Digital build & consultancy

www.panlogic.co.uk

National Operational Guidance Programme

NOGP Phase 2: Service Integration Tool
Specification summary for consultation

23 October 2017

Panlogic
Marcar House
13 Parkshot
Richmond
Surrey
TW9 2RG
Tel: 020 8948 5511
Fax: 020 8948 6611
www.panlogic.co.uk

Contacts:
Steve Beakhust
sbeakhust@ukfrs.com
07585 306 690

Will Danckwerts
will.danckwerts@panlogic.co.uk
0208 948 5511

© Copyright Panlogic Ltd. | www.panlogic.co.uk | info@panlogic.co.uk | blog.panlogic.co.uk | twitter.com/panlogicltd
Tel: +44 (0)20 8948 5511 | Fax: +44 (0)20 8948 6611
Panlogic Ltd, Marcar House, 13 Parkshot, Richmond, London TW9 2RG UNITED KINGDOM

© Copyright Panlogic Ltd. | www.panlogic.co.uk | info@panlogic.co.uk | blog.panlogic.co.uk | twitter.com/panlogicltd
Tel: +44 (0)20 8948 5511 | Fax: +44 (0)20 8948 6611
Panlogic Ltd, Marcar House, 13 Parkshot, Richmond, London TW9 2RG UNITED KINGDOM

1 Introduction

Traditionally, fire and rescue services maintain vast amounts of paper and digital documentation for all policy, procedure, training packs, equipment notes and other supplementary material. This was an area highlighted in the investigation and report into Atherstone on Stour by Justice MacDuff. Adapting this content to support national operational guidance may be no small feat, and fifty services doing it fifty times will inevitably produce a great deal of duplicated work requiring a large amount of resource.

The Service Integration Tool is our answer to how we can best help services implement a digital-first approach to national operational guidance, allowing full integration of local policy and procedure into a standardised digital platform, all with minimal time, effort and resource required from the organisation.

The National Operational Guidance Programme has engaged with UKFRSs to gather user requirements for a core solution. The core product will be developed using central funding and provided to fire and rescue services without charge.

The purpose of this document is to give an overview of the system specification and is supported by a more detailed technical specification and consultation questionnaire.

Each fire and rescue service is asked to review the proposal with their strategic, policy, training and ICT teams and respond to the consultation survey by **Monday 13 November 2017**.

Further information on the vision, process and development can be found on the NOG website.

The following link shows an interactive representation of the key functionality of the application:
http://l9ja7h.axshare.com

This interactive representation (wireframes) are shared/distributed centrally through ukfrs.com. The pages involved have a simplified graphic design to make it easier to see how things work. Within each page words marked as blue text are “clickable” and can be used (clicked on) to follow the flow from item to item.

This document summarises the features and functionality of the Phase 2 solution in accordance with the full specification developed for the NOG Programme team on 11 September 2017. If any issues arise during the implementation of these features and functionality which require discussion with all parties involved, this will be arrange through the NOG Programme team and an agreement made on the best way to proceed.

2 The product

In outline, the NOG phase 2 system is a set of separate installations, one for every participating FRS, comprising:

- A web server
- A Drupal content management system
- A content database
- An integration point to link the local instance with the central national operational guidance system

3 Security context

The product has been developed using currently recommended security practices and is designed for deployment in a secure cloud-based hosting environment. Security is assured through the development methodology used, system configuration, network perimeter devices, market leading hosting facilities, ongoing systems management, proactive security management and security monitoring.

The system will be resilient to external threats and attacks, such as viruses, unauthorised access attempts (hacking) and denial of service attacks. If for any reason the system “goes down”, in the standard offering the system will be brought back into service according to the timescale defined in the service level agreement. Within

© Copyright Panlogic Ltd. | www.panlogic.co.uk | info@panlogic.co.uk | blog.panlogic.co.uk | twitter.com/panlogicltd
Tel: +44 (0)20 8948 5511 | Fax: +44 (0)20 8948 6611
Panlogic Ltd, Marcar House, 13 Parkshot, Richmond, London TW9 2RG UNITED KINGDOM

the regime of ongoing system housekeeping, back-ups of key resources will be taken at regular intervals. These back-ups will be stored separately from the operational system and used if a system recovery is necessary, e.g. as part of business continuity processes.

The system operates with a minimal set of personally identifiable information, sufficient to enable individuals to use the system and to adjust certain profile preferences. Passwords and user related information are stored using industry standard encryption technology. Profile information is handled in compliance with the General Data Protection Regulation (GDPR).

In self-hosted and intranet scenarios, the FRSs are responsible for security of the hosting infrastructure.

4 Product components

The table below lists the main NOG Phase 2 system components:

System component	Description
Web platform	A Drupal web site, database system and associated hosting facilities – virtual server and storage.
Guidance database	A separate, local, instance of the central/national operational guidance with a copy management mechanism to keep the local copy synchronised with the national information in an auditable way.
Guidance content management	Guidance is managed at the national system and is made available to each FRS as a local copy, which is read only – the content cannot be edited or changed. This local copy is kept in step with the national system by a synchronisation mechanism which sends a copy of every change across to the local system.
Workflow	When updates are made to national operational guidance content, these updates and changes are sent down to the local instance through a synchronisation mechanism. The changes and updates are fed into a workflow system. This is effectively a queue which allows the FRS to assess and evaluate every update before those updates are accepted and applied to the local read only copy. This allows FRSs to perform their own processes in respect of every update, for example to carry out a risk assessment or to ensure they have an appropriate training package available.
Custom content fields	In the local copy, each content component has an associated custom content field which can be populated and managed/maintained locally. This allows each FRS to provide their own localisms to every piece of national guidance. For example: additions to NOG hazard knowledge with locally relevant hazard information
Product packs	Product packs are locally created content based on nationally held and managed templates. Product pack content can be linked to the locally managed copy of national guidance as well as local content (custom content fields and other product pack content items).
Change management	Changes made to the structure of the national operational guidance as well as any new or amended functions are made available to local instances through a change management control mechanism.

5 Overview of initial deployment

To bring an FRS on-board with the NOG Phase 2 system there are a number of high-level steps to be carried out. Automated deployment packages and scripts are an essential component of the deployment. The high-level steps are:

1. Acquire hosting environment
2. Deploy the installation package, which sets up the Drupal system, web server and all related code components
3. Use a recent back up of the relevant data from the national system to populate the local instance
4. Connect up the local instance to the national system and initiate the synchronisation process
5. Configure and enable user access

© Copyright Panlogic Ltd. | www.panlogic.co.uk | info@panlogic.co.uk | blog.panlogic.co.uk | twitter.com/panlogicltd
Tel: +44 (0)20 8948 5511 | Fax: +44 (0)20 8948 6611
Panlogic Ltd, Marcar House, 13 Parkshot, Richmond, London TW9 2RG UNITED KINGDOM

6 Branding

The local instance will allow a certain amount of localised branding to give the local system a clear identity and visual connection to the rest of the FRS's systems environment so that users have a sense of where they are and what it is they are accessing. This local branding includes: logo, colour scheme, stock imagery, certain title elements and home page custom text. Default content for these can be overwritten at the local level.

7 Workflow

The purpose of the workflow system is to control the way updates and changes to national content are received and managed at the local level:

- The synchronisation mechanism transports changes to the local system;
- The workflow system deals with the changes and the way these are managed locally.

Regular end-users will not be aware of the workflow system – they see the local content in its approved "live" state and have no visibility of any information which is yet to be accepted.

When a change arises with a piece of national guidance content a change transaction is shipped to the local FRSs. Each FRS has to work through formal business processes to assess the impact and risk implications of each change and to develop, revise or create new policies, procedures, training and product packs as a result. The detailed execution of these formal processes varies between FRSs but the fundamental requirement, that changes need to be evaluated before they can be accepted, is common, even if that acceptance is very lightweight or even automated.

Workflow is handled by people who have workflow administration responsibilities. Changes to NOG will progress through a series of simple approval states over a period of time as the FRS works their way through their respective processes. Changes can be acknowledged, marked in progress, put on hold and accepted. In general, it is not expected that a change could ever be rejected, it is more a matter of timing and preparation before all changes are ultimately accepted. The change contents and context can be viewed but cannot be changed. If an FRS has a requirement to contextualise a change then this can be handled as part of the change evaluation and usage of the custom content fields.

As items progress through the workflow system audit records are created. These records allow authorised users to look back at any change and find out what happened to it from the point the FRS became aware of it and its current status. Services will be able to scroll through the queue of workflow items to assess how up to date their currently accepted content is as compared with the central NOG. Workflow changes are "pulled" automatically by the system at a predetermined regularity.

8 Custom content fields

NOG content is represented at the local level as a read-only, system managed (synchronised) copy. The national content cannot be edited, changed or deleted at the local level. However, we recognise that FRSs may have requirements to be able to add to the national content to reflect their own particular requirements or situations in respect of what the national guidance is saying. This is achieved through the use of custom content fields which are linked to certain content components, e.g. sections, hazards and control measures.

Authorised users at the local level may use these custom content fields, if they wish, to provide additional content and information pertaining to the national guidance. Facilities are provided so that these users can edit and change what the custom content says. The system keeps a history of the changes that have been made and this helps FRSs manage their custom content over time.

© Copyright Panlogic Ltd. | www.panlogic.co.uk | info@panlogic.co.uk | blog.panlogic.co.uk | twitter.com/panlogicltd
Tel: +44 (0)20 8948 5511 | Fax: +44 (0)20 8948 6611
Panlogic Ltd, Marcar House, 13 Parkshot, Richmond, London TW9 2RG UNITED KINGDOM

9 Product packs

Product packs are locally created content based on centrally held and managed templates. These product packs encompass a defined set of document types, the following types are included as standard:

- Operational Information Notes (OIN)
- Equipment Notes (EN)
- Training Packages (TP or OTN)
- Supplementary Information (SUP)
- Impact Assessments (IA)

These templates were designed by services to help standardise the approach to common document types and enable easy sharing of best practice examples between services. The following link shows an interactive representation of the product packs, how they work and the format they currently adhere to:
http://l9ja7h.axshare.com

Each document type has a centrally managed document template which is used at a local level to create corresponding documents. Suitably authorised content managers on the local instance are able to create product pack items using these templates. To permit effective management of the templates some sections will be fixed while others will allow more flexibility to tailor and customise to circumstance.

These documents are stored and managed entirely at the local level. This allows FRSs to have their own product packs shaped around their own needs. Product pack content can be linked to the locally managed copy of national guidance as well as local content (custom content fields and other product pack content items). For example, an equipment note could be linked to a NOG control measure and a variety of impact assessments could be linked to the equipment note. This equipment note may be applicable to more than one control measure; when it is linked to other content the attached impact assessments will automatically follow.

Where appropriate, this will also allow product pack content to automatically integrate with the local instance of scenarios.

As product pack documents are updated and changed previous versions are captured automatically as a version history log. This log forms a record of every change made over time as a simple list and users can view the log entries one-by-one to see what each change entailed.

Product packs are one approach to localising guidance. Services may choose to just attach existing documentation (docs, PDFs, URLs etc.) to locally held national content using custom content fields (see Section 8 above).

More information on the product pack approach can be found in Section 2.1.7 in the accompanying full specification.

10 Good practises

It is envisaged that much of the product pack content will be universal to all services, with relatively few fields requiring local tailoring (e.g. local procedure within an OIN). As such, services will be able to share the workload in producing the generic content for each document type and submit them into a central repository. From here the documents can be downloaded into any local instance where the locally appropriate fields can be amended/populated.

To complete the cycle of central guidance and integrated localisms there is a facility to enable examples of local good practice to be shared to the central system. This works by the local user downloading their example and submitting it through the good practices area on the central NOG system. The National Implementation Forum will be the assurance board and coordinating forum for the development of product packs. This platform would be well placed to identify and agree best practice examples to upload into the central repository for download by other FRSs for local tailoring.

© Copyright Panlogic Ltd. | www.panlogic.co.uk | info@panlogic.co.uk | blog.panlogic.co.uk | twitter.com/panlogicltd
Tel: +44 (0)20 8948 5511 | Fax: +44 (0)20 8948 6611
Panlogic Ltd, Marcar House, 13 Parkshot, Richmond, London TW9 2RG UNITED KINGDOM

In some instances, it may be appropriate to have more than one version of a single product pack available in the central repository to account for the variation of approaches nationally. For example, an OIN for compartment firefighting could be written for a variety of techniques – one for traditional door opening procedures and gas cooling, one for cold cut cobra, and one that encompasses a mixture of both.

11 User functionality

Core user functionality is the ability for end users to be able to navigate, find and view national operational guidance along with any localisms, such as custom content fields and product packs.

Certain users will have responsibility for managing the localised content and these users will have additional editing capability attached to their user profile. Some users will also be involved in the workflow system and the approvals process and will be assigned a workflow role.

The standard roles and permissions model has been designed for simplicity with just three roles: authorised user, content manager and workflow administrator. In addition to these roles, access to certain categories of content are controlled through pre-configured permissions. So, for example a training manager could be assigned the content manager role. That assignment gives the training manager user editing and publishing capabilities as well as the permission to view NOG Training Specification content as opposed to a normal authorised user who may view training product pack material but not NOG Training Specifications when using the local Phase 2 site. The user account for the training manager is then given access to edit the training product pack material. The way content is categorised and grouped for permissions purposes also follows a simple model:

- Content that anyone with the content manager role can edit and publish;
- Content that can only be edited and published by users who are both content managers and have explicit permission for that particular category of content.

The standard content categories are:

- Site page content (home page, about pages, contact pages etc.);
- NOG custom content fields;
- Product pack items, one for each template type.

The model can be extended, through additional work, to meet more complex role requirements.

Beyond these capabilities, further functionality is provided for users:

Functionality	Description
User registration	Users need to be registered on the local system so that they can access content. This base level registration is either carried out by the user themselves or the registration is made on their behalf by a user administrator. Higher level roles, such as content managers or workflow administrators are additional permissions applied on top of the base user registration.
Bookmarking	This is the ability for users to bookmark local content and to set notification preferences, triggered when book marked content is updated.
Feedback	Ability for users to provide feedback on national and/or local content. Feedback on national content is captured locally and forwarded to the central system for collation.
Printing	The ability to print content.
Combined printing	The ability to mark several pieces of content and print as a single entity.

12 User access

To access protected content users are required to present a set of account login details and achieve a successful login. The user account used to access the FRS local instance is a separate login name and password from any other account users may utilise to access other FRS systems. As standard, there is no integration and synchronisation of accounts, for example with the FRS windows network login, and therefore no “single sign-on” experience.

© Copyright Panlogic Ltd. | www.panlogic.co.uk | info@panlogic.co.uk | blog.panlogic.co.uk | twitter.com/panlogicltd
Tel: +44 (0)20 8948 5511 | Fax: +44 (0)20 8948 6611
Panlogic Ltd, Marcar House, 13 Parkshot, Richmond, London TW9 2RG UNITED KINGDOM

Users on the FRS instance are local to that system. Should they wish to access central NOG content (e.g. beyond basic browsing) then they would need to separately register with NOG.

By default, as a cloud-based service the site will be accessible from any machine/network, but password-protected, without having to make any specific access exception rules as you may need to do on your internal networks. Further explanation of the options is outlined below:

- A website on a Cloud-based server is typically set up to be accessible through the internet (i.e. by any machine)
- An intranet site set up within an internal network is typically set up to be accessible from within that network only
- A Cloud-based site can be configured to only serve traffic from a specific network, and a locally-hosted intranet site can be configured to accept traffic from the wider internet as well
- For the Cloud-based options, configuring the sites to be accessible only from a certain network would be done on a case-by-case basis (rather than as part of an automated deployment) either by Panlogic or the local service, depending on who was managing the hosting infrastructure
- With any of the options the local instance can be password protected so that when someone reaches the site, they have to login to view or access the content

13 Adoption models

Four models are available for local implementation of the Service Integration Tool:

1. Standard platform as a service
2. FRS self-managed cloud infrastructure i.e. the FRS provides the hosting infrastructure but Panlogic manage the application installed onto that hosting
3. FRS self-managed cloud platform i.e. the FRS provides the hosting infrastructure, deploy the application provided by Panlogic and manage the application/apply Panlogic's application updates moving forwards
4. FRS self-managed on premise platform

13.1 Hosting platform

The standard offering uses a cloud based hosting platform (Amazon Web Services) which runs the Drupal web site, guidance database and synchronisation mechanism. Each FRS has their own separate slice of hosting running within a virtualised cloud hosting environment. The cloud hosting environment provides the basis for remote access to local FRS guidance from mobile devices.

FRSs provide a suitable domain or sub-domain name to be used as the URL for the service, e.g. www.midsomer.gov.uk or guidance.existingurl.gov.uk

The service sits outside of the FRS network and is accessed/consumed as a cloud service. FRS systems, network configuration and security policy must permit all users to navigate to and reach the cloud service.

Unlike the national system, the local instances implement a security layer which requires all users to go through a logon authentication process before they are able to access any content (beyond a logon landing page). Users will have a separate user identity and corresponding set of security credentials to access the service.

13.2 Standard support model / service wrap

For the standard hosting platform offering the standard support model addresses the following support requirements:

- Hosting support;
- Application support;
- Integration support;

© Copyright Panlogic Ltd. | www.panlogic.co.uk | info@panlogic.co.uk | blog.panlogic.co.uk | twitter.com/panlogicltd
Tel: +44 (0)20 8948 5511 | Fax: +44 (0)20 8948 6611
Panlogic Ltd, Marcar House, 13 Parkshot, Richmond, London TW9 2RG UNITED KINGDOM

- Deployment / set-up support;
- Training and knowledge transfer;
- Development support;
- Advice and guidance “how-to” type support;
- Service levels.

With the standard offering, Panlogic handles the on-boarding process by providing project management, technical resources and execution. We can mobilise quickly and we are largely self-managing, only requiring input where decisions need to be made around options. We would usually aim to be able to deploy the standard platform in **a week to 10 days** from the kick-off point.

13.3 Alternative models

The standard and alternative hosting and support models are:

Service layer	Standard platform as a service	FRS self-managed cloud infrastructure	FRS self-managed cloud platform	FRS self-managed on-premise platform
Description:	*Standard hosting and support model*	*Cloud based infrastructure managed by FRS*	*Cloud based platform managed by FRS*	*On-premise platform managed by FRS*
Hosting infrastructure provision + support	Panlogic	FRS	FRS	FRS
Application support (configuration + bespoke elements)	Panlogic	Panlogic	Panlogic	Panlogic
Drupal website and content database provision + support	Panlogic	Panlogic	FRS	FRS
Initial deployment project management	Panlogic	FRS	FRS	FRS
Service level	Panlogic full service level agreement	Panlogic operations level agreement (into FRS service level agreement)	FRS service level agreement	FRS service level agreement

For all these alternative hosting options, the FRS will be responsible for setting up the environment, deploying the application and testing. The stages involved in self-managing the initial deployment set up and “getting on board” are:

Activity
Prepare baseline knowledge (inc. read training materials)
Look at system requirements and prepare to procure hosting
Decide resources
Decide governance model
Build out project plan
Consider project risks
Decide how hosting will be handled
Identify dependencies
Estimate budget
Decide which product pack templates will be used
Agreement to proceed; Commit resources; Allocate budget
Procure hosting arrangements
Obtain installation package
Perform system installation

© Copyright Panlogic Ltd. | www.panlogic.co.uk | info@panlogic.co.uk | blog.panlogic.co.uk | twitter.com/panlogicltd
Tel: +44 (0)20 8948 5511 | Fax: +44 (0)20 8948 6611
Panlogic Ltd, Marcar House, 13 Parkshot, Richmond, London TW9 2RG UNITED KINGDOM

Perform post-installation tasks
Database import
Configure local branding and logo
Initiate synchronisation
Run commissioning tests
Switch to live operation
Content editor training
User/train-the-trainer training

Once the system is up and running there are support obligations, which need to be dealt with proactively, to keep the environment secure, resilient and operational:

Support activity
Apply patches and fixes to the linux operating system
Apply patches and fixes to the web server system
Apply patches and fixes to the database management system
Apply patches and fixes to the Drupal content management system
Ensure the timely application of any security related fixes across all the above platform layers
Maintain network perimeter security, reviewing port scans and any suspicious activity
Keep all Drupal community modules up to date
Check all system, security and application logs on a regular basis
Check system report on a regular basis
Maintain a regular cycle of system and database backups for recovery purposes
Perform periodic whole system upgrades to move the platform to the latest release levels

Our expectation is that FRSs will vary in their readiness, access to skills/experience and availability of resources. Depending where a particular FRS sits on this scale we envisage that the elapsed time required to get up and running will typically lay somewhere between **1 and 3 months**; what we describe as a reasonable minimum through to a typical deployment. The characteristics of each of these is denoted below:

Reasonable minimum elapsed time: 1 month
Assumes: ready to accept NOG content, business ready to proceed, organised, familiar with Drupal (e.g. have worked on a previous Drupal installation or managed a Drupal system), skilled and experienced resources, dedicated project manager, able to commit resources

Typical deployment of business and technical environment: 3 months elapsed
Assumes: not all NOG content accepted, business not fully ready, lack of in-house skills/experience, not dedicated project manager or no project manager, resources matrix managed against other business priorities

We also expect that some FRSs will want to take longer than these guidelines and may wish to gradually adopt the new system gradually running alongside their current processes. This is a valid option and can be supported.

In either case, for an FRS provided arrangement the following roles are required:

- Person or team responsible for installation and deployment
- Person or team responsible for supporting hosting and operating system
- Person or team responsible for supporting Drupal and database server
- Service manager / single-point-of-contact for service management

13.4 Training

The standard support allocation includes ad-hoc training and knowledge transfer. Panlogic can also develop a more detailed and dedicated set of training materials (i.e. videos/manuals, online screen casts etc.) should these be required and will have staff available for face-to-face training with local services, should they wish to arrange for this separately.

© Copyright Panlogic Ltd. | www.panlogic.co.uk | info@panlogic.co.uk | blog.panlogic.co.uk | twitter.com/panlogicltd
Tel: +44 (0)20 8948 5511 | Fax: +44 (0)20 8948 6611
Panlogic Ltd, Marcar House, 13 Parkshot, Richmond, London TW9 2RG UNITED KINGDOM

14 Costs

The core product will be developed from central NOG funding and provided to local services without charge. Beyond provision of the core product, local services will be expected to cover costs as follows.

14.1 Standard adoption approach

The following costs apply to the standard adoption approach:

- Onboarding cost per service (including technical and account setup costs): **£4,250**
- Monthly support cost for each service for fully-managed standard support model/service wrap including **(£1,751)**:
  - Application support;
  - Infrastructure support;
  - Development support;
  - Account management (2 days).
- Monthly hosting costs (as part of fully-managed standard support model/service wrap): This is estimated to be up to **£422.50 per month** but will depend on a number of factors such as economies of scale to be gained depending on number of services who have onboarded, volume of traffic to local instances and quantity of content changes made by the central NOG programme.

The proposed time and cost involved is based on assumptions around the likely support demands of local services and the amount of further development the NOG Programme team will look to invest in the tool. If a local service requires more support from Panlogic than is planned, this could be arranged and suitable time/cost agreements made on a case-by-case basis. If, in general, support required for all local services needs to be increased or the investment in changes and new features requested through the NOG Programme team also needs to be increased, this could also be agreed. Panlogic suggest quarterly review meetings/checkpoints where feasible to discuss and assess support availability.

An SLA would be agreed between the local services and Panlogic, should they make the decision to onboard.

14.2 Alternative adoption approach

In cases where a local service chooses an alternative option other than the fully-managed standard support model/service wrap, Panlogic would agree time and cost on a case-by-case basis in a bespoke SLA.

If a local service also wished to request Panlogic make feature developments to their instance which diverge from the core, centrally-provided solution, development and management costs would also need to be agreed on a case-by-case basis and with a bespoke SLA where appropriate.

© Copyright Panlogic Ltd. | www.panlogic.co.uk | info@panlogic.co.uk | blog.panlogic.co.uk | twitter.com/panlogicltd
Tel: +44 (0)20 8948 5511 | Fax: +44 (0)20 8948 6611
Panlogic Ltd, Marcar House, 13 Parkshot, Richmond, London TW9 2RG UNITED KINGDOM