the job is open)</td>
<td>• Number of casualties</td>
</tr>
<tr>
<td></td>
<td>• Request to clear a landing point for air ambulance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Type of violence on scene</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Weapons involved</td>
<td></td>
</tr>
<tr>
<td><strong>Police expect to receive from Ambulance</strong></td>
<td></td>
<td><strong>Police expect to receive from Fire</strong></td>
</tr>
<tr>
<td>• Information on patients where relevant</td>
<td></td>
<td>• Information about nuisance callers and the numbers or addresses involved.</td>
</tr>
<tr>
<td>• To be informed:</td>
<td></td>
<td>• Information on arson etc. If not already attended by police.</td>
</tr>
<tr>
<td>o When markers have been placed on addresses by ambulance due to violent or unpredictable residents</td>
<td></td>
<td>• Road closure requests</td>
</tr>
<tr>
<td>o If there has been a suicide</td>
<td></td>
<td>• Car fires</td>
</tr>
<tr>
<td>o Where ambulances are by job number</td>
<td></td>
<td>• Forewarning if area around incident is dangerous.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AMBULANCE</th>
<th>POLICE</th>
<th>FIRE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police provide to Ambulance Service</td>
<td>Internal Only</td>
<td>Fire provide to Ambulance</td>
</tr>
<tr>
<td>• Patient information - although not to the depth that ambulance would collect</td>
<td>• Confidential patient information: unless requested by the coroner or authorised by Gold command</td>
<td>• Type of incident</td>
</tr>
<tr>
<td>• Number of casualties, broad information.</td>
<td>• Data on names would not be kept in the control system</td>
<td>• Severity</td>
</tr>
<tr>
<td>• Cordon details</td>
<td>• Very open when Gold command is in place</td>
<td>• Number of Casualties</td>
</tr>
<tr>
<td>• Evacuation details</td>
<td></td>
<td>• Confidential information on crew eg. if they are hurt and need assistance may pass on details of allergies or similar</td>
</tr>
<tr>
<td>• Media briefing</td>
<td></td>
<td>• Information on chemical-related incidents, for officers safety</td>
</tr>
<tr>
<td>• Rendezvous points</td>
<td></td>
<td>• Wind speed</td>
</tr>
<tr>
<td>POLICE</td>
<td>AMBULANCE</td>
<td>FIRE</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td><strong>Ambulance expect to receive from Police Service</strong></td>
<td></td>
<td><strong>Ambulance expect to receive from Fire</strong></td>
</tr>
<tr>
<td>• Call contents</td>
<td></td>
<td>• A notification of house fire incidents in which people are known to be inside</td>
</tr>
<tr>
<td>• Any information on the patient’s injuries, for example</td>
<td></td>
<td>• Information on Fire appliances that may be of interest to Ambulance personnel (e.g., resuscitators, breathing equipment etc)</td>
</tr>
<tr>
<td>• Updates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Road closures and safe routes to incident</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Spillages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• If railway crossings are blocked</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• MET office updates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Confirmation of attendance (i.e. where domestic violence is suspected)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Crew safety information, where an address is flagged in the police systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Police provide to Fire Service</strong></td>
<td><strong>Ambulance provide to Fire Service</strong></td>
<td><strong>Internal Only</strong></td>
</tr>
<tr>
<td>• Minimal information, fire do not need much</td>
<td>• Type of incident</td>
<td>• Information on building notes from inspections (although this could be requested by Silver/Gold command)</td>
</tr>
<tr>
<td>• Location of incident</td>
<td>• Location of incident</td>
<td>• Contact details for other agencies that are personal - mobile numbers for example</td>
</tr>
<tr>
<td>• Type of incident</td>
<td>• Information on hazardous materials involved where relevant</td>
<td>• Names of fire-fighters</td>
</tr>
<tr>
<td>• Persons reported</td>
<td>• Parking positions and casualty clearing areas at an incident to prevent confusion</td>
<td>• If there is a broken asset or asset availability and spread not required by other agencies</td>
</tr>
<tr>
<td>• What is on fire</td>
<td></td>
<td>• Details of cover moves, ambulance movements related to maintaining adequate coverage of the local area.</td>
</tr>
<tr>
<td>• If a vehicle is carrying a hazardous load</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• If there any witnesses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Information on the safe route to an incident</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Unable to provide vehicle ownership information due to DPA (There are restrictions on Police sharing this information related to the policy of &quot;need-to-know&quot;)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Access to CCTV for cameras at the site of incident</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Fire expect to receive from Police Service</strong></td>
<td><strong>Fire expect to receive from Ambulance Service</strong></td>
<td></td>
</tr>
<tr>
<td>• Confirmation of attendance</td>
<td>• Persons trapped, this vital information is not always given</td>
<td></td>
</tr>
<tr>
<td>• Details of the location of the incident in as much detail as possible</td>
<td>• Location of incident</td>
<td></td>
</tr>
<tr>
<td>• Road closures, important for routing engines</td>
<td>• Number of vehicles – less critical</td>
<td></td>
</tr>
<tr>
<td>• For a bomb alert or suicide or chemical cloud (accidental or act of terrorism) fire would like a rendezvous point</td>
<td>• Confirmation of ambulance attendance</td>
<td></td>
</tr>
<tr>
<td>• Number of vehicles involved</td>
<td>• Attendance time of ambulance</td>
<td></td>
</tr>
<tr>
<td>• Persons trapped</td>
<td>• Updates, it would be useful to know what information that is being sent back to the ambulance control room pertaining to the incident</td>
<td></td>
</tr>
<tr>
<td>• Attendance time of police</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• If police are involved in a potentially risky operation (e.g., armed siege) – for fire to standby</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 1 Summary of current information sharing requirements and expectations between the PAF agencies

<table>
<thead>
<tr>
<th>POLICE</th>
<th>AMBULANCE</th>
<th>FIRE</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Registration information – registered keeper of a vehicle</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Updates, it would be useful to know what information that is being</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sent back to the police control room pertaining to the incident</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1 Summary of current information sharing requirements and expectations between the PAF agencies
2.3. **Other sources**

To supplement the information gathered through interviews, the results and lessons learnt from some previous trials were considered to see whether there are areas that Consequence could apply its technological solution to good effect.

The sources reviewed were:

- The OASIS-fp6 project's "Shropshire trials", in which the utility of data sharing for the emergency services was tested by an extensive series of exercises using emergency personnel in a simulated control room.
- The National Mobile Data Project, which considered how relevant information and collective experience is captured and made accessible in real time to officers at fire and other emergency services.
- Exercise Triton scenario, which covered an extreme flooding event with extensive flooding affecting nearly half of England and Wales. Over 60 organisations and agencies took part nationally, regionally and locally.
- The Pitt Report, which was an independent review of the flooding emergency that took place in June and July 2007 to assess what had happened and what might be done differently.

For further details see Appendix 6. All of these studies emphasised the importance of data sharing, and the majority also highlighted concerns about security-hampered data sharing.

2.4. **Implications for Consequence**

The interviews with the PAF services revealed the data sharing requirements that the organisations have with each other (Table 1). The reason for sharing the information is to ensure that the responders have all of the relevant information that they require for their own tasks. Therefore, any data that is not relevant would not, in general, be shared.

A number of issues related to security were raised. Category 2 organisations tend to be rather inhibited when sharing data, possibly due to organisational, legal and commercial licensing constraints. As described in Appendix 6, for Category 2 sharing information was the exception, not the norm, probably due to different organisational/cultural attitudes. Data sharing protocols between responders were not formally defined, so the decision makers were not sure how to request and access the required information. In some cases, the safest option appeared to not share information at all, while other responders may decide to exchange data via ad-hoc routes that may not be under control. The issue of sharing Personal Data is a well known problem that occurs across many sectors, not only in emergency response. Finally, information systems used by agencies are still at an early stage of development and do not exploit latest developments in network, system or data security that can be used to improve interoperability between different organisations.

Consequence assumes the availability of sophisticated information sharing systems between Category 1 responders at various levels. However, as the interviews have indicated the current reality is somewhat different. Furthermore, there is always going to be a trade-off between the requirement to protect data and the urgent requirements for sharing data to deal with an emergency. Agencies that are dealing with emergencies have the important requirement for quick and effective access to accurate and relevant information to perform their statutory...
duties. These requirements may take precedence over other legal considerations when dealing with sensitive data.

What is also clear is that there are needs for better information handling strategies. Part of this includes understanding what to share, when and with whom. An agreed method and format for sharing information would be valuable — eg. Who (classification/role/proximity), What (can be shared), Where (restricted, controlled or public area), When (criticality level) and Why (the information is needed). By means of suitable systems that facilitate data sharing, policies could help to implement these requirements through the application of data and information standards. Therefore, an alternative approach may be to consider the policy as the governance surrounding the activity of sharing as opposed to strict rules that are attached to the actual material that is shared.

The interviews showed that much of the information is currently transmitted and shared verbally, and so it is important to understand the extent to which a responder organisation can realistically accommodate the ambitions of a technology such as Consequence. A number of reasons were given for the bias towards using voice communications to share information, eg. a closed feedback loop means that the sender knows that the recipient has received it, they can confirm the message has been understood, and be sure of the action to be taken. Therefore, voice communications will continue to play a major role in the most critical communication activities and so it is possible that this reliance on verbal communications may set a practical limit to the extent that new IT technologies can be used in a responder organisation. The implications of this for Consequence is that policy based security may be a valuable adjunct but is of limited applicability in the current UK environment.

3. Scenario

3.1. Introduction

The purpose of this section is to explore a future application scenario that illustrates how new technologies could aid the information sharing process but also with the aforementioned data security concerns in mind.

The known security issues that have already been noted so far include:

1. protecting data connected with casualties, evacuees and their personal details
2. eliminating the uncertainties connected with releasing data, which can prevent release when this was unnecessary
3. protecting commercially sensitive information belonging to Category 2 responders
4. commercial license restrictions

The scenario is used to investigate a number of these and other security issues in greater detail. The scenario uses components and documents that are used in the OASIS-fp6 [2] framework. The following section briefly reviews the relevant aspects of that project before the description of the scenario itself.

3.2. The OASIS-fp6 Project

There is a recognition that current information systems used by agencies need to change in order to support improvements in operational tempo. Furthermore, there is an increasing interest within the emergency services towards using networked devices, sensors and applications from the operational command down to tactical response levels. This is to ensure that as much information on the incident can be captured and the correct decisions can be made.
Integrating different networked information sources from different organisations (both Category 1 and 2) presents the following benefits:

- Data becomes more easily accessible and can be integrated into the responders’ preferred operating environment. So incident data from police can be represented in a familiar way to the fire service using its preferred visualisation system, for example.
- Any shared data is more accurate and up to date, so there is greater trust and confidence in it when time-critical decisions are made.
- With improved data integration, Gold and Silver command officers do not necessarily need to be collocated, so response to incidents is quicker.
- Setting up third party systems for shared data becomes unnecessary and data synchronisation problems are avoided

It should be noted that technologies, such as those investigated in the OASIS-fp6 project [2] described here, are attracting interest from the emergency agency community as recent field trials in that project demonstrated. The work on interoperability within OASIS-fp6 offers great value in supporting different agencies in different countries working together to deal with a cross-border incident and where the effectiveness of voice communication may be compromised. This is a clear example of how technology stands to make a very positive impact on the emergency services decision making process.

OASIS-fp6 addressed the problem of interoperability with respect to information sharing between different responder agencies. In the European Union, the emergency services are organised separately between different countries, and even within a single country the services are fragmented. For example, in the UK the police are organized into some forty county services, which have defined statutory duties, but have considerable autonomy in how they organize and equip themselves. Consequently, even within a single region, interoperation between the various emergency services is based on co-operation procedures, and data exchange between IT systems is manually mediated, usually by re-entry of voice messages or print-outs. The latter example, however, should be understood to be due to the limitations in current system interoperability and connectivity rather than arising from any fundamental security requirements.

The OASIS-fp6 project was concerned with the development of a Common Operating Picture (COP) system to be used by the different control centres for the various emergency services, including both the permanent control rooms and mobile installations for tactical control at the site of the incident. The Tactical Situation Object (TSO) is a lightweight XML message designed to keep responders up-to-date with the situation, either through in-vehicle systems or hand-held devices. It provides details of the type of incident, control zones, casualties, resources deployed and the missions they are deployed on. This information can be used for supporting critical decisions.

Further information on the OASIS-fp6 TSO can be found in Appendix 3. Overall, one should regard any new IT technologies from projects such as OASIS-fp6 as complementing, rather than competing with, current practices based on voice communications. It is intended to aid decision making while retaining the most useful features of current systems and processes.

The OASIS-fp6 COP system offers clear advantages in sharing information between agencies in rapid time. However, not all information is relevant to an officer’s tasks or duties and so information overload from the COP is a potential risk. The problem is to make TSO information accessible to those responders who need it.

Furthermore, the TSO might have sensitive information, eg, personal details of casualties, or details of missions that other agencies are not permitted to see. Therefore, there is the
challenge of protecting some of the more sensitive information in the TSO from those officers who are involved but who have no need to know. For example, details of casualties should not be broadcast to the utility companies (ie, Category 2 responders) who are working with the Category 1 responders.

3.3. Scenario Description

With the preceding motivations and concerns in mind, a new application scenario is investigated. This is intended to exercise these new technologies and to pose more detailed requirements for data security. Before the scenario is presented, some important background information is first described in order to set the scene. The stakeholder organisations are identified along with the systems and infrastructure that would be used in the scenario. Finally, the scenario story is presented along with three main use cases concerning a) the pre-emergency phase, b) the emergency response phase, c) the post-incident phase.

3.3.1. Stakeholders

The profiles of the various stakeholders in the OASIS-fp6 system are described here. This also includes some details on their interactions or associations with the COP to provide a flavour of their duties and roles.

3.3.1.1. Organisations

At the organisation level, the stakeholders are the Category 1 and Category 2 responders as defined in the UK Civil Contingencies Act. It is assumed that each has agreed (possibly within a regional resilience forum) to co-ordinate their activities and to use the TSO as a standard means for sharing information on incidents, missions and emergencies.

3.3.1.2. Individual Users

The primary end users of the TSO will be the emergency responders. These responders may be Silver commanders in a control room who are making decisions using information displayed in a command and control system, or Bronze/tactical command officers who are at the scene of the incident (tactical level) with more limited facilities to display information from the TSO.

The emergency responders’ log into their systems and start to use the applications they need. The way this is done is not important, but it is safe to assume that systems will typically control access based on the user’s identity. This application could be running on a PDA used by a tactical command officer or on a desktop PC used by a control room officer. The application will allow the user to ask for more detailed information on a particular incident. In general, responders will not be concerned with incidents out of their area of interest, or for which they are not involved. Note that different control centres will have their own preferred applications with customised human interfaces.

The control centre systems for the Category 1 responders generate the TSOs for their particular organisations based on inputs from tactical units or from internal systems that maintain information on the current missions. Typically, the control centre staff will interact more with the COP, rather than the TSO as they prefer to have an overview of the incidents and missions associated with the emergency. Information to be input to the COP will follow incident specific procedures. Control centres for Category 2 responders may not use a COP,
but prefer to access the specific information from a TSO (or a number of individual TSOs) instead.

The people interacting with the COP and the TSO will not be IT specialists, but will simply be end users of the systems in which the COP and TSO related technologies are integrated or embedded. The data sharing policies for the TSO are likely to be defined by control centre administration staff who can be expected to have a higher level of IT literacy. These staff will assist end users in developing policies by capturing requirements, but cannot be expected to understand formal policy languages, eg, to the standard of a computer scientist.

3.3.1.3. Software Developers, Administrators and Maintainers

Other stakeholders will include software engineers and system administrators. They are not end-users of the TSO or of the COP system but are required to support and maintain it on behalf of the end users described above. The system administrators are not developers as such but are expected to have some technical competency in writing policies, scripts and other utilities that are used for their general work.

Each agency will have its preferred supplier of software systems, some of which may be bespoke to meet their requirements. It is important that these suppliers are able to update, extend or improve these applications over the full product lifecycle. In specifying the Consequence framework, it is important that any data security solution that Consequence provides must not disrupt, in any significant way, existing application architectures.

Finally, system administrators will be responsible for translating the high level organisational policies defined by management into a set of policies that can be enacted by computer and network systems. This is currently a painstaking process that may be lengthy, error prone and require rigorous testing and quality control procedures before it is successfully deployed.

3.3.2. Scenario Assumptions

3.3.2.1. Collaboration

The assumption of this document is that both operational and strategic levels of command across the two responder categories are located within their own organisational ‘domains’. The term ‘domain’ is deliberately imprecise as it does not necessarily denote a particular geographical location such as a headquarters building. It refers to all the offices, facilities, mobile command and response vehicles that belong to an organisation. Each domain has its preferred systems, applications and processes that it wishes to retain— it would not be willing to change these, for example, for the sake of a collaboration. The current procedure is for Gold command officers to be in the same room using notepads and minimal applications. It is an assumption of our scenarios that this is not necessarily the case. These and other decision makers are in their own domains using networked technologies to make their joint decisions.

The information that is shared between these organisations will be fused together, possibly with information from non-emergency agencies to form a Common Operating Picture (COP). As this information may be highly complex and detailed, condensed versions of this information are reported to Gold command.

The strategic command officers in the scenario will be in their respective organisational domains, communicating with each other using voice and/or video over a network while sharing information (missions, incidents, casualties etc) through the COP. For example,
depending on the pace at which the incident develops, these officers may be at home, abroad or travelling to their own control centres but connected to their domain systems.

### 3.3.2.2. Data Sharing Agreements

In this scenario, it is expected that there are multiple data sharing agreements between the parties before the incident begins. The normal assumption is that the timescales of emergencies generally prohibits the negotiation of a particular agreement for the incident in question. However, one of the defining aspects of a minor crisis evolving into a full blown disaster is that of a rapidly developing situation that does not conform to any of the rehearsed scenarios, requiring the rapid modification of policy to enable responders with an urgent need for specific time critical information to receive the appropriate data. A single universal agreement is unlikely as it would involve many overlapping jurisdictions. Furthermore, a Category 2 responder is a commercial organisation where the agreement must balance the risk of disclosing data that is needed for an incident and data that may be of value to a rival. It is therefore more likely that a number of separate agreements will exist between different services and between the Category 1 and Category 2 responders and can be considered as templates for local policies.

It is assumed that the agreement would be written using standard legal terms that cite the relevant legislation. It will clearly define what is to be shared, who is permitted access and under what conditions the material can be used. It would also define the protocols, duties and responsibilities of the parties within the data sharing process.

The data sharing agreement would primarily be supporting the aims of legislation such as CCA 04 (Section 2.1). Data that is related to individuals, eg, entries on evacuation lists, would be subject to DPA 98. CDA 98 is not directly related to the current scenario, but may be used in the planning of emergency response if the incident is in an area with high levels of criminal activity.

As described in the use case section below, the agreement is defined at regional or national level and may be adjusted to meet local regional needs. The agreement is intended to protect the interests of all parties and reflect the requirements of legislation. It should enumerate all points that both sides should understand when implementing the agreement.

There are two types of documents relevant to this discussion:

1. in the UK a so-called ‘data sharing protocol’ document - defining the general principles, purposes, relevant legislation and duties of the signatories when sharing data, and
2. a data sharing agreement specifying precisely what information is to be shared.

A protocol in the sense meant here often has an appendix with a pro-forma for a data sharing agreement. For brevity, we describe a single agreement that encompasses both of the above types of content. The basic format of an agreement between Category 1 responders, Police and Ambulance for example, could include:

1. A section defining the data controllers who sign the agreement from Police and Ambulance who are to implement the agreement.
2. The duration of the agreement, with review points defined.
3. The purpose of the agreement, stating why the data is being shared and what the signatories of the agreement intend to do with it. This gives a rationale for the sharing and indicates what agency tasks require the data for their successful execution.
4. The duties with regard to various legislatures. This section may cite CCA 04, DPA 98 and possibly CDA 98.
5. A section describing what types of data are to be shared, including whether personal data is to be shared or must first be de-personalised, and the treatment of data that has national security sensitivity. Other classifications of ‘document sensitivity’ may be declared in the agreement as well. In the scenario, sensitive information may include evacuation lists and lists of individuals particularly vulnerable to toxic chemical release etc.

6. A section defining the markings to be used by the document authors when identifying the classifications defined above.

7. A section defining the restrictions on material bearing these markings, eg, whether it can be viewed, modified, printed or whether it may be copied or is permitted to be disclosed to other parties without permission being sought.

8. A clear statement on how requests for disclosing material to a third party are to be dealt with.

9. What data security standards are to be used (eg, ISO17999 or BS7799) by each party in implementing the agreement.

10. Duties on the organisations with regard to the material - for example, to log access to certain types of document that include sensitive personal information, to provide justification for using the data, or to delete the documents after the emergency is finished.

11. A section with Indemnity clauses. This is used by a particular partner (the Indemnifying party) to protect a partner (or partners) from any adverse effects resulting from using or processing that data.

In the case of Category 2 responders, the agreement could be similar to above but would include ‘commercial sensitivity’ to the list of document markings.

Finally, the UK government may be implicitly involved in the scenario in the sense that it is entitled, under the provisions of CCA 04 to access data for evaluating the efficiency or performance of organisations when dealing with crises or emergencies.

### 3.3.3. Infrastructure and System Profiles

We assume a network that is composed of sub-networks (with different security classifications) and intranets that link the systems of the different agencies together. Each agency will rely on different operating systems (Windows™, miscellaneous Linux flavours, AIX, Solaris) and software technology platforms (Java, .NET, Python, etc). It is likely that budget and software procurement policies may limit the type of system and infrastructure that can be used.

The following table summarises the characteristics of the systems and infrastructure used through the scenario. Three infrastructure ‘tiers’ are identified:

- **Tier 1**: Responders within the immediate vicinity of the incident
- **Tier 2**: Control centres coordinating the responses from the Tier 1 groups
- **Tier 3**: Ancillary organisations providing services and information to Tier 2 control centres.

<table>
<thead>
<tr>
<th>Tier</th>
<th>Network Properties</th>
<th>Systems</th>
<th>Users</th>
<th>Operating Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ad-hoc, peer-to-peer, low bandwidth, intermittent connectivity</td>
<td>Mobile phones, PDAs, head mounted displays, laptops, in-vehicle PCs, video camera</td>
<td>Police, Fire, Ambulance officers at the scene of the incident</td>
<td>High tempo activities at the emergency scene</td>
</tr>
</tbody>
</table>
and microphones.

<table>
<thead>
<tr>
<th>Tier</th>
<th>Infrastructure and System Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Medium to high bandwidth, mixture of restricted network (eg, VPN) and public networks, high availability</td>
</tr>
<tr>
<td>3</td>
<td>High bandwidth, high availability, public network</td>
</tr>
</tbody>
</table>

**Table 2 Summary of Infrastructure and System Profiles**

Tier-1 has the most stringent performance requirements as it is directly involved with the incident and may have limited resources. These considerations may have priority over security requirements. Data may be cached and distributed using a smart peer-to-peer distribution algorithm, and is updated whenever high performance networks are detected.

Tier-2 infrastructure has a critical connection with Tier 1. Tier 2 is required to supply near real time data to Tier 1 responders and request/receive soft real time (5 minutes or so) data from Tier 3 in order to make assessments of potential threats. The ability to manage multiple Tier 1 responders with different data sharing policies is also a possibility. The following picture shows the relationships between the different infrastructure tiers in the scenario.

![Diagram of infrastructure tiers](image)

**Figure 1 Infrastructure and systems supporting the scenario, represented as a tier**

Further details can be found in Appendix 7.

A final point to note is that the infrastructure is composed of a mixture of different kinds of network where transport level security is difficult or may not be guaranteed. This implies that data level security should be used instead and so the aims of the Consequence are highly relevant here.
3.3.4. Scenario Application Architecture

The following diagram shows a simple application architecture for the scenario.

![Diagram of Scenario Application Architecture]

**Figure 2 Scenario Application Architecture**

The systems used by the various agencies are exposed as services and the various clients (responders and control room staff) have appropriately modified applications for using these services. The services owned by Police, Ambulance and Fire (PAF) and British Transport police export Tactical Situation Objects.

Access to TSOs is granted to responders according to access policies. Other Category 2 responders expose interfaces to their legacy systems- referred to as sources of ‘asset information’. For example, the Gas Utility would allow control room officers in the Fire service to view critical gas pipe routes, pressure distributions over an area etc, in the vicinity of the incident. Control room operatives can access both TSOs and information systems exposed by utilities and other Category 2 responders.

Note that the clients all make requests for information - the arrows indicate the direction of the request to the relevant service. The data returned is indicated as either a TSO or asset info document.

A more detailed description of the application architecture is given in Appendix 5.

3.3.5. Scenario Story

The scenario describes a vehicle accident in Bristol which rapidly escalates into a major incident. To be effective in the face of a major incident, the responders must be familiar with the systems involved, and, so the same system should scale from ordinary, day-to-day use to
responding to a major incident. The scenario aims to show this progression, and is located to bring in a wide range of possible responders.

Figure 3 below presents the scene.

![Figure 3 Crisis Management Scenario Picture](image)

The scenario is set at a bridge where Muller Road, a major road (A), is crossed by an important railway line. The immediate neighbourhood (within 50 m) is an open area used for allotments and a small DIY warehouse store. There is a small stream passing which is culverted as it passes under the road. The broader neighbourhood is mainly high density Victorian suburbs, and there are at least five schools within a kilometre of the site. There are also major infrastructure installations, including two sets of gas holders, an large electricity substation and a communications tower. There is also a specialist hospital, numerous nurseries and crèches and specialist residences for old people and the handicapped. The local geography means that the East-West routes are very restricted and Muller Road is the only major crossing of the railway between the M32 in the south to the ring road 3 km to the north. Consequently, this is an important access route for the emergency services.

The scenario plays out over a forty five minute period on a wet Wednesday morning. The eastbound traffic is backed up from the M32 junction almost the whole length of Muller Road, although westbound the traffic is clear until it reaches Gloucester Road in the West.

**Stage 1:** At 08:32 a call comes in to the police and ambulance services reporting a car "getting bashed" between a couple of lorries under the Muller Road bridge. There could be a couple of casualties. Police and Ambulance both dispatch response vehicles, and the Fire Service is alerted though the appearance of the incident in the COP.
Stage 2: A paramedic arriving from the East of the city and already close to the area calls in at 08:34. She reports that initial triage indicates one yellow and three green casualties (ie. one ambulance is needed). However, one of the vehicles is a petrol tanker, which is slewed across the road and there is a strong smell of petrol. The second lorry also seems to be a tanker, but is inaccessible because of the first slewed tanker. The Fire Services are following developments via the COP and despatch a unit.

Stage 3: The police arrive from the west at 08:42, and find several cars have concertinaed behind the second tanker, making it impossible for it to move. Concerned about the leak of petrol, they start clearing people from their vehicles. A second police vehicle is assigned to divert vehicles off Muller Road at the traffic lights 0.5 km further west. The Fire Service is arriving from both directions when the petrol tanker catches fire and there is a small explosion. The Police control centre is already in the process of alerting Network Rail and British Transport Police about the threat to the railway.

Stage 4: At 08:47, the second tanker is observed to be on fire, and both leaking some unknown chemical and spewing thick white smoke. The fire crews have donned breathing apparatus until the nature of the chemicals is established. A goods train is observed to have stopped on the railway above. An evacuation of the immediate area (100m cordon) is ordered.

Stage 5: A second small explosion has increased the rate at which smoke is spewing from the chemical tanker, and bystanders and unprotected responders are being affected by the fumes. At 08:56 the decision is taken to evacuate an area of 500 m around the incident, with planning to extend the cordon to 1 km. Additional Fire Service personnel with breathing apparatus are called in to support at the incident ground, and the police services from the adjoining constabulary are asked to provide cover since the local officers are fully engaged.

Stage 6: At 09:02, the goods train is identified as carrying a variety of flammable chemical for disposal though Avonmouth (a port approx 10km north of Bristol), some of which may contain highly toxic admixtures. The fear is that if this train catches fire, the resulting plume could involve evacuating a large portion of Bristol - say 120,000 people. Planning is put in place to close the M4 between Newport (20 km West) Swindon, (60km East). The central government COBR committee is alerted. Contacts are made with the Disaster Monitoring Constellation to identify whether satellite observations would be available to track plume dispersal.

Stage 7: At 11:15 the fire is reported under control and cooling water sprayed on the second tanker has eliminated further fumes. A heavy shower has washed the plume out, and evacuation plans have been scaled down. There is concern that the water run off from the scene has got into the local stream, and a pollution monitoring team is being called in by Fire. Traffic throughout the Bristol area is in chaos.

Stage 8: At 20:15 the scene is declared safe, the fire is out and the vehicles cooled, and spilled petrol and chemicals have been contained and removed from the site. Muller Road remains closed for decontamination.

Stage 9: At 07:00 Thursday the incident is declared closed and Muller Road reopened for traffic. There is some remaining decontamination to be done, and several families from nearby houses have had to be accommodated by the council while this is completed.

(Stage 10: Some weeks later, the incident investigation panel read the TSOs to establish the course of events, and prepares extracts from them for presentation in a court case.)
3.4.  **TSO Threat Analysis**

The TSO contains information about incidents and operations. This information can be misused in two ways: for general public dissemination or for malicious or criminal use.

General public dissemination may have two adverse effects. Firstly, it may alert people who want to loiter at the site and who thereby interfere with incident management. It is assumed that the media will not be permitted to have direct access to TSOs, but will be briefed about incidents by a press liaison officer. Secondly, in the case of a serious incident, especially one that risks a chemical or radioactive material release, it may cause panic among the local population if it is released at an inappropriate time.

Examples of potential malicious misuse of TSO information include attacks on fire engines attending a fire, or attracting protesters when police attend an incident, as in times of tension in the French 'banlieu chaud'. Examples of criminal misuse could include co-ordination of rioters or the targeting by burglars of homes where an ambulance has made an emergency call.

Another threat is from interception of the TSO within the potentially poor connectivity of the Tier 1 area. It is here that sharing of TSO data is most ‘promiscuous’ in order to meet demanding real-time operational requirements. TSOs may therefore be sanitised of sensitive data before release into Tier 1, although the definition of what types of data are sensitive may well change during the course of an operation. However, the capability to dynamically redefine data as sensitive or non-sensitive brings with it a potential hazard as well as a requirement that may be difficult to meet. For example, the declassification of the patients attending genitourinary medicine (GUM) clinic within the evacuation area during a flood alert may need to be time-bound to the duration of the alert even though the data would be essential to coordinate rescue services. It would be an unintended consequence if the patient list was then available to the personnel department of one of the utility companies for cross-referencing with their employee records.

With respect to the distribution of information to Category 2 responders, it is assumed that there is more potential for misuse or information being compromised through typical threats-ranging from viruses and spy-ware through to sophisticated social engineering attacks.

3.5.  **Scenario Phases**

The use cases considered here consider a) the pre-incident phase, where data sharing agreements are setup, b) the incident phase where information is shared according to these agreements, and c) the post-incident phase where an analysis of the incident is done and access is required to historical data.

3.5.1.  **Category 1 Control Centre- Data Sharing Agreement and Access Policy Definition**

Prior to the incident, a variety of data sharing agreements have been set up between the agencies. In this respect, the local control centres have a great deal of influence on how the access policies for TSO access are to be defined: they are also granted the right to modify the policy during the incident if it is expedient to do so.

It is assumed in this scenario that a pre-defined set of policies, derived from data sharing agreements, are used throughout the scenario and that general policies (and associated data sharing agreements) will be defined at regional or national levels, with the local control centres defining parameters such as operation cells over which units are alerted.

The following list is a selection of the agreements that are in place prior to the incident:
1. Police-Ambulance
2. Police-Fire
3. Fire-Ambulance
4. PAF-Local and Regional Councils
5. PAF- Network Rail
6. PAF-Gas utilities

Section 3.3.2.2 proposes a general structure for a data sharing agreement. The following table indicates the relevant content of these agreements.

<table>
<thead>
<tr>
<th>ID</th>
<th>What is shared</th>
<th>Access Restrictions</th>
<th>Purpose</th>
<th>Legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-3</td>
<td>1) TSO data</td>
<td>For each type of TSO event, who can access it, when and where it can be accessed</td>
<td>Coordinated response to incidents and to fulfil legislative duties</td>
<td>CCA 04</td>
</tr>
<tr>
<td>4</td>
<td>1) TSO Data. 2) Personal data held by the council on members of the public.</td>
<td>For each type of TSO event, who can access it, when and where it can be accessed. Personal information to be accessed by responders at the scene and by particular council officer roles.</td>
<td>To protect human life through evacuation</td>
<td>CCA 04, DPA 98</td>
</tr>
<tr>
<td>5</td>
<td>1) Train locations + cargo contents in the vicinity of an incident.</td>
<td>PAF Commanders, Control centre operatives assigned to the emergency only.</td>
<td>For identifying risks to general population during an incident</td>
<td>CCA 04</td>
</tr>
<tr>
<td>6</td>
<td>1) Gas pipe routes and gas distribution information in the vicinity of an incident.</td>
<td>PAF Commanders, Control centre operatives assigned to the emergency. To be accessed in emergency situations only.</td>
<td>To prevent damage to critical infrastructure, to maintain economic continuity</td>
<td>CCA 04</td>
</tr>
</tbody>
</table>

**Table 3 Table of Data Sharing Agreements**

Regarding TSO data (referred to in agreements 1-4), the access restrictions specify what can be shared, where, when and by whom it can be accessed. For the case of TSO data, the use case below in Section 3.5.2.1 describes the TSO access permissions that are active as the scale of the incident changes over time. All of these permissions ultimately derive from the above data sharing agreements.

For personal data such as individual names, addresses, health and mobility information, these can only be shared if it is asserted to be in the interests of the individual. Other information is not likely to be of relevance to Police, Ambulance and Fire, so access to this data would not be part of the agreement. Generally speaking, only responders assigned to the incident would be permitted access to this information during the course of the incident.

For information held by utilities (agreements 5+6), the restriction is that the data should be only used by selected control room staff, eg, by Fire control room officers only.

Other ingredients of the DSA include:

1. printing restrictions- ranging from constraints that certain TSOs should not be printed or may be restricted to a printer in the vicinity of the client, or possibly a printer with PIN protection
2. any shared data to be rendered inaccessible after the incident has ended
3. recognised security standards to be enforced in the protection of the data (eg, ISO1799 or BS7799)

4. a shared vocabulary defining the meaning of terms used in the agreement, for eg., ‘control centre’, ‘mobile HQ’ etc.

5. an obligation to log access to certain material.

These agreements are negotiated at ‘board room level’, ie, between contracts specialists, using conventional document management systems. The expectation here is that the negotiators create and exchange text based material that does not contain any obscure technical content. The term ‘negotiation’ here is meant the exchanging of copies of agreements between parties. The negotiators may use ‘contract templates’ to facilitate the process of composing these agreements. ‘Templates’ in this context refer to reusable document fragments and legal constructions that encapsulate best legal practice, reduce chances of errors and save time spent in composing agreements. During this negotiation phase, existing agreements and legislation are compared with the new proposed agreement and contradictions and discrepancies are detected and reported to the negotiators. The negotiation proceeds and has the goal of a) satisfying the interests of all parties, b) resolving any contradictions and conflicts with existing agreements or legislation. Once these issues are resolved, the signed agreement is stored within the business systems of the respective partners. This becomes the authoritative legal document that determines how shared material is protected when it passes over organisational boundaries.

The event of storing the final version of the agreement initiates a reconfiguration of security systems and processes within each organisation. This is in order to enforce the rules specified in the agreement when covered by the agreement are shared.

As an extension of this use case, it is possible that the centres modify the deployed policies according to the incident, eg. by identifying explicitly that the incident should include the British Transport Police. This would require that any change to the policy be authorized by the control centre manager and distributed, and that this authorization and distribution is logged.

### 3.5.2. Category 1 Local Control Centre - Read Access

The main Category 1 responders - police, fire and ambulance - maintain control centres to keep track of incidents and their resources. Local control centres for the Category 1 responders include both the static control centres which are responsible for the day-to-day operation of the service and temporary centres located at or near an incident.

The local control centres maintain a Common Operating Picture (COP) and generate the TSOs. They define the area over which the TSO is distributed. They may also close the incident, at which point it is deleted from the COP, and so no longer generates TSOs. They also maintain a secure log of all TSOs distributed.

In this use case local control centres can read all TSOs throughout the incident (stages 1 to 9), including TSOs from centres from the other services and from adjacent regions. Whether these are displayed will depend on the nature of the incident and the local situation. Note: for inter-control centre communications, the TSO provides the minimum of situational awareness information. The centres may use other messaging systems for higher levels of common situational awareness, but equally, these require closer co-ordination of the COP systems in use.
3.5.2.1. Summary of TSO Access Use Cases

The main set of use cases is where a user requests to read a TSO during the lifetime of the incident. The system can refuse access, or grant access to some or all of the parts of the TSO, depending on the type of incident and the information that the user needs to know. In the scenario, the information sharing needs change as the scenario develops, and the responder summary table shows this for a variety of responders and for different stages in the scenario. The TSO is split into four major sections (described in Appendix 2), with separate access rules for each section. Within these sections, there may be further security restrictions. The restrictions that are relevant here are

- Event:
  - Event identification and type;
  - Event location and relation to other events;
- Resources and Mission:
  - Restriction – for a specific responder, show only their own details and the missions they are mentioned in (do not show other responders) (control by responder identity)
  - Restriction - a control centre that owns resource is permitted to be shown the details of both the resources they have provided and the missions assigned to these responders (control by responder attribute);
  - Restriction - show all resources and missions (free access to all information);
- Casualties;
- Evacuees.

In the table below, the use cases are summarised as a four character code, with the interpretation that a user can read only those data that they have a code for.

<table>
<thead>
<tr>
<th>E/D</th>
<th>Event type / event Details - type, location, relation to other events</th>
</tr>
</thead>
<tbody>
<tr>
<td>S/O/A</td>
<td>resource and mission: Self only (responder) / Own (control centre) / All</td>
</tr>
<tr>
<td>C</td>
<td>Casualties</td>
</tr>
<tr>
<td>V</td>
<td>Evacuees</td>
</tr>
</tbody>
</table>

Table 4 Responder Code Values used in the Use Cases

For emphasis, the first three use case entries are responders (eg. patrol vehicles, fire engines, etc) are coded yellow in the table. The remainder belong to two types of control centres. The first of these are the other Category 1 responders (colour coded in green) and the second the Category 2 responders with the colour code blue. Where users have a similar profile, only one line has been shown - for example, it is assumed that the ambulance and fire services have a similar profile.

The term "Local" refers to the organization that has jurisdiction over the incident, to be contrasted with "Area", referring to equivalent organizations in the surrounding area. In the scenario, Avon and Somerset Police would be the local responder, and South Gloucester Police, whose jurisdiction starts 2km to the North, is an "Area" responder. In practice, of course, the Restrictions would allow a wider range of tactical events to be defined, the policies would be far more complex and the resource descriptions would be extended to include a wide range of responder types eg. NGO, military and country-specific descriptors.
<table>
<thead>
<tr>
<th>Responder</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Police Responders</td>
<td>DACV</td>
<td>DACV</td>
<td>DACV</td>
<td>DACV</td>
<td>DACV</td>
<td>DACV</td>
<td>DACV</td>
<td>DACV</td>
<td>DACV</td>
<td>-</td>
</tr>
<tr>
<td>Area Police Responders</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>E</td>
<td>DO</td>
<td>E</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Local Fire Responders</td>
<td>-</td>
<td>DOCV</td>
<td>DOCV</td>
<td>DOCV</td>
<td>DOCV</td>
<td>DOCV</td>
<td>DOCV</td>
<td>DOCV</td>
<td>DO</td>
<td>-</td>
</tr>
<tr>
<td>Area Police Control</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>E</td>
<td>DO</td>
<td>DO-V</td>
<td>DO</td>
<td>E</td>
<td>-</td>
<td>DACV</td>
</tr>
<tr>
<td>Transport Police</td>
<td>-</td>
<td>-</td>
<td>D</td>
<td>EO</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>E</td>
<td>DO</td>
</tr>
<tr>
<td>Coastguard</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Local Council</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>E</td>
<td>D--V</td>
<td>D--V</td>
<td>D--V</td>
<td>D--V</td>
<td>D--V</td>
<td>D--V</td>
</tr>
<tr>
<td>Area Council</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>E</td>
<td>E--V</td>
<td>E</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Port Health Authority</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>D</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Local Health</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>E</td>
<td>E-C-</td>
<td>E-C-</td>
<td>E-C-</td>
<td>E-C-</td>
<td>-</td>
<td>E-C-</td>
</tr>
<tr>
<td>Health Protection Agency</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>E</td>
<td>E-C-</td>
<td>E-C-</td>
<td>E-C-</td>
<td>E</td>
<td>E</td>
<td>E-C-</td>
</tr>
<tr>
<td>Environment Agency</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>E</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>E</td>
<td>D</td>
<td>-</td>
</tr>
<tr>
<td>Electricity Distrib.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>E</td>
<td>D</td>
<td>E</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Water and Sewage</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>-</td>
</tr>
<tr>
<td>Telephone Service</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>E</td>
<td>D</td>
<td>E</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Network Rail</td>
<td>-</td>
<td>-</td>
<td>D</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>E</td>
<td>DO</td>
</tr>
<tr>
<td>Train Operating</td>
<td>-</td>
<td>-</td>
<td>D</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>D</td>
<td>-</td>
</tr>
<tr>
<td>Highways Agency</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>E</td>
<td>D</td>
<td>E</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Health and Safety Exec</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>E</td>
<td>E</td>
<td>D-CV</td>
<td>D</td>
<td>E</td>
<td>E</td>
<td>D-CV</td>
</tr>
</tbody>
</table>

Table 5 TSO Access Use Cases by Responder and Incident Stage
It is assumed here that the local police will normally take control in major incidents like this, and have full information throughout the incident. The fire service responders, since they will be involved in the physical rescue of the injured, are also fully informed once the incident escalates beyond a police-only matter. Police responders drafted in from the surrounding forces become aware only when it is likely to affect them, and get details only if they are tasked to respond to the incident.

The regional police control rooms for the surrounding constabularies are alerted when the incident starts to increase to a significant scale, so that they can be prepared to support, either by taking on duties for the local constabulary, or by actually providing resources directly to the emergency. It is assumed that they need keep track of their own units, since detailed control will remain with the responsible force. However, the scenario also shows an external force being put in charge of the subsequent investigation, and so needing access to all the TSO.

The Coastguard is never involved in this scenario, and the Port Health Authority is made aware of the incident only when it looks like becoming a regional emergency that includes Avonmouth. The local authority typically provides the control centre for major emergencies, as well as taking responsibility for re-housing evacuees. In the case of the largest scale emergencies, they would be supported by the authorities from surrounding districts.

The local health authorities need to be aware of large and major emergencies in order to make treatment facilities available, to free up beds if needed, and to call in off-duty health care professionals. In doing this, they may also use other emergency messages, such as the OASIS-open standard for Hospital Availability (HAVE), and may use similar policy-based access controls for such messages.

The Environment Agency initially becomes involved because of the proximity of a water course (the stream), but will later have more extensive monitoring and assessment responsibilities, following the release of the chemicals.

Control centres for utilities, such as electricity and gas distribution, are made aware of the incident only when the incident starts to affect a significant area. In this case, it is evident that they also happen to have important facilities in the affected area. The water and sewage services are made aware much earlier, since the incident involves a chemical spill and they need to be aware of the risk of it entering the sewage system.

The proximity of the railway also requires the alerting of Network Rail and the train operating companies, not least because they need to stop trains entering the sector.

### 3.5.2.2. TSO Access Policies

The aim of this section is to identify the data sharing requirements under which an organization should receive TSOs, and the policies which would achieve this. The ‘policies’ described here are not prescribing the structure and content of either the formal or enforceable policies that are explored elsewhere in the Consequence Framework. Instead, they are intended for exploring the requirements for Consequence in greater detail by means of informal “if-then-else” rules that control TSO access.
To aid this investigation of policies, we first focus on two particular examples that are outside the scenario, namely that of exercise (or ‘drill’) and test activities. The affect of ‘incident-scale’ discussed in Appendix 3 is explored in this preliminary analysis along with the topic of how location constraints are specified. With this done, policies for the scenario are then proposed.

The data sharing requirement identifies why it is necessary for an organization to receive TSO data and what criteria are used in making that decision. The policies as used here are identified as predicates against the TSO data elements. In some cases, these are defined against roles or functions, rather than against whole organizations, as the policy for an organization will depend on its function.

In what follows, it is assumed that there are three structures that may be used in policy evaluation: the policy, the TSO and the unit or team that will use the TSO. In the case of the TSO, this is an XML structure, and the elements are prefixed TSO, and are identified in the TSO structure standard. In the case of the policy and the unit, for simplicity these are also treated as TSO structures.

An exercise is a test of the organizational response to an emergency situation. In general, only specific units allocated to the exercise will respond. A unit will be able to access exercise TSOs only if it is involved with that particular exercise.

There are three options towards defining an ‘exercise’ policy:

1. The units are explicitly identified in a policy for exercises distributed to all units;
2. The TSO explicitly identifies the units as resources in the resources section of the message.
3. The units are provided with an "exercise token" which is part of a standard policy

In all cases, the policy must include a guard condition of the form:

if (TSO.context.mode = "EXERC"") AND X then -- TSO read allowed

where

context.mode is the mode sub-element in the context element of the TSO, and
X is the secondary condition (described below)

Options 1 and 2 require that units know their own identity as a resource, and consequently, there is a resource identification standard for supplying identities to units. These would either be static identities (eg. for a fire engine, programmed in to the vehicle’s TSO system), or dynamic (eg. for a crew member, who logs in to a vehicle TSO systems). In option 1, the secondary guard clause would take the form:

(∃ p a policy s.t. unit.identity in {p.exercs-list})

where

unit.identity is the unit identify provided by the unit;
the policy p is one of the currently applicable policies;
{p.exercs-list} is a set of unit ids listed by policy p as being part of the exercise.

In option 2, the secondary guard condition would take the form:

(∃ r a Resource element s.t. TSO.r.id = unit.identity)

where
r is a resource element of the TSO;
\(r.id\) is the identity sub-element of the resource element;
\textit{unit.identity} is the unit identify provided by the unit.

In option 3, the TSO system would need to distribute exercise tokens at the beginning of an exercise, and the TSO reader in a unit would need to store that token. In this case the secondary guard condition would have the form

\((\text{unit.exercs} \neq \text{null})\)

A test is a technical test of the system, and is ignored by all responders. However, from the system maintenance and testing viewpoint, each unit must be testable. This implies that the TSO reader must be able to be explicitly set into a TEST mode, and that policies include a guard condition of the form

\text{if (unit.test) then -- TSO read allowed}

A number of policy decisions will depend on the position of the event, the geographic area it is significant for, and the location of the recipient.

The EDXL Distribution Element (see Appendix 3 for a description) provides a regional boundary for the distribution of the TSO. This can specify the region by one of the following:

- Circle
- Polygon
- Country
- Subdivision (of country)
- UN Location Code

The TSO itself provides geographical location of the event. It can specify a position as a point, line, circle, surface, grid, polygon and ellipse, though only point, circle and polygon are likely to be used to specify the location of an event. The XML structures for such geographic elements are sequences of optional elements (rather than a choice of one), for which the semantics is not clear, however it is assumed that the message will use exactly one type of location.

The specification of Country, subdivision and UN Location Code are all based on ISO 3166, which provides a two digit code for each country. The coding systems for subdivision and UN Location Code suffix the country with a three letter code representing usually an administrative area or town.

The geographical positions are specified by latitude and longitude. The TSO may also specify height, but this is probably not relevant for location based access-control policies. Translation from other co-ordinate systems, such as a map grid, would be provided as a service if needed.

It is assumed that a fixed unit, such as a control room, knows where it is both as a latitude and longitude, and by location code. It is also assumed that mobile units "know where they are", for example, they have built in GPS. In the case of location codes, it is assumed that either they have a default (static) code for the area (city, country) they are expected to patrol in, or that there is a service to convert the GPS into a location code.

From the computation viewpoint, it is further assumed that there is a service that compares locations, returning

- \textit{in} if the unit is inside the area or region designated
- \textit{on} if the unit is "close to" a designated point or region boundary
• *out* if the unit is not close to the designated point, or outside the region boundary
The concept "close to" has a minimum value determined by the accuracy of the location
service, but may be defined more broadly if necessary. For example, for a subdivision
corresponding to a city, it may include the surrounding suburbs. The scale of the incident will
affect the "close to" calculation, but note that, for example, a major disaster is of significance
if it occurs anywhere in the same country, or in adjoining countries.

The policies based on proximity to an incident will therefore take the form:

```plaintext
if (compare (unit.location, designated-location, TSO.event.scale) = in) then
  -- TSO read allowed

or

if (compare (unit.location, designated-location, TSO.event.scale) ≠ out) then
  -- TSO read allowed
```

In addition, control centres (treated here as a subtype of unit) will have a designated area of
responsibility, and use the compare function to see if they have direct responsibility for an
incident or should take notice of an incident. These policies would take the form:

```plaintext
if (compare (designated-location, control.location, TSO.event.scale) = in) then
  -- TSO read allowed

or

if (compare (designated-location, control.location, TSO.event.scale) ≠ out) then
  -- TSO read allowed
```

where

designated-location is either DE.targetArea or TSO.EGEO.POSITION

```plaintext
compare(a, b, scale) returns

• in when a ∩ b ≠ ∅
• on when a ∩ b* ≠ ∅
• out when a ∩ b* = ∅
  o where b* is b extended by its boundary zone, dependant on scale
```

A police patrol car will generally be made aware of all police related incidents in its
immediate area, and of any significant incidents in the general area. In the context of a GIS,
this provides awareness of where other patrol cars are and of any areas that may need to be
avoided. The policies will change depending on the scale of the incident and the regions of
responsibility of the constabulary (see Appendix 3).

It is assumed that for minor incidents (scales 1 & 2) the distribution of the TSO is limited to
the boundaries of responsibility of the control centre generating the TSO. This leads to the
following sequence of data sharing requirements and policies

**Scale 1:**

A scale 1 incident is a minor, day-to-day incident that would be ignored by patrol cars not
directly involved. It is assumed that a patrol car will need visibility of a TSO if it is generated
by its own control centre, and it is close to the incident (eg. within 2km), or it is a designated
resource to respond to an incident.
A police car will need visibility of a TSO generated by another control centre and it is
designated as a resource to respond to the incident, either in that TSO, or in TSO generated by
its own control centre and citing the other TSO as the main event.

Note: the operational details of how a TSO will be used may vary from region to region.
However, it is assumed that when a unit is allocated to an event, then either it is recorded in
an update of the original TSO or by creating a sub-event linked back to the original TSO. This
may be the preferred option when the TSO originates with a different organization, for
example, when the fire service calls on the police to provide crowd control at a fire. Note that
this policy is concerned with whether the unit reads the TSO, not whether it actually responds
to it.

This leads to the following policies:

**pc1-1:** if (scale=1) AND
(unit.control_room = TSO.ORIGIN.org_id) AND -- generated by unit's control
(compare(unit.location, TSO.EVENT.EGEO.POSITION, 1) = in) then
--- read TSO as unit is near event

**pc1-2** if (scale=1) AND
(unit.control_room = TSO.ORIGIN.org_id) AND -- generated by unit's control
(∃ TSO.RESOURCE.id s.t. TSO.RESOURCE.Id = unit.id) then
-- read TSO as unit is asked to respond by it's own control room

**pc1-3** if (scale=1) AND
(∃ TSO.RESOURCE.id s.t. TSO.RESOURCE.Id = unit.id) then
-- read TSO as unit is asked by some control room to respond

**pc1-4** if (scale=1) AND
(∃ TSO.RESOURCE.id s.t. TSO.RESOURCE.id = unit.id) AND
(TSO.EVENT.main_event_id ≠ ∅) then
-- read TSO where TSO.CONTEXT.id = this.TSO.EVENT.main_event_id
-- this is the situation where the unit is tasked through a subsidiary TSO

Note, the second policy pc1-2 is redundant, as pc1-3 will be true whenever pc1-2 is true,
however it reflects one of the data sharing requirements.

**Scale 2:**
A scale 2 incident is a more significant incident, but one that can be dealt with by the local
resources without outside aid. This can include more significant incidents such as a tanker
fire.

It is assumed that a patrol car will be made aware of any scale 2 incidents in its vicinity (say,
within 5km) and within the area of its constabulary's authority, whether it is being asked to
respond or not. This requirement adds an additional policy (pc2-2) over the previous scenario.

This leads to the following policies:

**pc2-1:** if (scale=2) AND
(unit.control_room = TSO.ORIGIN.org_id) AND -- generated by unit's control
(compare(unit.location, TSO.EVENT.EGEO.POSITION, 2) = in) then
--- read TSO as unit is near event

pc2-2 if (scale=2) AND
(unit.control_room ≠.ORIGIN.org_id) AND -- generated by another control
((compare(unit.location, TSO.EVENT.EGEO.POSITION, 2) = in) AND)
(compare(unit.authority_area, TSO.EVENT.EGEO.POSITION, 1) = in))
--- read TSO as unit is near and it within the bounds of its constabulary's areas
-- Note - in the second compare, the area is limited to the immediate of
-- competence

pc2-3 if (scale=2) AND
(unit.control_room = TSO.ORIGIN.org_id) AND -- generated by unit's control
(∃ TSO.RESOURCE.id s.t. TSO.RESOURCE.Id = unit.id) then
-- read TSO as unit is asked to respond by it's own control room

pc2-4 if (scale=2) AND
(∃ TSO.RESOURCE.id s.t. TSO.RESOURCE.Id = unit.id) then
-- read TSO as unit is asked by some control room to respond

pc2-5 if (scale=2) AND
(∃ TSO.RESOURCE.id s.t. TSO.RESOURCE.Id = unit.id) AND
(TSO.EVENT.main_event_id ≠ ) then
-- read TSO where TSO.CONTEXT.id = this.TSO.EVENT.main_event_id
-- this is the situation where the unit is tasked through a subsidiary TSO

Scale 3 and upwards:
A scale 3 incident is one which needs support from neighbouring regions, a scale 4 incident
needs resources from the whole country (a recent example being the UK Bunsfield fire) and
scale 5 needs an international relief effort.

In terms of policies, the main difference is that the distribution area for the TSO can be
assumed to be larger than the local administrative boundaries, and hence, if the patrol car can
receive the TSO, it should read it. Effectively, this replaces the scale 2 policy pc2-2 with

pc3-1 if (scale ≥ 3) then -- read TSO.

Note, although still applicable as matching data sharing requirements, if the scale 3
equivalents of pc2-1 and pc2-3 to 5, then pc3-1 will also be true, which makes them
redundant.
Scenario Policies

With the preceding findings in mind, specific policies within the scenario are now considered. First of all, the scenario describes the risk of pollution to the water course and the subsequent sharing of TSOs with the Environment Agency. The data sharing requirement here is that the Environment Agency should be alerted to all incidents in which water pollution occurs, or in which there is a significant risk of it occurring. This is interpreted as referring to situations where there is a significant incident near a water course, including road accidents and fires, as well as incidents involving chemical spills. The unit being alerted is the control centre, and it is its job to make a decision as to whether it should respond. It may then allocate specific resources to respond to the incident. This illustrates the case of an organization that needs to respond to certain types of incident, or where the risk is identified through the physical environment.

This leads to the following policies:

wp1-1 if (unit.type = control-centre) AND (TSO.EVENT.scale = 1) AND (compare(unit.authority_area, TSO.EVENT.EGEO.POSITION, 1) = in) AND (∃ category s.t. TSO.EVENT.ETYPE.category in {POL, EXP/CHM, FLD}) AND -- event is pollution, chemical explosion or flood (∃ loctype s.t. TSO.EVENT.ETYPE.loctype in {COAST, INW, ROAD}) OR -- and the event occurs on the coast, inland waterway on a road (∃ actor s.t. TSO.EVENT.ETYPE.actor in {BEV/NRES/XPL, VEH/TRK/HAZ}) then -- a tanker with hazardous materials -- read event summary

The following policy describes minor incidents in which there is a particularly high risk of pollution.

wp1-2 (unit.type = control-centre) AND (TSO.EVENT.scale = 2) AND (compare(unit.authority_area, TSO.EVENT.EGEO.POSITION, 1) = in) AND (∃ category s.t. TSO.EVENT.ETYPE.category in {POL, EXP, FLD}) OR -- event is pollution, explosion or flood (∃ loctype s.t. TSO.EVENT.ETYPE.loctype in {COAST, INW, ROAD}) OR -- event occurs on the coast, inland waterway on a road (∃ actor s.t. TSO.EVENT.ETYPE.actor in {BEV/IND - industrial BEV/NRES - storage and non-residential VEH/TRK/HAZ}) then -- read event summary

The categories of notification are broadened to include any significant incident in industrial or storage premises.
wp1-3  \( (\text{unit.type} = \text{control-centre}) \text{ AND } (\text{TSO.EVENT.scale} = 3) \text{ AND } (\text{compare(unit.authority\_area, TSO.EVENT.\text{EGEO.POSITION}, 2) = \text{in}}) \text{ then} \)

--read event details

Significant event, which the control centre should be aware of, at least in case of secondary incident.

wp1-4  \( (\exists \text{ TSO.RESOURCE.id} \text{ s.t. TSO.RESOURCE.Id} = \text{unit.id}) \text{ then} \)

--read TSO as control centre of unit is asked by some control room to respond

A train operating company will need to be informed when any significant incident occurs on or near a railway, which may potentially disrupt the operation of the network. The following policies apply to the rail control centre

to1  \( (\text{TSO.scale} \geq 2) \text{ AND } ((\text{TSO.EVENT.\text{ETYPE.actor}} \in \{/\text{VEH/TRN}\}) \text{ OR } -- \text{a train involved} ) \text{ OR } (\text{TSO.EVENT.\text{ETYPE.loctype} = \text{RAIL}}) \text{ OR } -- \text{on or near a railway} ) \text{ OR } (\text{TSO.RESOURCE.id} = \text{unit.id})) \)

It is clear that the form of the policies may become complex when attempting to deal with some of the possible incidents that occur.

### 3.5.3. Category 1 Control Centre – Post Incident Investigation

The control centres are responsible for maintaining the COP, including identifying the incident and recording reports of casualties and evacuees. They are also responsible for allocating resource identities, and for generating resource allocations and missions reported in the TSO. All of this information may be required in subsequent incident analysis (stage 10).

The control centres will provide TSO logs for incident investigation and follow-up (stage 10). These logs may have associated access policies which will be separate from the operational policies. There will probably be general policies dependant on the nature of the investigation - eg. general statistical analysis by the local service, access to academic investigators, records for use in a court of law.

Specific policies may be needed for an inquiry into a major incident, which would allow designated investigators extensive access for a limited period of time during their work. The organizations leading the investigation would be permitted to designate both their own and related staff in their own organisations to whom they delegate temporary access rights.
4. Requirements Arising from the Scenario

The requirements specified here use keywords recommended in [1]. The following terms will be used when expressing the individual requirements:

- “MUST/REQUIRED/SHALL” must always be met,
- “SHOULD/RECOMMENDED” acknowledges that a requirement may not be practically met, but the reasons for not implementing it must be clearly recorded
- “MAY/OPTIONAL” a purely optional requirement
- “IS DESIRABLE” a stretch requirement that is not critical but enhances a solution, making it more attractive

4.1. Business Requirements (BR)

1. A Data Sharing Agreement (DSA) shall be the means for defining data security and sharing requirements between two or more organisations.

2. A DSA must be clearly understandable to a managerial or legal expert. It should be expressed in non-technical language, which provides the legal text of the agreement. A Data Sharing Agreement that has substantial technical data within the legal text body is not acceptable.

3. A DSA may have a separate technical annexe containing technical system security requirements, and if included it shall be consistent with the protocols and agreements in the main text.

4. It shall be possible to identify conflicts in the DSA or DSAs which prevent consistent policies being defined.

5. There shall be a means for an organisation to verify that a DSA is consistent with its legislative duties.

6. A DSA based on a controlled vocabulary or set of terms is permissible.

7. The controlled vocabulary must be based on standards such as, for example, RDF and OWL. Note that the choice of these particular standards is not mandatory and that other standards are permitted: the most important criteria is that they should be widely supported across the different applications, platforms and systems that each organisation may elect to use.

8. A policy for protecting TSOs shall be derived from the DSAs that are entered into by the parent organisation. Such a policy will be consistent with all of the data sharing agreements, enforcing all obligations of the agreements entered into by that organisation. Such a policy must be used by the enforcement mechanisms to ensure that the terms of the DSAs are respected.

9. There must be a reconfiguration of systems and services within each participating organisation in accordance with the agreement. This process must be automated as much as possible.

10. Multiple access restrictions (policies) may apply to the same TSO, possibly derived from different data sharing agreements. The system needs to enforce them in a coherent and consistent fashion or permit the detection of inconsistencies.
11. A TSO shall be divided into a set of separate elements, and shall have different access policies for each element. Access to a given element is permitted only where the access policy permits it and not otherwise.

12. Once the TSO is obtained by a responder and the access rights of the user established, access to the TSO shall not be interrupted until after the close of the incident or some time specified in the policy.

13. The policy decisions shall be based on elements within the TSO and on context data (eg. geospatial location, tier 1, 2 or 3) provided by the responder.

14. Access policies shall be definable for the responders for the period of the incident. These policies will include the right to read the TSO and to generate a new (updated) TSO from the existing TSO.

15. Certain personnel (eg Tier 1 responders) shall be provided with the ability to access otherwise protected data if there is an urgent operational need.

16. The solution must be able to support the separate data security requirements for multiple incidents.

17. Access policies shall be definable for designated users after the incident. It should be possible to define an archive access policy, which prevents deletion or alteration of a TSO before a pre-defined archive review date.

4.2. Administration Requirements (AR)

1. An organization must be able to designate a controlled set of responders who are permitted to set and modify low-level enforceable TSO policies.

2. The definition and control of the primary access policies shall be administered by a controlled set of (Category 1) responders. It shall be possible to resolve conflicts between the policies of different responders.

3. Other responders are permitted to set policies within their organization which are more restrictive than those of the primary access policies, ie. they specify further restrict rights or impose additional obligations. Primary policies always take precedence over other policies.

4. An access policy shall be translatable into a natural language that is comprehensible to administrators. It would be desirable to provide alternate natural language translations (eg. English and Welsh). It is not required, however, that the translation into natural language is identical to the DSA from which the policy is derived.

5. Administrators shall be able to take an access policy and be able to trace the rationale for the policy, including references to statutes, regulations and data sharing agreements.

6. Administrators shall be able to validate the access policies. This should at least identify policies that have no effect (always evaluate to True) or always fail (always evaluate to False). It may also identify inconsistent policies based on knowledge of the TSO, such as allowing access to casualty figures but not the event description.

7. Verification of the access policies should be supported. For example, it may be possible to play through a scenario and identify which users are granted access at a particular point in the scenario.

8. It should be possible to revise a policy part way through an incident, and set it to apply to all TSOs distributed subsequently.
9. It should be possible to create a policy specific to a particular user or group of users to over-ride all other policies (eg. to grant access rights in a special case to non-registered users).

10. The setting and propagation of policies shall be logged in a secure way, such that claims about the policy in force during an incident can be used in a court of law.

11. The authentication of users such that they can make use of access rights policies should be logged in a secure way.

12. There shall be the ability to propagate policies to other administrators in other organisations.

4.3. **Policy Implementation Requirements**

This section describes the types of access criteria and obligations that the scenario requires. It identifies the way that policy decisions are related to the data available to make those decisions.

1. The policy language must be able to restrict rights and impose obligations based on information extracted from the TSO and/or from the context in which the TSO is to be used.

2. The policy shall be able to use the criterion that the reported location of the unit is within a rectangular bounded box aligned to and defined by latitude and longitude;

3. The policy may use the criterion that the reported location of the unit is within a polygon.

4. The policy shall be able to use the criterion that an identifier in a TSO field matches a given identifier (eg. a responder's id).

5. The policy shall be able to use logical combinations of the above criteria.

6. The policy shall be able to specify controls on read, copy, update and delete, and specify the obligation to delete after a given event has occurred or time elapsed.

4.4. **System Procurement Requirements (SR)**

The various agencies involved will independently purchase (or implement via external contractors and consultants) software to implement the COP and the TSO distribution system. This requires that the component architecture that defines the proposed solution should be clearly defined so that the system management authorities can select a complete and consistent set of software components.

1. Interfaces between these components should be precisely defined, identifying any preconditions, parameters and errors or events returned. Formal languages are desirable for this purpose.

2. Each interface should also define protocols such as the possible and required sequences of calls to the component interfaces. If necessary, the interface shall have a set of conformance classes associated to it, defining different levels of capability for a software component.

3. Each component should be certifiable as meeting defined conformance classes (if no conformance classes are defined, then the component shall meet the entire interface specification). Certification tests and criteria should be defined.
4. Where interfaces link to business systems, the interface must be related to the business data from the systems.

5. The terms used and their scope shall be defined so that the terms are used in the same way by different organizations; this may involve identifying where organizations must develop a specific vocabulary in order to be able to work together (for example, the TSO provides a series of specific vocabularies for the emergency services).

6. Existing application architectures must not be affected by the introduction of data security solutions produced by Consequence. The solution must not be disruptive and mandate the replacement of operating systems and platforms (unless these are on a reasonable upgrade path).

7. The solution must be interoperable with a variety of technology platforms including (but not restricted to) .NET and Java. It is recommended that Python should also be supported.

8. The solution should support the use of human agents who can enact a system component role (eg, context or identity provision) when the component has broken down, is unavailable or when connections to it have been lost.

5. Testing and Evaluation
This section defines how the various requirements will be tested and evaluated. These experiments serve two purposes: a) to validate the Consequence Reference Implementation and b) to show customers (both EC and BAE SYSTEMS business units) a tangible demonstration of the project concepts and business possibilities.

Given the available resources and the maturity of the concepts and tools being addressed by the project, it would not be appropriate to conduct full-scale trials. A more reasonable goal is to consider small scale experiments and demonstrations using a number of representative software applications, devices and ‘synthetic’ data. By ‘synthetic’ is meant something that simulates the behaviour or key features of the actual data, application, system, component etc without being the real thing.

Therefore, the section will first describe the methodology to be followed when addressing the above scenario requirements and will follow this with a list of evaluation criteria that are used for assessing to what extent Consequence meets the end-user requirements.

5.1. Experimental Methodology
The experiments may be split into those specific to Tier 1, and those specific to Tier 2 and 3.

Typically the software suite within a crisis management scenario would include a GIS client application eg. [12] or [13], a mapping server eg. [14] together with a GIS database such as [15] to store geospatial objects such as the TSO. The Tier 1 software suite would differ in that the mapping information would generally be held locally on each device and would include a GPS unit for positional information. The task therefore encompasses managing access to the TSO in the GIS database and propagating a sanitised TSO to Tier 1 networks.

An example of an API for interaction with a navigation tool can be found in reference [16].

The following diagram shows the broad architecture typically involved in a GIS. This is representative of the kinds of systems within which the Consequence framework would be deployed.
The GIS consists, in its most simple form, of a server linked to a database containing information of interest to browser based clients. The clients request layer or feature information from the GIS server and add the data to mapping information requested from servers such as Google Earth, NASA’s WorldWind or proprietary mapping systems.

The Consequence enforcement layer would appear to best sit between the GIS server(s) and the requesting client applications either enabling or denying access to the data-stores eg. TSO repository. It is expected that access to basic mapping information would not be controlled by the Consequence layer as this is publicly accessible data and is not restricted.

Relevant points concerning Tier 1 experiments are:

- An ability to create ad hoc networks
- Sharing of controlled TSO among other Tier 1 responders assigned to same operation
- Automatic propagation and update of latest TSO within group, especially in areas of low connectivity.

The following is a possible demonstration for responders working within a Tier-1 environment. There are two actors from Fire and Ambulance command officers at the scene, both assigned to the incident in an area of low connectivity. A possible short story connected with this would be:

1. Fire officer meets up with Ambulance officer at incident scene which is burning building with 10 unaccounted people (last info that Fire receives)
2. Ambulance has been at the scene and has collected its own preliminary data but is unable to update the ‘greater COP’

3. Preliminary data held by Ambulance includes personal data on casualties that are already under care (2), but which Fire do not need to know

4. There are 8 unaccounted for people in the blazing building. Ambulance update their TSO to reflect this revised number

5. Fire arrives with the latest TSOs in the ‘greater COP’. Fire believes there are 10 unaccounted people in the building

6. TSOs are exchanged to have a new COP they both share. Fire now has the updated values.

7. Both proceed to work on the incident together.

8. Fire pushes in a new TSO into the local COP

9. The TSO is read by the other officer in Ambulance, but has only restricted access- access is granted based on context of requestor.

10. Paparazzi at the scene try to monitor the events and are able to access these protected TSOs but are unable to open them.

A proposed evaluation exercise would be:

- Room with 1 wireless access point and 2 laptops representing tier 1 responders from different organisations assigned to emergency ‘A’. Wireless access point is switched off – both laptops to share and display updated TSO in ad hoc mode.

- A 3rd laptop is brought into room in tier 1 mode also in emergency ‘A’. Laptop to join the ad hoc network and TSO to be shared and updated where necessary.

- Repeat experiment with laptop in tier 1 mode but assigned to a different emergency mission ‘B’– access to all emergency ‘A’ objects to be rejected. Note that for the limited connectivity trials, the laptops are to hold the majority of the mapping data locally and the TSO is to be displayed as a layer within the GIS client.

The Tier 2 experiments will involve:

- Rapid creation, modification and deployment of policies- at both DSA and enforceable policy level.

- The ability to prevent access to sensitive data from TSO depending on policy and context.

- The visualisation of the implications of a policy change. This is a research question that will be pursued, ie, how are the implications of these changes represented to the user?

The story for a possible experiment would be:

1. flooding encroaching on a power sub-station, which supports a hospital and retail park

2. power failures trigger alarms

3. the alarm supplier has information on the location and status of the alarms

4. the Fire control request access to this alarm information
5. alarm company change the policy for this alarm data
6. alarm company can visualise the impact of the changes in the policy on their overall security management system
7. information is released, but only permitted to Fire control roles, in their control rooms, for the duration of the emergency.
8. Fire can now access the alarm data and update the COP with the ‘false alarm information’
9. Police can now see the (filtered) alarm data as well- this shows that false break-in alarms can be discounted

The evaluation exercise would involve:

- Equipment including a server with Microsoft SharePoint™ and GIS server eg. GeoServer and GIS database eg. PostGIS. Also, a small number of laptops with GIS client eg. uDig installed. Connectivity to a Tier 1 wireless access point.
- Task 1 is to demonstrate automatic propagation of a TSO within Tier 2 group. Similarly to demonstrate propagation of updated TSO from Tier 1 group to Tier 2 group.
- Task 2 is to demonstrate update of TSO within Tier 2 with sensitive information – aim is to demonstrate automatic desensitising of TSO for use within Tier 1 group.
- Task 3 is to change policy and to visualise the consequences of policy change to access tree model. Tools such as [17] may be useful.

Tier-3 experiments would take a similar form to Tier-2 and so are not explicitly considered here. The aforementioned descriptions should provide sufficient coverage.
5.2. Evaluation Tests

The following table describes the potential tests that could be used to evaluate performance at the different tiers within the scenario.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Tier 1</th>
<th>Tier 2</th>
<th>Tier 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data (TSO) sharing</td>
<td>Ad-hoc sharing</td>
<td>Automatic propagation and update of TSO within Tier 2 without data loss</td>
<td>Automatic propagation of DSA from Tier 3 to Tier 2 and TSO</td>
</tr>
<tr>
<td></td>
<td>Automatic TSO update within incident</td>
<td>Automatic desensitising of TSO for use within Tier 1</td>
<td>Automatic propagation of DSA between groups within Tier 3 organisations</td>
</tr>
<tr>
<td></td>
<td>Hardware-driven (e.g. blue-light status)</td>
<td>Ability to ‘open’ or ‘close’ incident to additional resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ability to join an ‘open’ incident</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Separation of incidents resulting in different visibility of data within TSO</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time sensitive display of TSO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy change visualisation</td>
<td></td>
<td>The implications of a modification to a policy on data access are to be clearly visualised within a multiple policy environment. Areas of policy conflict are to be highlighted.</td>
<td></td>
</tr>
<tr>
<td>Policy deployment</td>
<td></td>
<td>Modifications to a data sharing policy are to be rapidly propagated to both Tier 2 and 3 responders</td>
<td></td>
</tr>
</tbody>
</table>

Table 6 Evaluation Test Cases for the Crisis Management Test Bed

The main focus should be on the interface between Tier 2 and Tier 1 responders and on the visualisation of the implications of policy changes both within and external to the Tier 1 boundaries of the incident.

The configuration of the experimental setup is shown below:
The evaluation criteria for each experiment are defined in Table 7.
<table>
<thead>
<tr>
<th>Tier</th>
<th>Aims of experiment</th>
<th>Experiment</th>
<th>Evaluation criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1</td>
<td>Automatic update of TSO within incident</td>
<td>A restricted incident geographical area is created by Control Room and responders 1 and 2 allocated to the incident. Responder 1 enters area covered by access point.</td>
<td>On connection to network, and if Responder is within incident geographical area, TSOs are to be transferred and updated in the client COP.</td>
</tr>
<tr>
<td></td>
<td>Multiple incident data access</td>
<td>Two incidents are created on the Control Room COP. Responder 1 allocated to Incident 1, Responder 2 allocated to Incident 2. Three TSOs generated – TSO-1 is restricted to Incident 1, TSO-2 is restricted to Incident 2 and TSO-3 is shared data containing information on the location of both Responder 1 and 2. TSO-3 should be available within Incident 1 but not Incident 2</td>
<td>As Responders join the incidents, TSOs are to be transferred to relevant client COP. TSO-1 is only visible to Responder 1, TSO-2 is only visible to Responder 2. TSO-3 is visible to Responder 1 but not to Responder 2. In the Control Room all TSOs are to be accessible.</td>
</tr>
<tr>
<td></td>
<td>Time sensitive display of TSO</td>
<td>Continuation of experiments as above – TSOs are updated by Control Room some time after Responder joins the incident. A sample TSO is subsequently updated by Responder 1. Responder 2 then is allocated to and joins Incident 1.</td>
<td>1. Appropriate TSO is to be clearly indicated as ‘stale’ and updated on Responder 1 COP. 2. Sample TSO updated by Responder 1 should be signalled as updated in Control Room 3. As responder 2 joins the incident, the most recent TSOs are to be uploaded to COP.</td>
</tr>
<tr>
<td></td>
<td>Hardware-driven (eg. blue-light status) ability to join an ‘open’ incident</td>
<td>Responder 2 to leave the area. Incident to be reclassified as ‘Open’ but with only Responder 1 allocated. Responder 2 to re-join the incident. Responder 2 activates hardware switch.</td>
<td>1. As Responder 2 rejoins incident, access to incident specific TSOs are to be refused. 2. On activation of switch, TSOs are to be shared and Responder 2 becomes part of incident reflected in Control Room COP</td>
</tr>
<tr>
<td>Tier 2 and 3</td>
<td>Ad-hoc sharing of time sensitive TSO</td>
<td>Policy (or Data Sharing Agreement) change visualisation</td>
<td>Policy deployment</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------</td>
<td>------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>Responder 1 obtains full update of TSOs for restricted incident with both Responders allocated. Access point switched off. Responder 2 to be brought within wireless range of Responder 1. A sample TSO is to be updated by Responder 2. Access point switched on.</td>
<td>Two laptops configured as Tier 2 or 3 responders with appropriate COP and connected to Control Room access point. Two incidents (1 and 2) are created. Remaining laptop as Responder 1 allocated to incident 1. A Policy (DSA) concerning data access in Incident 1 and access for Tier 3 is proposed for modification. (May require more responder devices eg Samsung NC10 Netbook to stress test system and provide realistic demo)</td>
<td>Experiment as above. The Policy (or DSA) modification is approved and New Policy is deployed</td>
</tr>
<tr>
<td></td>
<td>Ad-hoc network to be created between Responder 1 and 2. Relevant TSOs defined by Policy are to be updated and displayed on client COP. When access point is active relevant TSOs to be updated on Control Room COP.</td>
<td>Effects and implications of change in policy to be visually clear eg Tier 3 information contributors to be colour coded according to access status with proposed changes to be highlighted.</td>
<td>Responder 1 to see TSOs updated as access policy changes. Responders in Incident 2 should be unaware of any policy changes Tier 3 responders to see new data access</td>
</tr>
<tr>
<td></td>
<td>Data access within TSO and sanitising of data</td>
<td>Data access within TSO and sanitising of data</td>
<td>Tier 2 Control room to have full access to TSO. Tier 3 responder to have access to part of TSO. Responder 1 to have access to basic TSO with TSO-low and TSO-high to be removed, Tier 3 to only access TSO basic + TSO-Low. Control room can access all of the TSO-high.</td>
</tr>
</tbody>
</table>

Table 7 Description of Experiments for evaluating the Consequence Framework
If time permits, some further evaluation will be done using human factors performance metrics. These are described further in Appendix 8.

6. Conclusions
Recent innovations from projects such as OASIS-fp6 present an opportunity for making information more accessible between emergency agencies and delivering it in a timely fashion to a greater community of users. This information can be used for improving the decision making process, making it faster and more directed. However, this very connectivity poses a number of security issues, particularly when the data is commercially sensitive or has personal data in it. The ability to control access to this data once it has left the organisational boundaries is the next objective of a secure networked enterprise.

Consequence proposes a data-centric security approach which addresses this particular problem directly. The supporting components of this framework are a) a data sharing agreement management system, b) an enforceable data security policy, c) a supporting set of services that ensures the data security requirements are enforced. This document has developed an application scenario that has been used to identify the top-level requirements that can help in designing and developing these components of the framework. We quickly review these components in term,

The first of these components is critical since the DSA will be the primary means for expressing the security requirements. Ideally, the DSA should be written in a non-technical language suitable for policy makers. Any tools for facilitating the translation of the DSA into enforceable policies would provide a huge change in capability- the ability to quickly deploy an organisational security policy in seconds rather than the days/weeks of effort that would normally be required. An important aspect here, however, is the ability to check a DSA, and the visualisation approach recommended here is one way of representing the effects of the DSA to these non-technical roles.

The second component is the enforceable policy. By means of the data-centric policy, the Consequence framework should autonomously decide whether or not a responder has access to protected material. If successful, this would enable the decision making process to proceed more quickly. There would be less time spent pondering whether the material should be released as the document policy would make the correct decision based on the circumstances of the requestor. It should also eliminate the need for a request to be approved by a hierarchy of managers, which is current practice. However, not all circumstances may be foreseen in a data sharing agreement and so it is important to cater for circumstances where human intervention is required where there is an urgent operational need. The tools for doing this should be easy to use.

The third component is the infrastructure that enforces the data policy. It is assumed that the parties are basically trustworthy and committed to upholding the rights of the partners as expressed in the agreement between the organisations. The infrastructure becomes critical in ensuring the various systems and applications used by the partners can enforce the policy. In some sense, this infrastructure is ‘Trusted’ to make the right actions in a secure way. Other than the general assumption made above, our understanding of Trust is still at an early stage and so will be further explored in the next phase. Finally, it should be noted that for general crisis management activities, the ability to deal with intermittent or unreliable network connectivity must also be taken into account.
It should be emphasised that the architecture and systems developed within Consequence should be aimed at improving the access to data rather than hindering access. In this way, the output of Consequence is seen as an enabler rather than a disabler and must be a positive enhancement to a crisis management scenario. It is also important that Consequence is perceived to enhance data sharing from both sides of the equation: the data providers should be reassured that security of sensitive data is not compromised; the data consumers should not perceive that operationally critical data may be hidden or otherwise restricted.

From interviews with end users together with a description of an example crisis scenario it has been possible map Category 1 and 2 responders onto a 3 Tier data access structure according to data requirements, network connectivity and security constraints. From this it has been possible to develop a set of preliminary requirements that reflect the need within the agencies responding to the emergency for quick and effective access to accurate data together with some form of positive feedback to ensure that information has been received. Requirements have similarly been developed from the viewpoint of the data-supplying agencies where there is a clear legislative need to protect sensitive information. It has also been possible to highlight the need for a method for a simple, easy-to-understand visualisation of the consequences of a data sharing agreement, though the specific requirements still need to be worked out. The experiments are an opportunity to prototype ideas for DSA visualisation to further understand the requirements in greater detail.

Finally, it has been possible to define a sequence of small scale laboratory experiments that will demonstrate and validate the critical aspects of the Consequence framework in a structured and well understood manner. These will be used in the next phase of the project to a) have definite test cases to design, develop and test against, b) provide feedback to the teams who are developing the reference implementation and c) provide feedback to the Consequence architecture team.

7. References
1. Key Words for use in RFCs to Indicate Requirements Levels. S Bradner, IETF RFC2119
2. OASIS EU Project Home Page http://www.oasis-fp6.org/
6. Fundamentals of measurement for stability operations Bullock R MORS Publications 2005
8. SENAC website www.semb.co.uk/reference/glossary.htm
9. Question 92: Why is it important to explicitly state the intended business result of an IT project? How should this be done? The Customer Service Representative Improvement Project. Casey W.W Business driven information technology: answers to 100 critical questions for every manager (ed D Laube & R Zammuto), Stanford Press (Online version: www.executiveleadershipgroup.com/Question%2092.pdf) 2003

11. UK resilience Web Site: Local Resilience Forums
   (http://www.ukresilience.gov.uk/preparedness/ukgovernment/lrfs.aspx)


15. http://postgis.refractions.net/


Appendix 1. Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBRN</td>
<td>Chemical, Biological, Radiological, Nuclear. A common classification for a threat arising from an incident- whether accidental or intended.</td>
</tr>
<tr>
<td>CCA 2004</td>
<td>Civil Contingencies Act 2004</td>
</tr>
<tr>
<td>CDA 98</td>
<td>Crime and Disorder Act 1998</td>
</tr>
<tr>
<td>COP</td>
<td>Common Operating Picture. A set of data or information entities that provide an up-to-date view of an incident.</td>
</tr>
<tr>
<td>Defra</td>
<td>UK Government Department for Environment, Food and Rural Affairs</td>
</tr>
<tr>
<td>DPA 98</td>
<td>Data Protection Act, 1998</td>
</tr>
<tr>
<td>DSA</td>
<td>Data Sharing Agreement</td>
</tr>
<tr>
<td>FireMET</td>
<td>A system that provides accurate up-to-date weather information to Fire Services in the UK</td>
</tr>
<tr>
<td>GIS</td>
<td>Geographical Information System</td>
</tr>
<tr>
<td>OASIS-fp6</td>
<td>OASIS EU Framework 6 Project</td>
</tr>
<tr>
<td>OASIS-Open</td>
<td>Standards body for Internet and e-Business standards, eg, ebXML, XACML, SAML, BPEL and various WS-* web service standards</td>
</tr>
<tr>
<td>PAF</td>
<td>Police, Ambulance and Fire</td>
</tr>
<tr>
<td>SOA</td>
<td>Service Oriented Architecture. A means of exposing software components as formally defined interfaces, accessible using standard Internet protocols.</td>
</tr>
<tr>
<td>TSO</td>
<td>Tactical Situation Object. A common representation of emergency situation data that can be shared between different agencies.</td>
</tr>
</tbody>
</table>

Appendix 2. Responder Organizations

The basis for emergency response planning in the UK is the Civil Contingencies Act, laying out who should be involved in planning and what their responsibilities are. The act divides the main responders into two categories, which, in England are:

Category 1:
- Emergency Services
  - Police forces
  - British Transport Police
  - Fire Authorities
  - Ambulance Services
  - Maritime and Coastguard Agency
- Local Authorities
o Metropolitan districts, shire counties, shire districts and shire unitary authorities
o Port Health Authorities

• Health Bodies
  o Primary Care Trusts
  o Acute Trusts
  o Foundation Trusts
  o Health Protection Agency

• Environment Agency

Category 2:

• Utilities
  o Electricity Distributors
  o Gas Distributors
  o Water and Sewage
  o Telephone service providers (fixed and mobile)

• Transport
  o Network Rail
  o Train Operating Companies (including freight)
  o London Underground & Transport for London
  o Airport operators
  o Harbour authorities
  o Highways Agency

• Strategic Health Authorities
• Health and Safety Executive

The act also acknowledges that other organizations may be called upon to help in an emergency, including:

• the armed forces;
• retail companies, including supermarkets;
• insurance companies;
• bus and road haulage companies;
• taxi firms;
• airlines;
• shipping companies and ferries;
• media companies;
• private communications networks dedicated to public safety users;
• offshore oil and gas industry;
• security firms;
• internal drainage boards;
• general practitioners and chemists.

The main Category 1 responders, the Police, Ambulance and Fire Services, generally put in place a three tier command structure, generally known as the Gold, Silver and Bronze commands, corresponding roughly to strategic, tactical and operational commands. In general, Gold command is put in place only for the larger emergencies. The services vary in their interpretation of what these terms mean, and may also vary as to whether a particular incident requires them to have the higher tiers of control. For example, the Bunsfield fire required a
nationally co-ordinated response from the Fire Service, but, as there were few injuries, very little response from the ambulance service.

In the UK, the most major emergencies are supervised by the COBR committee, consisting of members of the government and other key officials, and which may be chaired by the Prime Minister.

Appendix 3. TSO Structure

A 3.1 TSO Background

The TSO was developed as part of the EU project OASIS-fp6 on emergency response (referred to below as OASIS-fp6, to distinguish it from OASIS-open, the standards body). In the OASIS-fp6 model, the TSO is generated by a control centre from the Common Operating Picture (COP), and is a lightweight XML message designed to give an overview of the situation to first line responders, either to individuals with hand held devices or to vehicles. It could also be distributed between control centres to provide situation awareness where a control centre is only peripherally involved in an incident, however it is not sufficiently comprehensive to provide the whole detail of the COP.

Situation awareness is a combination of knowing what is going on, who the other agents are, and what their plans are. This is reflected in the three main information sections of the TSO: the event description, the list of resources involved and the missions planned or underway. The TSO also provides a section on context, that is, who is providing the information, whether it is live or a test or an exercise, etc. (A more sophisticated view of situation awareness distinguished between three levels of initial perception of the information, comprehension of it and projection into the future, but the TSO is limited to providing the information for perception).

In addition, the TSO can use the EDXL-DE (Distribution Element) structure to control the distribution of the message. EDXL is a set of standards for Emergency Data Exchange being developed by OASIS-open and includes a message giving the status of a hospital (EDXL-HAVE) and a set of transaction messages find resources and negotiate their deployment (EDXL-RM). The EDXL initiative is related to the US Department of Justice standard GJXML, although the COP and the TSO are based on the NATO Multilateral Interoperability Programme (MIP) JC3I EDM standard for command and control.

A 3.2 Measures of Scale

The scale of an incident has profound effects on the way an incident is managed, since it not only increase the number of responders needed, but also the range of responders needed, the area from which responders are drawn and facilities used, and the complexity of control structures. The TSO defines a five point scale to characterise incidents, in which an increase by a scale point indicates the effort involved increases by an order of magnitude. The scale points are:

1. A minor, domestic scale incident, such as road traffic collision, a domestic fire, or a heart attack. This will be dealt with as part of the routine operation of the services involved, although may involve co-ordination between fixed operational control centres for each service.
2. A larger incident, within the capability of the local services, such as a local football match, a fire on a petrol tanker or a car crash with multiple injuries. A service may expect to resource one or two such incidents in parallel with its normal duties, but may need outside support if there more incidents it can deal with. A service may set up a local incident control centre.

3. A major incident, in which support and resources are required from the neighbouring service organizations, such as a riot, a major factory fire, or a passenger train crash. Local tactical incident control is likely to be reinforced by a strategic control centre.

4. A national emergency, such as the summer floods in 2007 or the Bunhill depot fire, which will draw resources from beyond the surrounding area, and may involve large scale evacuation. In the UK, the government's COBR committee could be activated.

5. A disaster, where national resources are insufficient, such as the destruction of New Orleans, the Dec Myanmar cyclone or the earthquake in Sichuan.

Note that the scale is defined in terms of the capabilities of the local organizations to respond, rather than on an absolute scale, since this matches the operational problems of control. For example, the fire service for a large metropolitan area such as Manchester may have capacity for two larger incidents, such as tanker fires, whereas in a rural area resources are fewer, more widely spread and often staffed by volunteer firemen, and here the capacity plan may be limited to a single incident, such as a fire in a thatched cottage.

The perception of scale will also vary with service. For example, for a fire service, a fire in a thatched cottage requires a much larger response to one in an ordinary domestic building, whereas the ambulance service might regard them as being on the same scale. For example, the July 7th bombings in London were regarded as major incident by the hospitals, since they had to plan to accommodate a large number of seriously injured people, whereas it was a lesser incident for the ambulance service, since the numbers needing an ambulance at any one time were within the normal operating capacity of the service.

The TSO was primarily designed to deal with major incidents (scale 3 or larger), however, in practice it would need to be deployed at least for scale 2 incidents, if not scale 1, to ensure when it comes to a major incident that personnel are familiar with the information and the systems using it. Also, it is also not always possible to identify the scale of an incident at the outset. Firstly, an incident may be phoned in by several members of the public, each with a different viewpoint and assessment. Secondly, the responder arriving first may not be trained or qualified to assess the incident, and any assessment may need confirmation. Thirdly, an incident may rapidly change in scale, say, from a small fire in some rubbish to burning down a major building or a forest fire. Consequently, the ability to share ordinary situation information is seen as a useful capability, forewarning a service of an incident they may be asked to attend.

A 3.3 TSO Model for Consequence

The TSO object model presented here is based on the XML implementation of the full object model that was adopted in the OASIS-fp6 project. Note that the XML implementation used a sub-set of entities from the original model. The model includes some hidden relationships, in which cross references (foreign keys) are used, rather than being explicitly shown in the object model.

The following figure proposes a modified TSO message model structure for use in the Consequence study based on the XML message. In Figure AF3.1, each box corresponds to an
The first modification proposed is to drop the Link and External_Info objects from the TSO. In both cases, the entities refer to objects external to the TSO - another TSO or an external document - which would use an independent access control policy. Since the focus of this work is the use of policies for a TSO, these elements may be dropped without loss. Note that the omission of these two elements still produces a valid TSO structure.

The second modification is the explicit use of the EDXL-DE (distribution element) as the message wrapper. This is permitted by the TSO, but not required. EDXL-DE has the ability to specify a delivery address by location, including geographic zone. The ability to restrict access to the TSO to a specific geographic zone is likely to be one of the access control criteria, and would therefore require this information. The other geographic zones specified within the TSO refer to the area of the event, or the position of a resource or mission, however it is likely that the TSO will be accessed over a wider area than that of the event itself to enable the responders en route to be briefed on the incident.

A 3.4 TSO Component Distribution

It is proposed to treat the TSO as being split into five components, and to apply separate access policies to each:
- **Event identification** - given by the Context, Event and Event/Event-type elements, as this is the basic information needed to identify what is happening;

- **Event Location** - giving its location (Event/Event-location) and relationship to other events (Event.Main-event-relation & Event.Other-event-relation);

- **Casualties** - giving estimates of different classes of injured and dead (Event/Casualties) and people to evacuate (Event/Evacuees);

- **Resources** - giving the identity and location of the resources involved in the event (Resources and sub-objects);

- **Missions** - describing the missions planned or in progress to deal with the event, together with the resources allocated to the mission (Missions and sub-objects).

The basic rationale for this split is that, for a larger event, the Category 1 responders' control centres should be aware of all that is going on. Front line responders not directly involved in the response need to be aware of the event and its location, since, for example, it may block an access route. Front line responders need to be aware of the missions they are involved in, but do not necessarily need to know the details of every one at the event.

For Category 2 responders, the control centres need to know about the event and its location, but not the details of casualties or evacuees. Only their front line responders involved in the event need details of missions they are being sent on.

Information about casualties and evacuees would not be freely circulated, firstly, since the initial estimates would not be reliable, and secondly, because of the possibility of spreading panic in the general population. Release of casualty figures to the media would be through media liaison officers, rather than feeding the press raw data.

One potential development on the emergency response domain is the distribution of alerts by area broadcast over the mobile phone network, using the OASIS-open Common Alerting Protocol (CAP). This is part of the EDXL family of messages, and has been adopted as a standard by the ITU (International Telegraph Union). Potential uses include ordering civilian evacuation over an area, or asking off-duty responders to report or to check an emergency response web site. Again, information would not be fed to the alert system by the TSO, but filtered through a liaison process.

The aim of splitting the TSO is therefore to tailor the information available to the information needs of the various parties with access to the TSO.

### A 3.5.1 Mechanisms and the TSO

Access to the TSO has been described above as the TSO being broadcast over an area. Other possibilities are that the TSO is sent to a particular distribution list, or that users poll in to a central system. However, in terms of access control to the content of the TSO, the requirement is not changed by the mechanism by which the TSO is delivered.

Further, the central system could choose to filter the TSOs before distribution, and distribute the according to the information needs of the user. However, the information needs of the user may be location dependent, and will change as the event progresses. That is, from the viewpoint of access policy, this is a question about the enforcement mechanism for filtering, rather that policy requirements.

The need to apply different policies to different parts of the TSO is equivalent to having an application that unpacks several documents with separate policies attached, or to multiple applications, each of which extracts a particular section of the document. The difference
between a TSO reader and an application oriented to applying policies to a single file is that either the TSO may need to make multiple requests for access keys, one for each part of the TSO, or that the enforcement point may need to issue multiple access keys, depending on which parts of the TSO are authorised for reading. This is a question of architecture rather than access policy requirements.

A 3.5.2 TSO and Metadata

The working assumption is that the TSO contains its own access control meta-data. That is, the policy for access to TSO data uses data within the TSO to decide whether access is permitted. For example, any responder within the outer cordon of an event would need to know where the boundary was, if only to evacuate themselves; the TSO contains the event boundary, and a policy would allow any responder whose location (from GPS) was inside the boundary to decode the event information.

A priori, policies may be based on the following:

- The security classification of the event;
- The event mode (live, test, etc)
- The type of event:
  - the scale;
  - the type of event (fire, medical, etc)
  - the type of location (eg. events involving railways need to be notified to the train operators);
  - the type of things involved (vehicles, animals, etc)
  - potential side effects, such as pollution or evacuation;
- The geographical location of the event and any surrounding zones;
- The organization of the TSO originator or the responder;
- The organizational role of the responder;
- The specific identity of a responder;
- The resource type of the responder;
- The duties/missions of a responder;

Most fields corresponding to needed elements are carried by the TSO. Those not covered (except the transmitting organization) are specific to the responder, however, since the TSO is a general message, it would not be used to carry role or responder organization specific messages.

The majority of the information in the TSO is contained as codes rather than free text, with the codes taken from a set of controlled tables. Consequently such data is available for straightforward automatic processing, since its representation is fixed.

Further, the code tables are hierarchical, which allows organizations to subtype the classes they represent to provide more specific subtypes where needed. A consequence of this is that policies will need to specify what type of hierarchy traversals will be allowed when calculating policy fulfilment. For example, a police force resource may identify itself as a fire-arms-officer, a Category not in the TSO code dictionary, but which can be defined as a subclass of police-officer. A policy stating that the information is available to a police-officer would be satisfied by someone who is classed as a fire-arms-officer using the traversal rule "valid for any subclass". However, a policy permitting access to a fire-arms-officer would not
allow access to someone who recorded as a police-officer, that is, the rule "not valid for a superclass" applies.

## Appendix 4. UK Legislation

This appendix presents some brief notes on the UK legislation of possible relevance to the BAE Consequence work. It attempts to put each act within the context of the BAE crisis management scenario. Each section summarises the scope of the legislation and inserts additional opinions on the possible motivations and its intended uses.

This report has not included the original legislation document itself. The UK government generally provides guideline documents that describe in non-legal terms the requirements of the legislation in a format that is accessible to those affected by the act. This has been the primary source of information for this report.

The following legislation is relevant:

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil Contingencies Act 2004</td>
<td>Duties on local government and other responders in the event of civil</td>
</tr>
<tr>
<td></td>
<td>emergencies/disasters</td>
</tr>
<tr>
<td>Data Protection Act 1998</td>
<td>For the lawful processing and management of individuals data.</td>
</tr>
<tr>
<td>Crime and Disorder Act 1998</td>
<td>Defines duties for the police and local government for preventing crime and</td>
</tr>
<tr>
<td></td>
<td>disorder</td>
</tr>
</tbody>
</table>

*Table AT4.1 Relevant UK Legislation*

In the following sections we review the relevant UK legislation concerning information management and information sharing that is relevant to emergency scenarios.

### Civil Contingencies Act 2004 (CCA 04)

The UK Government provides simplified guidelines to help the various responder agencies to understand the implications of CCA 04, such as [4,5]: these have been the main sources of material in this section. The author is not a legal expert and time constraints prevent him from delving into the legal details further of this act, so this report should be considered to be provisional and subject to review.

The act puts a statutory duty on organisations to prepare for, identify and contain the effects of a major disaster, terrorist attack or any event that threatens to disrupt the life of the UK. One concern is that of data sharing between so-called ‘Category 1’ and ‘Category 2’ responders. Category 1 concerns not only emergency agencies such as Police, Ambulance and Fire themselves, but also local government, customs (air and sea-ports) and environment agencies. Category 2 agencies includes utilities (water, electric, gas, telecoms), highway agencies and strategic health authorities - some of which are commercial organisations in the UK. Some of the Category 2 may decide to take responsibility for emergency response in their area of responsibility and may need to liaise informally with Category 1 agencies to ensure co-ordinated response. If these informal requests for information from Category 1 are denied by Category 2, then a formal request may be submitted.

Both classes of responders sit on a Local Resilience Forum (LRF) or at a regional level on a Regional Resilience Forum and both may be used to submit requests, possibly with other responders.

Category 1 responders have a statutory duty to:
1. make continuous risk assessments
2. to provide emergency plans
3. to warn and inform of crises
4. to provide business continuity plans
5. to share information
6. to cooperate
7. to undertake joint training

Overall, the responders have complementary roles. The scale of the emergency is likely to influence the degree of information sharing requirements to deal with it. A major crisis that threatens infrastructure for example will rely for its resolution on information from the utilities. An accurate risk assessment for a Community Risk Registry will also require information from these commercial organisations; furthermore, it is possible they may be other relationships between Category 1 and 2 responders that may need to be carefully managed. Local Authorities may perform risk assessments of utilities/infrastructure in a particular area of a city while being customers themselves of that utility provider, for example [4, Chapter 3 §3.44]. Category 2 responders may be commercial rivals to each other, so it is important that any valuable company data they disclose to Category 1 is not inadvertently leaked to their competitors in Category 2.

A UK or Scottish minister can also make emergency regulations within the act to require or permit information to be shared between responders. One imagines that this is done quickly if there is an urgent public interest. Furthermore, the government may intervene to facilitate this data sharing if there is not time to pass the relevant legislation.

It is noted that in the general case responders will share information on an informal and free basis but there may be particular cases where the information may be classed as ‘sensitive’ because:
1. it may be prejudicial to national security
2. it may affect public safety
3. it may be commercially sensitive (many of the Category 2 are commercial organisations)
4. the information may be related to an individual, so may be subject to the Data Protection Act 1998.

In such cases further consideration is required before disclosure to a fellow responder is made.

Regarding 1, if the agency came by the information via the intelligence services (IS) then this information cannot be disclosed unless permission is requested to the IS. One envisages that of the three services the police are the most likely to hold this information. This kind of information should be accompanied by some security classification that indicates the level of protection that is expected. The responder agency must also specify the purpose for using this sensitive information; if this changes or another purpose arises then a new request to the IS needs to be made.

It should not be automatically assumed that all data and information from this IS agency is sensitive by default. Furthermore, the originator of this information must make his/her classification decision on the basis of disclosure to the public. If the responder organisation could be trusted to protect the information then it is conceivable that it could still be shared and a more flexible security requirement could be negotiated. This may permit data sharing between responders in the context of an emergency. However, the final criteria that this kind
of sensitive data should not be shared with fellow responders is if it is accompanied by a certificate from a Minister asserting that loss of the data would jeopardise national security.

An agency is entitled to withhold information from other agencies if it falls into any of the above categories. According to the guidelines document, the refusal must be accompanied by a reason except in the case of national security as discussed above. However, this offers a potential risk in that responses to requests may be used to infer whether the information that was requested was related to national security or not. If, however, the reasons for an access decision can only be given to an authenticated requestor who is certified to belong to a particular organisation then this threat can, to some degree, be mitigated.

Data that is sensitive because there is a public safety interest may be shared if there is ministerial approval. Commercial data may be shared if there is explicit authorisation from the originator to do so. Personal data can also be shared as well if it is in the individual’s interest to disclose it, eg, to share personal information about casualties with counselling agencies. In both cases, if there is a strong argument that a public interest is at stake then this may override the initial restrictions.

The guidelines do not specify how non-sensitive data should be treated, other than to state that the agency must observe the usual duty of confidence or, if it is present, a private contract that covers the data in question. The latter may be the case if the owner is a private company, though this excludes those cases where commercially sensitive information is in question (which is item 3 in the above sensitive data list). Furthermore, the originator of the data must be aware that if the data is classified as non-sensitive then the responder organisation that is given the information may be obliged to share it in accordance with other legislation, eg, Freedom Of Information Act 2000 or Environmental Information Regulations 2004. An interesting point is made of data ‘sensitivity within different environments’, so any decision to share non-sensitive data should consider the possible impact if it is accessed by the public.

To date the author has not found any specific examples of data sharing agreements or protocols that are intended for data that falls under the scope of this act.

Sensitive data that originates from national security agencies would be managed using well-established procedures based on standard agreements. It is unlikely that this material would be accessed directly by Category 2 responders- a more likely scenario is the police being granted access to this kind of material. As noted earlier, these agreements may mandate having clear security markings on the material and restrictions on dissemination. Organisational policies would be enacted to ensure the data was adequately protected, possibly by limiting its accessibility (eg, can only be viewed by certain organisational roles and only in certain locations) and preventing its copying to removable media.

For non-sensitive data the situation is rather less clear. We would envisage that if a formal data sharing agreement were to be drawn up, it would involve aspects such as:

1. defining what material was being shared
2. the purpose or task the material was been used for
3. duties, such as logging who had accessed the material
4. how the material would be used
5. who has access to it
6. the responsible officer for ensuring the requirements were being met
**Data Protection Act 1998 (DPA 98)**

This concerns the protection of information or data on individuals. The act ensures that this kind of data is not exploited and that the individual’s welfare is respected. [6]. Two classes of personal data are identified:

1. data that can be used to identify an individual. This also includes opinions about the subject or of intent towards them;
2. data that is ‘sensitive’ and which refers to the subject’s race, gender, sexual orientation, political beliefs, religion, criminal history etc.

There are 8 data sharing principles. Stored Personal Data shall be:

1. processed fairly and lawfully
2. only processed for specified purposes
3. adequate and relevant for specific purpose
4. accurate and up-to-date
5. not kept longer than necessary for that purpose
6. processed under the rights of the subject
7. held with adequate security measures to prevent unlawful use
8. not transferred out of the European Economic Area without an adequate level of protection for the rights of the subject

DPA98 has been a major source of confusion to emergency responders who have to decide whether private information should be released and whether consent is required. In general, the recommendation is that if there is a critical need and consent cannot be granted (because the individual cannot be located for example or is incapacitated) and it is in the individual’s interest to disclose the information, then the responder holding this information organisation should release it. Public interest is also a factor that should be decided in releasing the information.

The act has a section, ‘Schedule 2’, which lists the conditions that need to be met when deciding to disclose this kind of data. Among these are 1) the individual’s consent, 2) for protecting the individual’s interests, 3) because a court order requires it, 4) the responder needs to disclose to meet its legal and statutory obligations, 5) there is a public interest to disclose, 6) the requestor has a legal/statutory obligation to have the information. Reference [6] emphasizes the point that it is sufficient for one of these requirements to be met - not all need to be satisfied. If information is disclosed, then ideally the subject should be notified wherever it is convenient to do so.

Access to personal data held by private organisations is less clear cut. Telecoms and financial sectors are particularly sensitive about releasing this kind of customer information for example. In normal practice, a business cannot be compelled to release the information to responders, unless it is for the police within a criminal investigation. The guide recommends that responders should establish working relationships with these organisations so that requests for this category of data can proceed quickly when it is required for an emergency and it is in the individuals’ (or in the public) interest to share it.

The document also recognises the importance of responders having access to personal data for the pre-emergency phase- ie, for planning and risk assessment purposes. This could involve, eg, having direct access to personal information held by care homes, charities, health trusts etc, though it recognises the administrative difficulties in obtaining this consent. The Guide recommends that the precise data requirements be identified before the systems could be
integrated- not all personal data needs to be disclosed for example, and perhaps a summary of the data would be sufficient. For example, the numbers of vulnerable individuals and their locations in a given area could be accessed but other data attributes could be ignored.

The guide also has a section on GIS and its important role in assessing threats. Sharing GIS data can be difficult due to national security and commercial sensitivity issues though these concerns are not in scope of DPA 98 (perhaps more relevant to CCA 04).

The document also contains a flow chart that describes a decision process when considering whether information is shared or not.

Sharing personal data is a sensitive matter for local and national government bodies. There are now a number of publicly accessible documents that present data sharing template agreements or describe possible data sharing protocols to assure the public that personal data is being processed lawfully and fairly by these organisations.

The following items are outlined in a template DSA specified by Ealing Council in the UK [7]:

1. **Stated purpose** of the agreement
2. **Extent and type** of information to be shared
3. **Uses** of the information
4. **Information to Data Subjects**- what information is to be given to the data-subjects that describes the purposes of the data and how they can access it etc
5. **Breaches of Confidentiality**- how breaches are to be dealt with
6. **Staff Awareness and Training**- how the requirements are to be met by the organisation
7. **Governance**- the officers responsible for overseeing the compliance with the agreement
8. **Review**- when the agreement would be reviewed
9. **Closure and Termination**- how the agreement can be terminated

**Crime and Disorder Act 1998 (CDA 98)**

This is the statute that places a duty on policy and local authorities to work together to reduce criminal activities. Local governments and other organisations now have to implement a strategy for reducing criminal activities and part of this involves sharing information from a variety of local government departments with the police. This enables a picture of incidents and patterns of behaviour to be identified over a city and thereby lead to a coordinated strategy for reducing criminal activity.

This is clearly a sensitive issue since in the general case local government data from social services is subject to Public Interest Immunity. There are, however, circumstances when releasing this kind of information can help to reduce criminal activity and anti-social behaviour and so a greater public interest is at stake.

Reference [9] is a template for a data sharing protocol intended for CDA 98. It describes the purpose of the data sharing, the partners’ duties, data use and exchange, data protection and confidentiality etc.

1. **Purpose**- to identify effects and costs of crime and disorder in the area, people at risk of crime, the profiles of likely offenders, contextual information to help decision makers and the wider aspects of crime and disorder that need to be considered.
2. **Partner Commitment**- to cooperate with each other fully for the purposes of the act; time limits for requests; named officers who represent the interests of each organisation in
implementing the act; to acknowledge rights of the data owners; the list of types of information to be exchanged;

3. **Management** - definition of the management group for overseeing the implementation of the agreement;

4. **Principles, Use and Exchange** - the purpose of the data, formats for data delivery and agreed common terminology; agreed categories of data collection; agreed definitions and duties in association of personal, non-personal and de-personalised data; a declaration to use the data for its intended purposes, respect data confidentiality and the destruction of data when it is no longer needed; disclosures of information should also be logged.

5. **Protocols**

6. **Designated Officers** - Primary Designated Officers

7. **Complaints and Breaches**

The agreement cites a ‘Crime and Disorder Reduction Database’, suggesting a new system is used to store this kind of data. This may be to ensure that the data is separated out from other data that the organisations do not wish to share. A significant amount of information is GIS based.

Bristol City Council published a data sharing agreement for CDA 98 [11]. The agreement has many signatories from police, health, counselling, probation and local government agencies. As with the above examples, it does not explicitly define the particular material to be shared, rather, it defines the process by which requests for restricted documents can be made. It contains the following sections:

1. **Signatories**: Members of the Avon and Somerset Partnership

2. **Purpose**: to facilitate exchange of personal data in accordance with duties specified in CDA98

3. **Introduction**: 

4. **Definitions**

5. **Information Exchange**: signatories bound by DPA 98, Human Rights Act 98.

Depersonalised data to be used wherever possible. Criteria for disclosing personal data (including consent of individual, duty to abide by CDA 98, public interest, etc). Data that is disclosed must be minimum and fit for its intended purpose. Source of data must be recorded against the disclosed data. Principle of ‘proportionality’ - being fair to rights of public and the individual. Excessive data, ie, data that is not being used, to be removed. If data is inaccurate then data originator must be notified. Requests for disclosures of data can only be made by registered personnel and can only be disclosed by registered personnel.

6. **Security**: partners must have in place mechanisms for protecting confidential data in accordance with DPA Principle 7. In this protocol, the agencies agree to use ISO 17799 or BS7799.

7. **Complaints and Breaches**: 

8. **Requests for Information**: Requests to be made to a Data Controller in that partner organisation. If a partner indirectly comes into contact with personal data, ie, is passed via a third party, then that partner must notify the originator to confirm if the data should be accessed.

9. **Training**: an acknowledgement that staff will be trained to deal with the data in accordance with the principles of this agreement.
10. Indemnity

11. Confidentiality: all personal data to be kept confidentiality.

12. Signatures: put your cross here ;)

The agreement has two appendices, the first of which describes a ‘disclosure form’, ie, the data to be disclosed. The data is disclosed under the following conditions:

1. only to be used for specified purpose
2. must be retained securely
3. that the data be destroyed when it is no longer used.

A section contains the reasons for disclosure, ie, the reasons for public interest outweighing the interests of the individual in this particular case.

The request form for this data specifies the reasons for requesting the data; categories for these are defined or alternative reasons may be specified in writing.

**Miscellaneous Data Sharing Agreements**

This section considers other data sharing agreements and protocols are not specifically related to the legislation identified above. Some of these are related to sharing information between the police and local authorities in criminal investigations.

Reference [8] describes an information sharing protocol between the social services in the south west of England and the police concerning child abuse investigations. This contains the following sections:

1. **Undertakings:** including by the police to keep the information confidential; neither party to give press briefings, social service to fulfil any requests for information
2. **The information to be exchanged:** agreements on the distinctions between the different individuals or subjects of the data;
3. **Police access to social service data** which defines:
   a. the rights and duties of the social services are respected;
   b. the conditions for releasing the data;
   c. the conditions for requesting the data;
   d. the named officer who makes the decision to release the data;
   e. the council undertakes to locate the data requested;
   f. a registry to be updated with a record of the documents seen;
   g. original copies of the documents requested should not be removed unless the request is via a court order
   h. an undertaking by the police to use the relevant parts of the material in accordance with the Criminal Procedure and Investigation Act 1996;
   i. the police should not disclose the notes based on the material to unauthorised individuals or organisations, including colleagues not part of the investigation;
   j. the suspect does appear to have rights to access this investigation notes- probably as part of the legal process
   k. to destroy the notes if there is no prosecution
   l. if new information is generated in the context of an inquiry by the service and if the police request this information then the council notifies the court before enacting the protocol.

**References**
Note that links to these references often break as web sites get updated. It may be necessary to do an online search for the document based on its title before retrieving it.

2. [http://www.ukresilience.gov.uk/preparedness/informationsharing.aspx](http://www.ukresilience.gov.uk/preparedness/informationsharing.aspx) information sharing in the context of UK Resilience. This appears to be the main source of UK Gov information on information sharing for crisis management.
3. [http://www.hm-treasury.gov.uk/independent_reviews/poynter_review/poynter_review_index.cfm](http://www.hm-treasury.gov.uk/independent_reviews/poynter_review/poynter_review_index.cfm) the Poynter report in the loss of HMRC Child Benefit Data
10. *Information Sharing Agreement, Leeds NHS.* [http://www.leeds.nhs.uk/attachment/00000000aeff19d226d36b62a8a8a96c10/0000000081578e05f28ac4b674492b6b/isa_template_version_2.pdf](http://www.leeds.nhs.uk/attachment/00000000aeff19d226d36b62a8a8a96c10/0000000081578e05f28ac4b674492b6b/isa_template_version_2.pdf)

**Appendix 5. Application Architecture**

The following describes the application architecture within the scenario. Note that this is based on the OASIS application architecture and contains some, though not all, of the major elements in that system.

The architecture is intended to facilitate the sharing of information between different emergency responder agencies described in the story board in Section 3.3.5. It does this by the fusion of data from different information systems owned by each agency.

**A 5.1 Use Case Diagrams**

These illustrate the individual use cases in the scenario, showing the interaction of the actors with systems and applications. Here we concentrate on human actors and their interactions with applications that have Human Computer Interfaces (HCIs).

The applications and systems identified here include:

1. Mobile Data Terminals- used by officers at the scene for making reports to control
2. COP Browser Client - for visualising information/TSOs associated with the current emergency. This covers both hand held devices used by officers at the scene and the desktop applications used in the control room.

3. Command despatch system - used for identifying the available resources and issuing commands to them for dealing with the incident.

Figure AF5.1 is a Use Case diagram showing an operative interacting with a TSO Browser. This is a graphical application that presents information from the TSOs on a map, for example, though the details of how it is presented and what information is selected will vary from agency to agency.

![Figure AF5.1 TSO Browser Use Case](image)

The following diagram (Figure AF5.2) shows a responder entering information into his Data Terminal at the scene.

![Figure AF5.2 Data Terminal Use Case](image)
Figure AF5.3 is a Use Case that shows a control room officer despatching a unit to the incident. We assume here that the application can also show some information on the available assets that the officer can use to allocate to the scene.

![AF5.3 Command Despatch System Use Case](image)

**A 5.2 Sequence diagrams**

Figure AF5.4 shows a top-level view of the application architecture.

![AF5.4 Top-level OASIS Architecture](image)

The principal components are:

1. A Legacy Information system: owned by an agency, it contains information associated with incidents such as event information (location, type of incident, numbers of casualties etc), information on assets assigned (eg, officers and vehicles assigned to an emergency) etc, reports from the scene, and geographical information etc.

2. An Information Fusion system, which enables information to be combined from various legacy systems to form a shared Common Operating Picture (COP).
3. A TSO Distribution service- for disseminating this fused information to fellow agencies- via either push or pull mechanisms.

4. A TSO Browser- a client application that is connected to the TSO Distribution service and which uses the TSO objects described earlier to be rendered in some suitable form.

The following interaction diagram (Figure AF5.5) shows a client application connecting to the OASIS Application service to retrieve TSOs:

![Interaction Diagram](image)

*Figure AF5.5 Client Browser interaction with the OASIS Application Server*

Note that in the current edition of the system the TSO distribution service does not push messages to the client. Instead, the client app must regularly poll the service to retrieve information. The delivery mechanism does not affect the security requirements discussed here, however.

Figure AF5.6 shows how new information is stored into the agency information system by a responder. It shows how this information is fused with other information to create a new TSO, which can be accessed via the interactions shown above.

![Interaction Diagram](image)

*Figure AF5.6 Legacy Information to TSO transformation*
There are a similar set of interactions when a client issues a command to despatch a unit to an emergency. This is also stored into the legacy information system and the above sequence of interactions take place as shown above.

There are some research questions with respect to the incident association function of the system:

1. The system critically relies on data fusion from different sources and each of these data items may have different security classifications. How can data fusion be done effectively when this is the case? Is the quality of the resulting data compromised?

2. Can data be transformed into a form that has a lower classification and should this be used for the fusion? Or should the original data be fused and then an overall classification imposed? (e.g., an intersection of the original security requirements)

Appendix 6. Studies and Trials into Inter-Agency Data Sharing

A 6.1 OASIS Shropshire Trials

One of the general aims of the EU OASIS-fp6 project is to improve the interoperability of the different systems that are used by different responder organisations across the EU. The Oasis Framework 6 project (OASIS-fp6) [2] conducted a number of separate trials of its technology with representatives from emergency services across the EU. These trials involved using operatives to assess whether decision making was improved by use of shared information facilitated through the OASIS-fp6 technology framework.

In the UK the Shropshire trial assessed the benefits of information sharing between different emergency control rooms. The relevant requirements that were confirmed by the Shropshire trial are:

1. A key requirement for information sharing is to allow any user in any organisation to have direct access to all information relating to an incident, regardless of its origin.

2. There is a need for an acknowledgement function when sharing time critical information, i.e., without an acknowledgement a user would typically require voice confirmation call to ensure that the intended recipient had noted the information.

3. The ability to append metadata such as confidence levels, information source or provenance, to key parts of shared information is also recommended.

The OASIS-fp6 TSO and Common Operating Picture system is intended to address requirements 1 and 3 and is described in detail in Appendix 3.

A 6.2 National Mobile Data Project

National Mobile Data Project considered how relevant information and collective experience is captured and made accessible in real time to officers at the fire ground and to other emergency services. This project investigated the use of information by the Fire & Rescue Services and allocated these to various phases of an incident. They noted that the first few minutes after arrival at the scene of an incident are absolutely critical and that the urgency and volume of the information required varies—see Figure AF6.1 below. Existing information

---

1 Source: www.cass.city.ac.uk/media/stories/resources/Cass_UnlockingHiddenWealthofOrganisations.pdf
systems did not cater for the fact that information requirements can vary significantly over time and according to the individual role responsibilities of users.

![Graph showing data traffic and urgency of information requirement during an emergency](image)

*Figure AF6.1: Data Traffic and Urgency of Information Requirement during an emergency*

Relevant requirements for mobile data access and observations are as follows:

- The information requirements can only be satisfied if the personnel concerned are equipped with suitable devices for accessing remotely-held data.

- A range of mobile solutions — from a variety of sources — were being employed across the fire and rescue service. *No standardisation existed in terms of technical capabilities, interoperability or functional capability.*

- Difficulties arose due to a *lack of standards for the capture and presentation of data.*

- Data must be kept in an *accurate state,* and *data subject to change must be transmitted at the moment of need.*

- It will be *necessary to use common standards, formats, and presentation tools* to ensure consistency and interoperability.

- The end user has a requirement to know that messages have been processed by the receiving system — *the system must provide full end-to-end acknowledgement.*

**A 6.3 Exercise TRITON**

Exercise Triton scenario covered an extreme flooding event affecting nearly half of England and Wales. Over 60 organisations and agencies took part nationally, regionally and locally. Lessons identified covered aspects were relegated multi-agency working, the plans and
procedures used, access to resources, and understanding the influence of the Civil Contingencies Act (Environment Agency, 2008²).

Relevant requirements on data sharing and observations are as follows (Environment Agency, 2005³):

- An important aspect of multi-agency working is the ability of all organisations to share information in order that each partner has the facts necessary to manage its own response.

- 5.2.18 Establish membership of a Defra-wide Strategic Co-ordinating Committee, with all relevant directorates represented and including representation from the Environment Agency. Defra and the Environment Agency should consider if attendance of Liaison Officers in the Defra Operations Room and the Cabinet Office is the best option to strengthen information sharing and briefing. This would also mirror successful arrangements in place at Gold controls, WAG and the RCCCs. [Therefore these groups would benefit from Consequence-style data policies.]

- 5.2.20 One of the most effective methods of communication between all organisations within control posts was considered to be the use of verbal team briefings.

- 5.2.23 If strategic groups such as CCC(O) are to make timely and effective decisions, information and data management processes must be streamlined.

- 5.2.27 A strategic review of systems is required to support operational activities and promote partnership working and efficient delivery of latest information. The review should include the potential of the Environment Agency’s proposed ‘Event Management System’. [This is partly covered by the OASIS-fp6 study, and it can be assumed that such a system would benefit from automated data sharing policies.]

- 5.2.28 Explore the potential of an Internet based ‘Decision Support’ programme (or secure web site) to strengthen the individual and joint ability of organisations to eliminate delays and assimilate information. Including, for example: greater use of visual displays, message boards, electronic mapping systems, global email systems, and video links between centres. [See above note.]

A 6.4 PITT Report

The Pitt Report is an independent review of the flooding emergency that took place in the UK between June and July 2007. The review was intended to assess what had happened and what might be done differently (Cabinet Office, 2008⁴). Urgent recommendations included improving information sharing and the practicalities of emergency response. Within the report the following aspects regarding better planning through information sharing are relevant. Comments or points to emphasise are in italics.

- ES .91 During the summer of 2007 emergency responders needed more information such as the location of critical sites, their vulnerability to flooding, the likely

² Source: http://www.environment-agency.gov.uk/subjects/flood/1217883/1218121/1218156/
⁴ Source: www.cabinetoffice.gov.uk/thepittreview
consequences of their loss and interdependencies between sectors. The information available was at best inconsistent, and at times unavailable. Agencies were severely hampered in their ability to respond quickly as events unfolded.

- ES .92 The duties under the Civil Contingencies Act for Category 2 responders to cooperate and share information were shown to be insufficient. Critical infrastructure providers must become much more active in local and national emergency preparedness and response, with greater contact between the public and private sectors at national and local levels. [What was discovered was that while Category 1 responders share more often than not, especially in emergency situations, the Category 2 responders did not. This is possibly due to being greater concerns over to legislative consequences (eg, concerning privacy) and litigation over commercially sensitive data after the event.]

- ES .93 We also need to be more direct with the public about risk. The balance between protecting information about critical infrastructure sites for security reasons and the need to share information with local agencies about such sites to protect them from flooding needs to be re-thought. Guarding against one risk can exacerbate the other. As the summer floods showed, actual risk to these sites is much higher than communicated risk, and the public were shocked by the loss of essential services. Responders were poorly prepared, and levels of protection of these key sites did not match the public’s expectations. Critical infrastructure operators and security organisations should be more open about the risks which exist and play a wider role in civil protection arrangements.

Out of these the following recommendations were made that are relevant to Consequence:

- RECOMMENDATION 55: The Government should strengthen and enforce the duty on Category 2 responders to share information on the risks to their infrastructure assets, enabling more effective emergency planning within Local Resilience Forums.

- RECOMMENDATION 56: The Government should issue clear guidance on expected levels of Category 2 responders’ engagement in planning, exercising and response and consider the case for strengthening enforcement arrangements.

In addition:

- 10 .31 A future means of sharing data from different organisations will be via the National Resilience Extranet (NRE) currently under development by the Cabinet Office and Communities and Local Government. The NRE will provide a resilient browser-based tool to enable efficient and secure exchange of information during both routine planning and emergency response. The Review has been informed that there will be a pilot of the NRE in selected local authorities during 2008, with the full roll-out expected in 2009 […]. [This represents a potential opportunity for Consequence.]

- 12 .61 Existing Cabinet Office guidance, ‘Data Protection and Sharing’ has sought to address some of the myths surrounding data protection as an aid to emergency planning, response and recovery. This guidance is intended to provide a framework within which personal information can be used with the confidence that individuals’ rights to privacy are respected. One of the key principles in it is that

---

data protection legislation is not a barrier to appropriate information sharing. The Review considers that this is a key point worthy of re-emphasising.

Chapter 18 deals specifically with the issue of information sharing and engagement and considers that: “Information is the lifeblood of effective emergency planning, and, as such, the sharing of information across the Category 1 and 2 divide and among all bodies involved in dealing with natural hazards such as flooding is essential. Effective working should also be based on wider engagement and cooperation with Category 2 responders. In particular, multi-agency response is likely to be more effective where all responders are well practised and versed in the relevant protocols” [Emphasis added]. Relevant points are given below:

- 18.7 […] Feedback from stakeholders has been mixed with some Local Resilience Forums (LRFs) displaying uncertainty and confusion over the process. At least two LRFs we heard from had received no briefing as yet, due to security sensitivities. Others had received their briefing but were advised not to cascade this information down to their risk and planning subgroup, again due to security concerns. As such, many planners are still taking an ad hoc (and possibly inefficient) approach to obtaining the information that they need.

- 18.9 More than one piece of feedback from LRFs mentioned problems with accessing the Environment Agency’s Receptors Vulnerable to Flooding (RVF) data. On further consultation with the Environment Agency, it appears that there are legal issues around the sharing of RVF data. The data is composed of information from Ordnance Survey and the Centre for Ecology and Hydrology and is subject to an Environment Agency approved-access procedure. This deals with issues around third-party intellectual property and contractual rights and as such, the Environment Agency cannot license it for access by others. [Again this is an aspect that consequence could help address.]

- 18.15 Under the current framework, Category 2 responders are supposed to work on the presumption that non-disclosure is the exception rather than the norm. Evidence from the response to the 2007 floods indicates that Category 2 responders have not been putting this principle into practice effectively.

- 18.19 Category 2 responders indicated that they feel they face a myriad of conflicting requirements, and that this is leading to uncertainty about what they can and cannot share. This in turn increases anxiety about the disclosure of material and discourages positive action.

- 18.21 In their response to the interim conclusions, Category 2 responders noted that it was not only the lack of a formalised process that led to their reluctance to share information. Security concerns were also a major issue. Western Power Distribution’s submission states: “When previously asked by local government to advise where loss of more than 100,000 customers might occur, WDP sought advice from the then UK Government Dept of Trade and Industry…[they] were advised to provide a ‘footprint’ showing an area affected but not to provide site location detail… the provision of such information is currently… against written advice.”

- 18.26 the question of why Category 1 responders, who have been entrusted with responsibility for leading civil protection work, are not equally trusted when it comes to accessing information that will allow them to perform that role effectively. We would welcome Government driving change, moving away from ‘need to know’ towards ‘need to share’. If necessary, this could include putting all emergency planners in local authorities through security clearance. Some LRFs we
spoke to had chosen to take this path, security clearing all of their emergency planning staff, and found that this avoided such serious problems in terms of being trusted with sensitive information. However, this process had been both time consuming and costly. [Again, the Consequence project could potentially help to address this issue.]

There is a greater awareness that moving from need to know’ to ‘need to share’ is critical. It is also recognised that while many of the issues around information sharing are ‘behavioural’, it would be beneficial to have clearer guidance and clearly defined information sharing protocols and networks.

- 18.34 Experience shows that the impact of natural disasters (such as floods) on critical infrastructure can be as big – or even bigger – than that of a security threat. In summer 2007, many tens of thousands of people were left without water and electricity, and hundreds of assets were flooded. Forward planning for such an event is impossible without information. Responders cannot legitimately be expected to identify what is critical without improved input from Category 2 responders. Greater willingness to share will also lead to greater cooperation, as individuals and agencies start to form effective working relationships and learn more about each others’ roles.

- 18.35 The CCA 04 states that: ‘In most instances, information will pass freely between Category 1 and 2 responders, as part of a more general process of dialogue and cooperation. This is the means by which the overwhelming majority of information sharing should happen...if this is not the case, it is probably evidence of a wider systematic failing in the way the Act is operating.’ The events of summer 2007 show that, in practice, neither the culture of cooperation nor the obligation to formally contribute information has flourished.

- 18.38 In order to develop clear and consistent guidelines, lead government departments should work together to develop guidance that clearly specifies what information can and cannot be released about critical infrastructure sites. Such guidance will also help to ensure that responders across the country have access to similar levels of information, that Community Risk Registers better reflect risks to critical infrastructure from flooding and other hazards and that the implications of both single points of failure and the complete loss of an asset are explicitly considered in all risk assessment and contingency planning undertaken by responders. Clearly defined information sharing protocols must be developed and new information sharing networks established as necessary to enable the level of sharing intended by the CCA.

The report gives case study examples of the strategies adopted by USA, Australia and the Netherlands to address the tension between greater transparency and control of information. They have been included here as they may be useful sources of information for the Consequence project:

- The US has developed the National Infrastructure Protection Plan (NIPP) a network approach to information sharing. It provides improved and more centralised mechanisms that support a real-time relay of strategic and tactical threat assessments, vulnerability assessments, threat warnings, situational or incident

---

6 CCA, Emergency Preparedness Guidance, p. 25, 3.7

Consequence Deliverable D5.1: Page 73 of 80
reports, lessons learned and best practices for critical infrastructure/key resources (CI/KR) information.

- Australia has a Trusted Information Sharing Network (TISN) for critical infrastructure protection. The TISN is not an operational network but is concerned with policy issues in a medium-to-long timeframe.

- The Dutch government set up the Critical Infrastructure Protection project. To make sharing of sensitive information possible, they recognised that there were three types of information: information that could be shared with everybody (green); information that could be shared in a previously defined professional group (orange); and information that would only be shared with the participants of the meeting (red). All participants were asked to sign a confidentiality agreement in which they promised to keep red information confidential. The classification of information was also used to ensure that the reports of the workshops were produced in such a way that confidentiality was respected. The reports are now available to other critical infrastructure operators and government. Another initiative used in the Netherlands has been the National Advisory Centre for Critical Infrastructure (NAVI), which is a public–private network between government and critical infrastructure operators who are able to share information on threats, risks and vulnerabilities. They use a similar colour-coding system for defining the level of confidentiality. Information can be shared via face-to-face contact, but also through closed websites.

A 6.5 Identifying People Who Are Vulnerable in a Crisis

The Cabinet Office issued “Guidance for Emergency Planners and Responders Civil Contingencies Secretariat” early in 2008. With regard to agreeing data sharing protocols and triggers, the following advice from the Cabinet Office (February 2008\(^7\)) should be of interest.

- **Agreeing data sharing protocols and triggers:** planning to meet the needs of vulnerable people in emergencies can only be done effectively through the proper sharing of data, which requires an understanding of data sharing parameters, busting data sharing myths, and the building of networks with relevant local and regional agencies. Reciprocally, in the response to an incident, effective data sharing ensures a timely provision of additional support for those that need it. The following section is in effect an abstract of data sharing guidance with relevance to vulnerable people in emergencies (for full details, see the Cabinet Office publication Data Protection and Sharing – Guidance for Emergency Planners and Responders).

- **Data Sharing and Civil Contingencies** CCA 04 allows the sharing of certain information for emergency planning purposes, although sensitive information – which would include personal data within the meaning of DPA 98 – needs to be subject to controls on the way it is handled, and the purposes to which it is put. *The restrictions that need to be placed on sharing information, at planning stage, are different from those applying in an emergency.*

Key points to consider are:

---

\(^7\) Source: www.ukresilience.gov.uk/~/media/assets/www.ukresilience.info/vulnerable_guidance%20pdf.ashx
The key law that governs the use of personal data is the DPA 98. The Act itself does not empower the sharing of data, nor does it prevent legitimate sharing: it puts in place a framework within which any sharing should take place.

It is likely that local authorities have legal powers to share information in the circumstances and context described within this guidance.

For the purposes of risk assessment and emergency planning, clear legal power to share information is found in secondary legislation made CCA 04.

Local and regional responders need to balance the potential damage to the individual (and where appropriate the public interest) in keeping the information confidential against the public interest in sharing the information as part of the response to an emergency (including the humanitarian response). A key question to ask is, ‘what would I want done if I were the data subject?’

Under DPA 98, consent of the data subject is not always a necessary precondition for lawful data sharing.

If personal data is collected by one organisation for a particular purpose, it does not mean that it can only be used by another organisation if the purpose is the same. The legal requirement is to ensure that the new purpose is not incompatible with the original purpose.

Appendix 7. Responder Infrastructure Profiles

In this Appendix we characterise the infrastructure and systems (the ‘resources’) profiles for the different stakeholders in the scenario.

From the point of view of infrastructure and systems, it is helpful to describe the responders in the scenario in terms of a 3 tier system:

- Tier 1: Responders within the immediate vicinity of the incident
- Tier 2: Control centres coordinating the responses from the Tier 1 groups
- Tier 3: Ancillary organisations providing services and information to Tier 2 control centres.

In the first tier the operatives are Category 1 responders at the scene. Tier 2 will involve Category 1 control officers, but may also include Category 2 officers as well. Tier-3 on the other hand may refer to a wider community including government agencies (weather, geophysical etc), commercial, charities and international agencies for example.

Tier 1

Tier 1 users are ‘blue light’ first responders including fire, police and ambulance. The communication channels with these responders would be via ‘voice’ and ‘data’ links. Voice links are used from control room commander to the responder on the scene. As pointed out earlier in Section 2.4 voice communications are, and will continue to be, an important means of transmitting commands and information to officers at the scene of these units.
The Data Link, on the other hand, is used for communicating application data such as video, (eg, video feeds transmitted from a camera on the responder), audio and maps (eg, building schematics for use on head mounted display devices) to command officers at the scene. The networks they use may be ad hoc, have limited bandwidth and capacity.

Tier-1 requirements are for accurate data on possible threats delivered in a timely manner together with coordination information to assist in complex rescue scenarios. Tier-1 users require real-time access to data while operating in a volatile environment with limited or intermittent data feed access. Any mission critical systems generally have multiple redundancies. Data should be updated whenever possible ie. by fast connection acquisition if it is available. The operating area for tier 1 is generally in close support of the incident, the radius can vary between tens of metres to a few kilometres. Typical hardware profiles will be of a hardened, robust, low power, hand held or vehicle mounted units with clear unambiguous displays. Within these groups data sharing agreements are, by legislation, secondary to life saving requirements. Nevertheless, life rescue missions can largely benefit from a timely and effective data sharing among 'blue lights' and other Tiers, eg, to view maps of facilities held by Category 2 responders for example.

**Tier 2**

Tier 2 users are the Control Centres associated with each of the ‘blue light’ services. They are tasked with commanding and coordinating the response, liaising with the other services and ensuring sufficient resources are available for the missions.

Tier 2 systems are used by the control centres to supply the Tier 1 users (ie, the responders at the scene) with guidance and information as well as maintaining a tactical overview of the incident. Generally Tier 2 control centres are not collocated and have good and established data links over public networks. Typical hardware profiles are desktop PC’s or laptops although applications are bespoke, ie, service-specific. The operating environment is relatively benign in comparison with Tier-1 (ie, is more like a conventional networked organisational system) though it may be subject to the typical threats on the wider Internet: spy ware, virus, email spamming etc. Their requirement is for near real time data to supply Tier 1 responders and request/receive soft real time (5 minutes or so) data from Tier 3 such that assessments of potential threats can be made. The management of appropriate data sharing agreements among Tier 1 and 2 responders in a timely and efficient way is a great challenge for Consequence.

**Tier 3**

Tier 3 users are the data proviers for the Tier 2 Control Centres. This includes utilities such as Gas and Electricity suppliers, local hospitals and could be as diverse as weather forecasting services from the MetOffice. In many cases it will be necessary to aggregate information from a number of Tier 3 responders prior to delivery of information to the Tier 2 control centres. Although the requirements from these responders is not as time critical as Tier 1, the responses would still be expected in minutes. The Tier 3 group will be geographically dispersed and will generally have disparate IT systems operating utility-specific applications. It is this group that is affected more than any other by data protection and access policies.
General Notes
There is thus a clear change in the characteristics of the systems that are used in a particular incident. The Tier 1 network is a very critical resource and is subject to far more rigorous management than other types of network. For example, detailed benchmarking through exercise drills ensures that operatives, processes, systems and applications they rely on meet the required overall performance standards. At the Tier-1 level, there are requirements for real time data access to ensure that operational efficiency is not compromised. Networks need to be resilient and may be ‘ad-hoc’, i.e., using any locally available networking infrastructure that can be assembled into a temporary working fabric for communications. However, despite this systems may be configured in preparation for data links that may be unreliable, slow and intermittent. To cope with this there may be strategies and algorithms for distributing data on a low bandwidth network, such as re-using data and a data refresh policy based on time-stamping. This amounts to the system entering a ‘blue flashing light mode’ to make optimum use of system and network resources. The client devices used will be highly portable, possibly integrated with suits and equipment.

Due to these performance constraints, it may be pragmatic to remove any detailed information from messages that is not required by the recipient in order to improve its delivery time. The question of ‘data-sanitisation’ as opposed to ‘data access control’ is for the evaluation studies to address. That is, what is the impact of data access control that Consequence promotes compared to the removal of information at source?

In Tier-2 these performance constraints are less apparent and there is more scope for accessing more detailed information, simply because it is possible to do so. In this regime, there is less practical need to reduce data size, information detail or message traffic because the systems can cope with it. Therefore, it may be difficult to control documents/messages that may contain personal/individual details and/or information that may be commercially sensitive and which can be shared across organisational boundaries at this level. Documents may be protected in transit between organisations by using transport level security (if this is possible - see below), Virtual Private Networks or by document level encryption. Document encryption, however, may not be always convenient to use and relies on the diligence of the individuals to be effective. Not least of the concerns here is protecting the document once it is un-encrypted.

The demarcation of Tier 1-2 system boundaries may often be blurred, but could in principle be determined by many methods. However due to the necessary redundancy requirements it may be necessary to link this to a hardware switch for the systems to enter the ‘blue flashing light mode’. Within Tier 1 connectivity to servers etc cannot be guaranteed thus manual override controls must be made available for a) sharing of data and b) moving systems into a Tier 1 status.

These organisations will use a variety of communications networks, some of which may be disabled by the incident, and some of which will have limited coverage, e.g., where buildings cast a radio shadow. The OASIS-fp6 project also developed techniques for ad hoc networks, using, for example, vehicle radios to relay messages where connectivity would be lost. Such a patchwork of networks and intermediaries may preclude the use of transport level security to protect the TSO data. In effect, the responsibility for controlling access to the TSO data is either pushed onto these ad-hoc network nodes or, in some novel way, onto the TSO itself. The first approach is a difficult network management problem and unlikely to be appealing, while the second approach is consistent with the general aims of the Consequence framework.
Fig AF7.1: Tier Infrastructure in the Scenario

The red regions in the centre of Fig AF7.1 represent the Tier-1 protected areas. The two non-overlapping regions, in this particular case, simply states that there are two responder units from different agencies assigned to different incidents and so do not have ‘contact’ with each other. The two are not required to share information in this case.

Fig AF7.1 can map directly onto the scenario description within the OASIS-fp6 project shown below in Fig AF7.2.

Fig AF7.2: Infrastructure Tiers within an OASIS Scenario
Appendix 8. Further Evaluation Methodologies & Techniques

This section contains an overview of measures that can assist the evaluation of crisis management systems from a Human Factors perspective. These will be investigated, if there is sufficient time to do so, in the final phases of the project when the basic top-level requirements presented in this document have been met.

A 8.1 Measures of Effectiveness

There is currently no standard explanation of what an MOE is, and to add to the confusion, there is a tendency to interchange other terms such as Measure of Performance (MOPs). Sproles [3,4] distinguishes between and MOEs and MOPs, by stating that MOEs measure external parameters or outcomes which are independent of the solution — a measurement of how well the problem has been solved, while MOPs measures the internal characteristics of a solution and how well it works. Essentially MOEs and MOPs are used to evaluate the performance of organizational units, teams or crews, and individuals (Gentner, [5]).

A 8.2 Measure of Effectiveness (MOE)

A definition for MOE is given by Sproles [3]: “Standards against which the capability of a solution to meet the needs of a problem may be judged. The standards are specific properties that any potential solution must exhibit to some extent. MOEs are independent of any solution and do not specify performance or criteria.”

A MOE, therefore provides a standard which helps to established how well some thing achieves the purpose for which it is intended. It answers the question “Does this meet my need?” (Sproles [4], 2002). In this context, a MOE is a measure of how effective the response was; “are we doing the right things?” and it is independent to the means of achievement, ie. the crisis management plan.

A 8.3 Measure of Performance (MOP)

A definition for MOP has been taken from SENAC website [8]: “Measure of how the system/individual performs its functions in a given environment (eg. number of targets detected, reaction time, number of targets nominated, susceptibility of deception, task completion time).”

From this perspective, an MOP is a measure of how efficiently the plan was followed, that is “are we doing things right?” It is directly related to the means of achievement, ie. the plan.

An MOP generally consists of two parts: an intended result or goal which is a measurable result, and parameters (restrictions or restraints) which are results not to be produced. Essentially an MOP would take this form: “Do this: [goal], subject to these [parameters]” (Casey [9]). It is important to note that an MOP statement does not describe how to achieve the end goal. See Table AT8.1 for an example.
Table AT8.1 Example of a MOP statement (taken from Casey, 2003)

<table>
<thead>
<tr>
<th>Goal: Reduce time to access database to two seconds or less.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters: No decrease in the amount of data available</td>
</tr>
<tr>
<td>No decrease in number of work stations running at one time.</td>
</tr>
<tr>
<td>Goal: Reduce abandoned calls rate to 8% or less.</td>
</tr>
<tr>
<td>Parameters: No increase in number of customers calling back because they have been cut off or because their problem was not satisfactorily resolved.</td>
</tr>
</tbody>
</table>

It is noted in the current literature that MOP and MOE are frequently interchanged, even though they measure different features. See Table AT8.2 for a comparison.

<table>
<thead>
<tr>
<th>Effectiveness</th>
<th>vs. Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measure of Effectiveness (MOE)</td>
<td>Measure of Performance (MOP)</td>
</tr>
<tr>
<td>• External measure from a stakeholder/results viewpoint</td>
<td>• Internal measure from the viewpoint of the solution/plan</td>
</tr>
<tr>
<td>• Invariant to means of achievement</td>
<td>• Coupled to means of achievement</td>
</tr>
<tr>
<td>• Are we doing the right things?</td>
<td>• Are we doing things right?</td>
</tr>
</tbody>
</table>

Table AT8.2 Differences between MOEs and MOPs (taken from Bullock[10], 2005)

To quote Sroles[3] “MOEs are concerned with how well the solution performs the intended purpose while MOPs look at how well the solution does what it actually does, and a parallel can be drawn with the distinction between effectiveness and efficiency or accuracy and precision.”

Essentially doing things right means efficiency — getting the most from your resources, whether they're people or products and you would use MOPs to check that this is the case. Doing the right things means effectiveness — setting the right goals and objectives and then making sure they're accomplished; MOEs would be used to measure this. It is important to consider both when analysing actions-to-effect to ensure that the plan was followed efficiently and that the outcomes where those desired.