BY OPENING THIS DOCUMENT YOU HAVE EXPLICITLY AGREED TO THE FOLLOWING TERMS AND CONDITIONS WITHOUT RESERVATION

You have requested access to a copy of a report prepared by PricewaterhouseCoopers LLP ("PwC") on the Electronic Staff Record Programme (ESR) ISAE 3000 Type II Controls Report Period: 1 April 2021 to 31 March 2022 (the "report"). NHS Business Services Authority, to whom the report is addressed, has confirmed that a copy of the report may be provided to you. PwC* has consented to release of the report to you on condition that you accept and agree to the terms below.

By clicking on the "I ACCEPT THE TERMS OF THIS AGREEMENT" button upon opening this document, you confirmed the following:

I accept and agree for and on behalf of myself and the entity I represent (each a "recipient") that:

1. PwC accepts no liability (including liability for negligence) to each recipient in relation to PwC's work or its assurance report. The report is provided to each recipient for information purposes only. If a recipient relies on PwC's report, it does so entirely at its own risk;

2. No recipient will bring a claim against PwC which relates to the access to the report by a recipient;

3. Neither PwC's report, nor information obtained from it, may be made available to anyone else without PwC's prior written consent, except where required by law or regulation;

4. PwC's report was prepared with NHS Business Services Authority's interests in mind. It was not prepared with any recipient's interests in mind or for its use. PwC's report is not a substitute for any enquiries that a recipient should make. The description of internal controls is for the period 1 April 2021 to 31 March 2022, and thus PwC's assurance report is based on historical information. Any projection of such information or PwC's opinion thereon to future periods is subject to the risk that changes may occur after the report is issued and the description of controls may no longer accurately portray the system of internal control. For these reasons, such projection of information to future periods would be inappropriate;

5. Any explanations that PwC may provide to any recipient in relation to the report are given on the same bases as those relating to the provision of the report itself;

6. PwC will be entitled to the benefit of and to enforce these terms; and

7. These terms and any dispute arising from them, whether contractual or non-contractual, are subject to English law and the exclusive jurisdiction of English courts.

If you have received this document and you have not confirmed your agreement to PwC's disclaimer in the terms of access by clicking the "I ACCEPT THE TERMS OF THIS AGREEMENT" button upon opening this document, you are an unauthorised recipient and should return or destroy the document.

* PwC refers to PricewaterhouseCoopers LLP, a limited liability partnership incorporated in England (number OC303525), whose registered office is at 1 Embankment Place, London WC2N 6RH

Electronic Staff Record Programme (ESR)

ISAE 3000 Type II Controls Report

Period: 1 April 2021 to 31 March 2022

Table of Contents

1. Report by Management

Background

The ESR Solution is a single payroll and Human Resources (HR) management system that has been fully implemented across the whole of the NHS in England and Wales. The system has replaced multiple fragmented payroll and HR systems which were previously in use within the NHS. Its implementation was completed by 31 March 2008. The system brings the following benefits:

- Integrates every aspect of payroll, HR and staff management;
- Eliminates multiple data entry;
- Allows self-service by staff and management;
- Enables records to move with the employee; and
- Produces consistent reports at local, regional, and national levels.

Scope

This report covers the design and operating effectiveness of the Information Technology (IT) general controls in place, which facilitate the integrity, stability and reliability of the service. These controls are predominantly designed and operated by IBM. Additionally, there are certain controls related to the NHS General Ledger Interface, which are the responsibility of the NHS ESR Central Team.

This report covers the following six areas for the period 1 April 2021 to 31 March 2022. Each of the areas relate to one of six control objectives for which independent testing has been performed and the results documented in this report (refer to section 6):

- Change Management;
- Logical Security;
- Problem Management and Performance and Capacity Planning;
- Physical Security and Environmental Controls;
- Computer Operations; and
- Payslip Distribution.

The proceeding sections in this report detail:

- Management’s description of the ESR Programme and the internal control environment for the period 1 April 2021 to 31 March 2022 [section 4 and 5];
- Management’s description of the IT general controls and controls over payslip distribution for the ESR Service for the period 1 April 2021 to 31 March 2022 [section 4, 5, and 7]; and
- The results of testing performed to confirm the design and operating effectiveness of controls [section 6].

Impact of COVID-19

When COVID-19 and the associated risk to NHS BSA staff and business operations came to light in March 2020, the NHS BSA initiated plans to ensure as many staff as possible could work from home. Alongside the focus on staff safety and working arrangements, the NHS BSA has stood up new services and enhanced existing services to support health and care as part of the government response to COVID-19.

Operational processes were reviewed and amended, where required, to support home working, while maintaining service performance levels and changing physical audit documentation to digital records.

2. Management and subservice provider statements

NHS
Electronic Staff Record
Fifth Floor
Don Valley House
Savile Street East
Sheffield S4 7UQ

www.esr.nhs.uk
@nhsesr

Service organisation's management statement on controls at NHS Business Services Authority (the "Service Organisation")

As Directors of NHS Business Services Authority ("NHS BSA") we are responsible for the identification of control objectives relating to the provision of controls supporting the provision and maintenance of the Electronic Staff Record system ("ESR system") by the Service Organisation and the design, implementation and operation of the Service Organisation's controls to provide reasonable assurance that the control objectives are achieved.

In carrying out those responsibilities we have regard not only to the interests of user entities but also to those of the NHS England and the general effectiveness and efficiency of the relevant operations.

NHS BSA uses IBM United Kingdom Limited ("IBM UK"), an inclusive Subservice Organisation, to provide IT and payslip printing services to the Service Organisation. The Service Organisation's description includes a description of IBM UK's IT and payslip services used by the Service Organisation to process transactions for user entities, including the relevant control objectives and related controls. The description indicates that IBM UK has subcontracted elements of the services provided to the Service Organisation to other third-party providers including OPUS Trust Communications (OPUS), which provides payslip printing services. IBM UK monitors the performance of third-party subcontractors including OPUS, and remains fully accountable for outsourced services including payslip printing and delivery of payslips to NHS Organisations that use the ESR system. The description includes only the controls at NHS BSA and the included subservice organisation, IBM UK, and not controls at OPUS or any other third-party subcontractor.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of NHS BSA's controls are suitably designed and operating effectively, along with related controls at the Service Organisation. The description does not extend to controls of the user entities.

The accompanying description in Sections 5 and 6 (the "description") has been prepared for user entities who have used the ESR system and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by its customers, when assessing the risks of material misstatements of its customers' financial statements.

We have evaluated the fairness of the description, and the design suitability and operating effectiveness of the Service Organisation's controls having regard to the International Standard on Assurance Engagements 3000 (ISAE 3000), issued by the International Auditing and Assurance Standards Board.

We confirm that:

1. The accompanying description, in Sections 5 and 6, fairly presents the Service Organisation's provision and maintenance of the ESR system, and the services provided to the Service Organisation by the included Subservice Organisation, throughout the period 1 April 2021 to 31 March 2022. The criteria used in making this statement were that the accompanying description:

   - presents how the services were designed and implemented, including:

     - the types of services provided, and as appropriate, the nature of transactions processed;
     - the procedures, both automated and manual, by which user entities' transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for user entities;
     - the related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for user entities;
     - the systems which captured and addressed significant events and conditions other than user entities' transactions;
     - the process used to prepare reports for user entities;
     - relevant control objectives and controls designed to achieve those objectives;
     - controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve the control objective stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone; and
     - other aspects of our control environment, risk assessment process, information systems (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting user entities' transactions.

   - includes relevant details of changes to the systems during the period; and
   - does not omit or distort information relevant to the scope of the services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities and their auditors, and may not, therefore, include every aspect of the services that each individual user entity may consider important in its own particular environment.

2. Except for the matters referred to in the 'Controls exceptions identified' paragraph below, the controls related to the control objectives stated in the accompanying description were suitably designed and operating effectively throughout the period 1 April 2021 to 31 March 2022, if user entities applied the complementary controls assumed in the design of the Service Organisation's controls. The criteria used in making this statement were that:

   - the risks that threaten the achievement of the control objectives stated in the description were identified;
   - the identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
   - the controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period.

Controls exceptions identified

As stated in Section 6 of this report, the controls necessary to ensure that access to the development and production areas of the NHS hub was controlled and appropriately restricted, were not designed effectively from 1 April 2021 to 6 June 2021 but updated controls were implemented on 7 June 2021. As a result, there were insufficient logical access controls in place to appropriately restrict access to the development and production area of the NHS hub for part of the reporting period and therefore controls were not suitably designed to achieve Control Objective 2 "Controls provide reasonable assurance that security configurations are created, implemented and maintained to prevent inappropriate access" during the period 1 April 2021 to 6 June 2021.

Director for and on behalf of the Board of Directors
NHS Business Services Authority

Andrew McKinlay
04/05/2022

IBM United Kingdom Limited
76 Upper Ground
South Bank
London, SE1 9PZ
Tel: +44 (0)20 7202 3000
Fax: +44 (0)20 7202 5935

Subservice Provider's Statement

04/05/2022

Statement by the Directors of IBM United Kingdom Limited

As Directors of IBM United Kingdom Limited ("IBM UK"), service providers to NHS Business Services Authority ("NHS BSA"), we are responsible, together with NHS BSA's directors, for the identification of control objectives relating to the provision the IT and payslip printing services that are relevant to the Electronic Staff Record (ESR) workforce solution system. We are also responsible for the design implementation and operation of IBM UK's controls to provide reasonable assurance that the control objectives are achieved.

The description indicates that IBM UK has subcontracted elements of the services provided to NHS BSA to other third-party providers, including OPUS Trust Communications ("OPUS"), which provides payroll printing services. IBM UK monitors the performance of the third-party subcontractors including OPUS and remains fully responsible for those outsourced services including payroll printing and delivery of payslips to customers that use the ESR system. The description does not include the controls at OPUS or other third-party providers that IBM UK has outsourced services to.

The accompanying description including the services provided to NHS BSA and the details of the controls have been prepared for entities who have used the ESR system during the period 1 April 2021 to 31 March 2022 and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements.

In carrying out those responsibilities, we have regard not only to the interests of user entities but also the general effectiveness and efficiency of the relevant operations.

We have evaluated the fairness of the description and the suitability of the design and operating effectiveness of controls over services provided by IBM UK to NHS BSA, having regard to the International Standard on Assurance Engagements 3000 (ISAE 30000), issued by the International Auditing and Assurance Standards Board and the control objectives for the IT and payslip printing services provided to NHS BSA and relevant to the ESR system.

We confirm that:

a) The accompanying description in section 5 and 6 fairly presents IBM UK's services provided to NHS BSA and relevant to the provision of the ESR system and payslip printing services throughout the period from 1 April 2021 to 31 March 2022. The criteria used in making this statement were that the accompanying description:

i. Presents how the services were designed and implemented, including: the types of services provided, including IT and payslip printing, the functions by which access to systems and data was restricted, the degree of systems integrity and resilience commensurate with the nature and confidentiality of the information processed and external threats, the requirements for maintaining and developing systems hardware and software; the means by which recovery from processing interruptions was achieved as necessary; and other aspects of the control environment, risk assessment process, monitoring and information and communication systems, that were relevant to the control activities.

ii. Includes relevant details of changes to the IT systems and services during the period from 1 April 2021 to 31 March 2022.

iii. Does not omit or distort information relevant to the scope of the services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of the ESR user entities and their auditors and may not, therefore, include every aspect of the services that each individual ESR user entity may consider important in its own particular environment.

b. The controls related to the control objectives stated in the accompanying description were suitably designed and operating effectively throughout the period from 1 April 2021 to 31 March 2022. The criteria used in making this assertion were that:

i. The risks that threatened achievement of the control objectives stated in the description were identified;

ii. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated IT control objectives from being achieved; and

iii. The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period noted above.

Confirmed for and on behalf of the Board of Directors of IBM United Kingdom Limited

....

[Name and signature of authorised client signatory]

Louis Bilella, IBM Consulting,Public Sector - Vice President & Senior Client Partner - UK NHS ESR Account
....

[Title of authorised signatory]

4th May 2022
....

[Date]

Independent service auditor’s assurance report on controls at NHS Business Services Authority (the “Service Organisation”) To the Directors of NHS Business Services Authority

Scope

We have been engaged to report on NHS Business Services Authority (“NHS BSA”)’s description of its controls supporting the provision and maintenance of the Electronic Staff Record system (“ESR system”) throughout the period 1 April 2021 to 31 March 2022 in Sections 5 and 6 (the “description”), and on the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The controls and control objectives included in the description are those that management of the Service Organisation believe are likely to be relevant to user entities’ internal control over financial reporting.

IBM United Kingdom Limited (IBM UK) (the “included Subservice Organisation”) is a subservice organisation that provides IT and payslip printing services to the Service Organisation. The Service Organisation’s description includes a description of the included Subservice Organisation's IT and payslip printing services used by the Service Organisation to provide controls supporting the provision and maintenance of the Electronic Staff Record system to its user entities, as well as relevant control objectives and controls of the included Subservice Organisation.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Service Organisation’s controls are suitably designed and operating effectively, along with related controls at the Service Organisation. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls. The description also indicates that IBM UK has subcontracted elements of the services provided to the Service Organisation to other third-party providers including OPUS Trust Communications (“OPUS”), which provides payslip printing services. IBM UK monitors the performance of third-party subcontractors including OPUS, and remains fully accountable for outsourced services including payslip printing and delivery of payslips to NHS Organisations that use the ESR system. Our examination only applied to the controls at the Service Organisation relevant to the ESR system and the included subservice organisation, IBM UK, and did not extend to controls at OPUS or any other third-party subcontractor.

While the controls and related control objectives may be informed by the Service Organisation’s need to satisfy legal or regulatory requirements, our scope of work and our conclusions do not constitute assurance over compliance with those laws and regulations.

Our independence and quality control

In carrying out our work, we complied with the Institute of Chartered Accountants in England and Wales (ICAEW) Code of Ethics, which includes independence and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour, that are at least as demanding as the applicable provisions of the IESBA Code of Ethics. We also apply International Standard on Quality Control (UK) 1 and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

PricewaterhouseCoopers LLP, Central Square, 29 Wellington Street, Leeds, LS1 4DL T: +44 (0) 1132 894 000, F: +44 (0) 1132 894 460, www.pwc.co.uk PricewaterhouseCoopers LLP is a limited liability partnership registered in England with registered number OC303525. The registered office of PricewaterhouseCoopers LLP is 1 Embankment Place, London WC2N 6RH. PricewaterhouseCoopers LLP is authorised and regulated by the Financial Conduct Authority for designated investment business.

The Service Organisation's and the included Subservice Organisation's responsibilities

The Service Organisation and the included Subservice Organisation (where specified) are responsible for: preparing the description in Sections 5 and 6 and the accompanying management statements set out in Section 2, including the completeness, accuracy and method of presentation of the description and the management statements; providing the controls supporting the provision and maintenance of the ESR system covered by the description; specifying the criteria and stating them in the description; identifying the risks that threaten the achievement of the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

The control objectives stated in the description in Sections 5 and 6 are those specified by the Service Organisation. Management remains solely responsible for determining the suitability of the control objectives to address the needs of intended users.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in that description based on our procedures. We conducted our engagement in accordance with International Standards on Assurance Engagements 3000 (Revised) "Assurance engagements other than audits or reviews of historical financial information" issued by the International Auditing and Assurance Standards Board ('ISAE 3000 (Revised)". This standard and guidance requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description. An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description based on the criteria in management statements in Section 2;

- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;

- testing the operating effectiveness of those controls we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and

- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the Service Organisation and the included Subservice Organisation in their management statements in Section 2.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our qualified opinion.

Inherent limitations

The Service Organisation's and the included Subservice Organisation's description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the Service Organisation's ESR system, or the services provided to the Service Organisation by the included Subservice Organisation, that each individual user entity may consider important in its own particular environment. Also, because of their nature, controls at a service organisation or included subservice organisation may not prevent or detect and correct all errors or omissions in processing or reporting transactions. Our opinion is based on historical information and the projection to future periods of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls would be inappropriate.

Basis for qualified opinion

As stated in Service Organisation's Management Statement in Section 2 and as noted in Section 6 of this report, the controls necessary to ensure that access to the development and production areas of the NHS hub was controlled and appropriately restricted, were not in place from 1 April 2021 to 6 June 2021 but were implemented on 7 June 2021. As a result, there were insufficient logical access controls in place to appropriately restrict access to the development and production area of the NHS hub for part of the reporting period and therefore controls were not suitably designed to achieve Control Objective 2 “Controls provide reasonable assurance that security configurations are created, implemented and maintained to prevent inappropriate access” during the period 1 April 2021 to 6 June 2021.

Qualified opinion

Except for the effect of the matter described in the Basis for Qualified Opinion section above, in our opinion, in all material respects, except for the matter described in the ‘Basis for qualified opinion’ paragraph above, based on the criteria described in the Service Organisation’s and the included Subservice Organisation’s management statement in Section 2:

- the description in Sections 5 and 6 fairly presents the Service Organisation’s provision of the ESR system, and the IT and payslip printing services to the Service Organisation provided by the included Subservice Organisation to the Service Organisation, as designed and implemented throughout the period 1 April 2021 to 31 March 2022;

- the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period 1 April 2021 to 31 March 2022 and the user entities applied the complementary controls referred to in the scope paragraph of this assurance report; and

- the controls tested, which, together with the complementary user entity controls referred to in the scope paragraph of this assurance report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period 1 April 2021 to 31 March 2022.

Description of tests of controls

The specific controls tested and the nature, timing and results of those tests are detailed in Section 6.

Other information

The information included in Section 7 is presented by the Service Organisation and the included Subservice Organisation to provide additional information and is not part of the Service Organisation’s description of controls that may be relevant to user entities’ internal control as it relates to an audit of financial statements. Such information has not been subjected to the procedures applied in the examination of the description of the Service Organisation, related to the ESR system, and accordingly, we express no opinion on it.

Intended users and purpose

This report and the description of tests of controls and results thereof in Section 6 are intended solely for the use and benefit of the Board of Directors of the Service Organisation and solely for the purpose of reporting on the controls of the Service Organisation and the included Subservice Organisation, in accordance with the terms of our engagement letter dated July 2019 and varied on 17 December 2019 (the "agreement").

To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the Board of Directors of Service Organisation for our work, for this report or for the opinions we have formed, save where terms have been agreed in writing.

In the event that, pursuant to a request which you have received under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 (as the same may be amended or re-enacted from time to time) or any subordinate legislation made thereunder (collectively, the "Legislation"), you are required to disclose any information contained in this report, you will consult with us prior to disclosing such report. You agree to pay due regard to any representations which we may make in connection with such disclosure and to apply any relevant exemptions which may exist under the Legislation to such report. If, following consultation with us, you disclose this report or any part of it, you shall ensure that any disclaimer which we have included or may subsequently wish to include in the report is reproduced in full in any copies disclosed.

PricewaterhouseCoopers LLP

PricewaterhouseCoopers LLP
Chartered Accountants
Leeds
4 May 2022

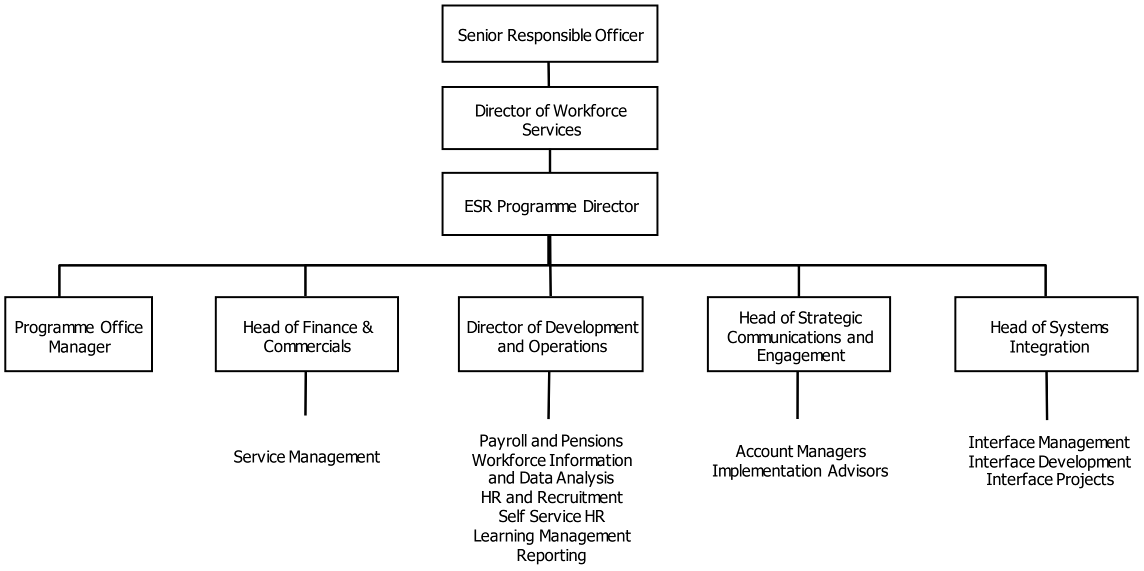
4. Overview of the ESR Programme

Programme structure / Internal control environment

NHS ESR Central Team:

Day to day delivery of the ESR programme is led by the NHS ESR Programme Director, reporting to the NHS Business Services Authority (NHS BSA) Director of Workforce Services and the Senior Responsible Owner (SRO) for the Programme (Director of Workforce, Acute Care and Workforce). The SRO sits within the Department of Health and Social Care (DHSC.)

The ESR Programme provides NHS organisations with a fully integrated HR and Payroll service. Day to day management of that service and the relationship with IBM as the sub service provider is the responsibility of the NHS ESR Central Team, who sits within the programme. Based in Sheffield this team are part of NHS Business Services Authority and are the main point of contact for NHS organisations. The organisational structure for the NHS ESR Central Team is as below:



IBM UK Ltd - Sub Service Providers

IBM is currently the primary contractor for the ESR Service. As it provides the Programme with day to day IT Operations, systems support and development for the ESR Service, it is responsible for the operation of the majority of the IT general controls that have been considered to be in scope (refer to Section 1). IBM employs approximately 175 employees to work on the ESR Programme in the UK.

NHS Systems Integration Team

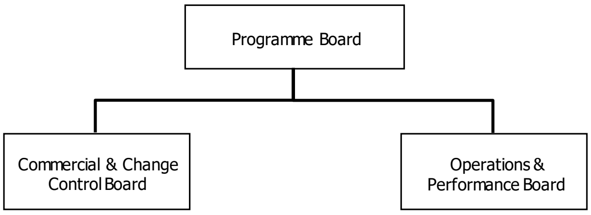
The ESR Oracle Human Resource Management System (HRMS) maintains one central chart of accounts for the whole ESR application. As individual NHS Organisations use different General Ledger (GL) applications, there is a requirement to reformat the GL interface files produced by ESR into a format that can be imported into each NHS Organisation's GL application. The NHS Systems Integration Team is part of the NHS ESR Central Team, and provides an additional service to NHS Organisations, enabling them to receive reformatted GL interface files. The NHS General Ledger Interface is managed by the NHS Systems Integration Team, and the IT general control environment for the Interface is shared between the NHS Systems Integration Team and the Sub Service Provider Technical Teams.

Responsibilities in relation to the IT General control environment for the ESR Service (application, operating system, database, network, and GL Interface) are as below:

Control objective ref:	Control objective	Responsibility in relation to ESR application, operating system, databases, and network	Responsibility in relation to NHS General Ledger Interface
1	Change Management	IBM	NHS Systems Integration Team and IBM
2	Logical Security	IBM	NHS Systems Integration Team
3	Problem Management and Performance and Capacity Planning	IBM	IBM
4	Physical Security and Environmental Controls	IBM	IBM
5	Computer Operations	IBM	NHS Systems Integration Team and IBM
6	Payslip Distribution	IBM	N/A

Programme Reporting Structure:

A formal monthly reporting structure is in place for managing the programme and escalation of issues. This is as below:


Programme Board
Commercial & Change Control Board
Operations & Performance Board

Key responsibilities of the Programme Board have been described below.

ESR Programme Board

An ESR Programme Board is in place which is responsible for managing the overall programme. Programme Board members are senior management representatives from the Sub Service Provider, the NHS ESR Central Team and NHS Wales Shared Service Partnership representatives. The Board's responsibilities are as follows:

a) provide senior level guidance, leadership and strategy for the overall delivery of the Services;
b) be the point of escalation from the Operations and Performance Board; and
c) carry out the specific obligations attributed to it in the responsibilities section below:
   - ensure that this Agreement is operated throughout the Term in a manner which optimises the value for money and operational benefit derived by the Authority and the commercial benefit derived by the Supplier;
   - receive and review reports from the Operations and Performance Board and review reports on technology, service and other developments that offer potential for improving the benefit that either Party is receiving, in particular value for money;
   - determine business strategy and provide guidance on policy matters which may impact on the implementation of the Services or on any Optional Services;
   - authorise the commissioning and initiation of, and assess opportunities for, Optional Services;
   - provide guidance and authorisation to the Change Control Board on relevant changes;
   - provide guidance and oversight for the delivery of benefits; and
   - provide guidance and oversight for the delivery of architecture.

Internal control environment

Management's philosophy and operating style

From the outset, the ESR Programme's strategic objective has been to ensure that ESR is regarded as the master workforce and learning management system for the NHS, and the central source of workforce information.

At the heart of the ESR Programme are three core values;

- Empower Staff and Managers to own and manage their data to improve workforce management and the experience of working in the NHS;

- Ensure NHS service users have safer, more effective care from staff who are well trained and managed, appropriately registered and whose skills and talents are developed and used; and

- Provide the public with improved value for money, resulting from transparent and evidence based strategic workforce planning and more efficient and accountable use of public funds.

Managing risks

The ESR Programme is aware of the importance of risk management. ESR Programme team leaders are responsible for managing their own risks and issues, and the Programme Board is responsible for programme level risks and issues. The relevant meeting will allocate an owner for each risk and issue and who is responsible for its resolution. Both Issue and Risk Management are addressed in four phases:

- Assessment and analysis of the risk/issue;

- Planning to manage the identified risk/issue;

- Implementation of the plans; and

- Monitoring and controlling the effectiveness of planned activities, whilst it still puts the affected parties at risk, or until the issue has been resolved.

The risk/issue owner monitors progress and reports changes in status, impact or likelihood to the Project Manager/Project Board. The ESR Programme Board meets on a monthly basis and monitors progress and helps ensure that the ESR Programme continues to achieve the milestones. Furthermore, the ESR Operations and Performance Board meets monthly to discuss operational activities relating to the ESR programme. Results from these meetings feed into the monthly Programme Board meetings.

Monitoring of service delivery

A Service Level Agreement (SLA) is in place between the NHS Business Services Authority and the Sub Service Provider, representing all NHS Organisations using the Service. Monitoring occurs at two levels:

- Service Delivery; and

- Monthly Service Review.

Every month the NHS ESR Central Team and the Sub Service Provider review the level of service that has been provided to NHS organisations in relation to the areas in-scope for this report. At the end of every month, the Sub Service Provider is required to deliver a monthly service report that details the level of services provided, achievement of the Performance Indicators (PIs) and areas that have not performed to target or threshold are reported on an exception basis. During the review process, the level of service credits required will also be agreed in accordance with the regime stated in the contract. For further details of service delivery please refer to section 6 of this report.

In addition to the above, the Operations and Performance Board reviews exceptions and steps taken to identify the root cause of the problems and remedial steps are taken to help ensure that there is no repeat failure. If there are repeated failures, these will be escalated to the Monthly Service Review.

Information and Communications

As a high-profile national NHS initiative, the ESR Programme has a wide variety of interested stakeholders. Communication channels range from updating the internal NHS ESR Central Team, to engaging senior stakeholders within the DHSC and Welsh Assembly Government (WAG) and NHS Organisations including NHS England and the Local Education and Training Boards. The NHS ESR Central Team is engaged with NHS Organisations through Special Interest Groups (SIGs).

An online magazine (ESR News) also provides an update on programme progress and information about current issues and matters of interest, and is issued on an approximately monthly basis. It is widely distributed and is a major source of up to date information about ESR for the NHS and the wider public. In addition, the ESR programme runs a Twitter account, designed to help the team reach a wider audience than the traditional professional users. The ESR Hub (my.esr.nhs.uk) provides both authenticated and non-authenticated information including the latest news about the ongoing development of ESR and ESR best practice, access to functionality guidance and documentation, and other service related information.

The ESR programme seeks to get ESR on the agenda at key NHS conferences and events as best as possible, as these are attended by key NHS stakeholders. Publicity materials such as brochures and promotional video films are made available via the ESR Hub and other electronic media channels. NHS ESR Functional Account Managers also continue to provide local support to NHS organisations.

Sub Service Provider internal control environment

Organisational structure:

Day to day management of the ESR service is delivered via IBM and NHS ESR ACT. The roles and responsibilities of the sub service organisation and NHS ESR ACT are substantially similar and have been outlined below:

- SLA Management – Performance monitoring against agreed service levels;
- Programme Office – Project and programme management, quality, and finance;
- Customer Relations – Manages effective communication between ESR and Trusts;
- Service Delivery – Application support, customer relations, SLA management, and education;
- Development – Developing changes to the ESR service further to requests from NHS Trusts;
- Testing – Ensuring that the developed changes operate correctly before these are promoted to the live environment;
- Technical Solutions – Providing support for the underlying operating system and database;
- Infrastructure and Security – Ensuring that the network that ESR is hosted on is stable and secure;
- Operational Services – Risk and Compliance; Production Services and Systems Analysis;
- Operations Service – Change & release management; and Incident & problem management; and
- Data Centre Operations – For both Warwick and Newcastle (disaster recovery site).

In the course of normal duties, sub service provider personnel do not authorise, initiate or modify customer transactions (i.e. they do not have access to make changes to NHS organisations data that resides within ESR). Segregation of duties exists between product development, operations, database development and technical support is in place.

Overall governance of IBM is provided by the Internal Programme Review. The Review is currently held on a weekly basis. This review incorporates all aspects of governance and compliance and reviews incidents, considers customer feedback, and reviews internal audit reports and other performance metrics.

External Payslip printing

Production of payslips is delivered via IBM’s sub-contractor OPUS Trust Communications (OPUS). IBM remains fully accountable for payslip production and delivery to NHS Organisations using ESR. OPUS is carved out for this report and its controls are not in scope for testing. IBM monitors the performance of OPUS.

Commitment to competence

Both sub service providers align to a number of key industry standards which demonstrate their ongoing commitment to maintaining a high level of competence. These include:

- ISO 9001 - The standard defines the requirements needed for an organisation to properly implement an effective quality management system; and

- ISO 27001 - The standard defines the requirements needed for an organisation to properly implement an effective Information Security Management Systems.

IBM do not currently hold certification in ISO 9001 to cover the specific ESR sites as it is not part of their contractual obligations. However, the processes and procedures operated by IBM are consistent with ISO which is unchanged from the previous provider. The ESR sites are ISO 27001:2013 accredited, with accreditation being awarded by Bureau Veritas as of 10 November 2018. IBM does have a global ISO 9001 certificate covering the Global Business Services unit.

- ITIL - the Sub Service Provider applies ITIL (Information Technology Infrastructure Library) principles within its IT Service Management functions. In addition, a number of staff have obtained the formal ITIL certification.

Sub Service Provider Internal audit and risk procedures

IBM has a comprehensive Internal Audit programme in place which includes a number of reviews each year covering ESR related functions, in addition to more general reviews which indirectly involve the ESR service. The overall audit programme is agreed by the Internal Programme Review, to which the results of reviews are also reported. Audits are individually scoped with due consideration of the relevant risks for that area, and signed off by an appropriately senior audit sponsor. Any actions arising are subsequently monitored by the Internal Programme Review.

To assist in the effective management of risks and issues related to the ESR Programme, a formal Risk and Issue Management Procedure is in place which outlines the overall process. IBM maintain a Risk and Issue log which ensures the recording of risks and issues are recorded correctly. There are five main stages:

- Identification - recognition of the risk or issue;

- Assessment - analysis of the risk or issue;

- Action Planning - planning, resourcing and performing activities to manage the risk or issue;

- Monitoring and Control - examining effectiveness of planned activities; and

- Closure - resolving and closing the risk or issue.

Individual risks and issues are managed at program or project depending on the potential impact and the level of management involvement required to resolve them. Each risk and issue has an assigned owner to ensure that there is clear responsibility for action. Risks are assessed by their severity and probability to define their priority. Issues are assessed according to the severity of the issue and priority of the impact. Risks are rated based on a score arrived at by multiplying impact by likelihood, as follows:

Very High	20 – 25	Critical disruption impacting costs, schedule and/or quality.
High	15 – 16	Significant disruption impacting costs, schedule and/or quality.
Medium	8 – 12	Impacts one or more areas within the programme (for example multiple work Enhance work packages or Transition work streams).
Low	1 – 6	Causing delays or additional work that requires additional funding.
Very Low	1 – 6	Minor impact to a single area of the programme.

Sub Service Provider human resources policies and practices

Recruitment is centrally managed by the IBM Global Business Services (GBS) team. All positions are required to have formal job descriptions in place outlining roles and responsibilities and the required skills, experience and knowledge. Since the transition to IBM as of 31 May 2015, candidates are typically drawn from the wider IBM organisation, which has a large pool of resource, they are then ranked accordingly to ensure the most appropriate individual is selected.

All Sub Service Provider employees are required to sign that they have read and understand IBM Cyber Codes of Conduct, Codes of Business Conduct and Ethics, Data Confidentiality Code of Conduct, Health and Safety Policies and Security Policies. Sub Service Provider employees are required to complete annual mandatory refresher training in codes of business conduct and Cyber Security. These form a basis of the contract of employment and controlled through normal disciplinary processes.

All staff have a defined job description which covers their role, responsibilities and expected behaviours. Both Sub Service Providers have an annual performance appraisal process to ensure that staff are working to the expected level against their objectives for the year and that any development needs are identified and remedial action takes place.

IBM employees effectively have two line managers, one responsible for all HR and career management (including the appraisal process) and another for Task management. Both of these managers will jointly evaluate employee job performance. This usually includes an element of client and colleague feedback. Performance appraisals are conducted annually using IBMs ‘Checkpoint’ process which is located on the corporate intranet. The appraisal process provides managers with a consistent set of rating definitions and scales for setting expectations and evaluation. Objective setting provides the overall goals agreed for an individual reflecting the requirements of a business unit, team and project level. Performance reviews may be conducted on a more frequent schedule if the situation warrants.

Training for employees is on a needs basis. Line managers are responsible for ensuring that the staff under their supervision are appropriately trained. The majority of training is via on-the-job learning which is complemented by e-Learning courses and formal technical training provided by external trainers.

Systems environment

The ESR application, operating system, databases and network are maintained by IBM at Globe House in Warwick. The NHS General Ledger Interface is maintained by the Interface Team who are NHS employees and are part of the NHS ESR Central Team. The physical infrastructure for the ESR Service, including the General Ledger Interface reside at the IBM data centre in Warwick and responsibility for their management and security lies with IBM.

A description of the IT General Control environment for the ESR Service is provided in section six of this report. A high-level overview of the General Ledger Interface is provided below:

Web Service

NHS organisation users access the NHS Hub using the ‘Web Service’ facility through a web based front-end system available on the NHS intranet via the NHS HSCN Network (was previously N3). The web based front-end system accesses the NHS Hub on the ESR network via a separate zone (zone 2, as per the diagram on the previous page) through the firewall managed by IBM. NHS organisation users are assigned a single user ID and password which they use to log onto the NHS Hub using Web Service. NHS organisation users are able to perform the following actions using their Web Service account:

- ***Ability to create and maintain local user accounts for access to the NHS Hub Web Service;***

- ***Download Target files*** - users are able to download target files to perform checks on their files to identify potential problems; and

- ***Update mapping tables -*** NHS organisation users are able to examine and manipulate the mapping tables to meet their specific NHS organisation requirements (such as expenditure grouping or creating period weeks). They are also able to re-process Source files to reproduce differently mapped (but identically formatted) Target files. This functionality allows NHS Organisations to manage their account code mapping. Once satisfied with the format and content of the Target file, they are able to release the file for collection by the IBM Hub.

Upon making changes to the mapping tables on the NHS Hub, it is the responsibility of the NHS organisation users to test and ensure that the account mapping on the NHS Hub is accurately set up.

Accessing ESR (local NHS users)

ESR Service users at each NHS Organisation (excluding NHS Organisations in Wales) predominantly log onto ESR using Smartcards. Those users who do require a smartcard are those which are accessing ESR only for eLearning and Employee Self Service. NHS Organisations in Wales are not connected to the NHS Care Records Service (CRS) and as a result continue to use the traditional username and password to login to ESR. The IBM Application Support Team creates two Administrator accounts for each local NHS organisation when they are first set up on ESR. Responsibility for assigning access to other local users then lies with each local NHS organisation administrator.

NHS Organisations are required to ensure that user accounts created within their NHS Organisation's database schema are controlled appropriately. The use of each User Responsibility Profile (URP) is defined in the set-up documentation for ESR; however, allocation of the URPs is a local decision. Local NHS Organisations should ensure that appropriate segregation of duties are maintained. It is the responsibility of NHS Organisations to distribute Smartcards to new local ESR users and to install Smartcard readers and NHS authentication software on local users' PCs. Users' are allocated a unique user identifier (UUID) when they have been assigned a Smartcard. This is associated to the user's ESR user account

NHS Organisation users are restricted from accessing the data belonging to other NHS Organisation's data. This restriction is achieved by setting up each NHS Organisation with a Virtual Private Database (VPD). This is enabled using Oracle Row Level Security which is a functionality component of Oracle. In instances where an NHS Organisation does not have its own payroll function, the NHS Organisation is able to delegate authority for payroll processing to another NHS Organisation or a shared service centre. In these instances, the organisation which is processing payrolls for other NHS Organisations would have an ESR account set up on each VPD to which they require access to. For Smartcard Enabled Access to ESR in England, users with access to multiple VPDs are presented with a screen listing the VPDs to which they have access. The user is then required to select the ESR VPD they wish to use.

The responsibility for setting up and allocating Smartcards and the authentication of the Smartcard user against the NHS CRS resides with the local NHS Organisations and their Registration Authority function. Consequently, these controls are not within the scope of this audit.

Logging in procedure for Smartcard users (local NHS users)

The user must first insert their Smartcard into the physical reader and then enter their Smartcard PIN. The Smartcard and PIN are then authenticated by the NHS Identity Agent software against the NHS CRS which is hosted on the NHS Spine (the set of national databases and connectivity that provides key information for patient's health and care to all NHS organisations). Once the user has been successfully authenticated on the NHS CRS, the user enters the ESR URL to access ESR. Users' are allocated a unique user identifier (UUID) when they have been assigned a Smartcard. This is associated to the user's ESR user account.

The user's UUID is passed back by the NHS CRS to ESR to validate whether the UUID exists within the ESR user record. If it does, it confirms that the user has an existing ESR account linked to that Smartcard. Upon successful authentication by ESR, the following will occur:

- If the user has only one existing ESR User account, the user is logged directly into ESR for that Virtual Private Database (VPD) that holds their organisation's data, which they have access to. They are then presented with the main ESR Application menu; or

- In the case where a user has access to more than one VPD (i.e. shared services providers), the user will be presented with a screen listing all their active ESR accounts per VPD. The user is then able to select the VPD that they would like to access.

A user is logged out of ESR in one of the following ways:

- The user selects to logout of ESR;

- The Smartcard is removed from the card reader. In order to re-connect to ESR the user is required to follow the login process described above;

- The user is automatically logged out of ESR after a period of inactivity. The user will be given the option to log back into ESR (assuming the NHS CRS session has not expired). If this is declined the user is required to follow the login process described above; or

- A user closes the Smartcard 'logout monitor'. In order to re-connect to ESR the user is required to follow the login process described above.

Complimentary End User Controls

The ESR Programme was designed with the assumption in mind that certain application and entity level controls would be implemented by NHS organisations. The application of which are necessary to achieve some of the control objectives included in this report. This section describes the internal controls that should be in operation at NHS organisations to complement the internal controls operated by the ESR Programme. NHS Organisations' auditors should consider whether the following internal controls are present and operating effectively.

There may also be additional control objectives and related controls that would be appropriate to the processing of NHS organisations' transactions that are not identified in this report. Therefore, NHS organisations should not regard the controls listed below as a full and comprehensive list of controls that should be employed:

General controls:

- NHS Organisations should ensure appropriate segregation of duties exists within their organisation in relation to the levels and types of access granted within ESR. User Responsibility Profiles (URPs) should be allocated in line with a full Internal Audit Process, in order to minimise any risk of fraud or security; and

- NHS organisations are responsible for implementing procedures and controls within their organisations to ensure that the account code mapping and set up on the NHS GL Interface are accurate, and reconciled on a routine basis.

- NHS organisation users have a responsibility to reconcile ESR payroll run totals produced by the ESR Application, to the totals imported into the individual NHS organisation's GL system, with the aim to confirm the 'end to end' accuracy and completeness of the payroll data. This is an overarching control which is the responsibility of individual NHS organisations.

Logical Security:

NHS organisations should:

- Establish procedures and documentation authorising user access to the ESR Service. Periodic access reviews of users' access rights should be undertaken to ensure that access remains commensurate with user's job roles;

- Establish policies and procedures for the creation, modification and revocation of users; access rights. Local administrators should be aware of users' job roles and whether access is appropriate in line with these;

- Establish appropriate policies and procedures for Smart Card administration for local users. This should include appropriate policies for acceptable use;

- Ensure that the User's Unique ID number (UUID) assigned to each ESR user account is accurate;

- Establish policies and procedures for ensuring that good practice in relation to password security is maintained. This should include prohibiting the use of shared usernames and passwords, and educating users on their information security related responsibilities;

- Implement a procedure to ensure that ESR Service configurations are set at an appropriate level to provide adequate security; and

- Establish suitable access controls around access to their Web Service account which provides them with access to the NHS Hub and GL mapping tables. This includes removal of access for leavers in a timely manner, and restricting access to an appropriate number of users as required.

Computer Operations:

- NHS Organisations should be aware that there are no scheduled jobs that are performed by the ESR Programme teams to produce weekly and monthly payslips. When an organisation requires payslips to be produced for its employees, a job must be submitted by an appropriate payroll user within that NHS organisation on a timely basis. Additionally, it is the responsibility of the NHS organisation to ensure the completeness of their payslips once a job is submitted;

- It is the responsibility of the NHS organisations to implement internal procedures and controls to help ensure that payroll related processes are run in the correct order and in accordance with the schedules provided by the ESR programme each year. Reconciliation of the ESR Payroll run totals produced by the ESR application, to the totals imported into the individual NHS organisation GL systems should form part of these procedures;

- NHS organisations should raise a service request or contact the ESR Service Desk to report operational or performance related issues with the ESR Service experienced by their own organisation; and

- NHS organisations are responsible for initiating the process to create source files in ESR to be sent to the GL Interface for processing on the NHS Hub. They should log any problems and incidents in relation to the processing of files for the GL Interface (e.g. timeliness of processing).

This includes monitoring the target files expected to be received. Any issues should be logged with the ESR Service Desk for escalation and further investigation.

5. Description of services provided by the ESR Programme

Control Objective 1: Change Management

Controls provide reasonable assurance that changes to the system software, hardware, and network components are documented and approved.

1.0 Introduction

Changes may be required to the ESR System and the NHS GL Interface during the year and these can affect software, hardware and other network components. The change management process followed in the event of change requests differs depending on the nature and scope of the requirement. The ESR Change Management Team is accountable for establishing and maintaining application change policies and procedures for the ESR Service. This helps to ensure that standardised methods and procedures are used for initiating, assessing, approving, implementing and reviewing changes to the IT environment, as described in EE25017 Service Change Management.

The main policies and procedures regarding change control are:

- ESR-NHS0018 – NHS Systems Integration Team Change Control Process;
- EE-25017 Change Management Process; and
- EE-25454 – ESR Agile Change Process

Changes are categorised into three types: (1) application changes, (2) system software and hardware changes, and (3) network changes.

1.1 NHS GL Interface application changes

Background

Changes may be required to the NHS General Ledger Interface during the year, and it is likely that these will relate to either one of two software elements: the GL Build Perl Scripts, or the supporting Perl Scripts. Both of which are described below:

GL Build - a GL Build is the discrete set of Perl Scripts and associated configuration and lookup files used by the NHS Systems Integration Team to manipulate data formats received from ESR into a format usable by an NHS organisation’s local GL systems. The GL Build transforms ESR files into exportable GL files which meet the agreed requirements of the NHS Organisation.

Supporting Perl Scripts - are run to perform a variety of common basic pre-check routines on each file received from ESR, including identifying which NHS Organisation the files belong to. Based on this, the supporting Perl script calls a corresponding GL Build to be used for the mapping activity.

The NHS Systems Integration Team Manager is accountable for establishing and maintaining policies and procedures in relation application change for the GL Interface. The ESR-NHS0018 – NHS Systems Integration Team Change Control Process is reviewed on an annual basis and updated as appropriate on an on-going basis.

Change management process

The NHS Systems Integration Team has processes in place for initiating, designing, building, testing, approving and implementing NHS General Ledger Interface application changes. These have been documented below:

Change initiation

Change requests for the NHS General Ledger Interface application are managed by the NHS Systems Integration Team and can be initiated by members of the NHS Systems Integration Team; or users of the ESR Service within NHS organisations.

Service Requests (SRs) are raised via the on-line ESR Customer Portal website, or by calling the ESR Service Desk. Requestors are required to assign an initial priority rating to their SR, which is then assessed by both the ESR Service Desk and the NHS Systems Integration Team and may be adjusted accordingly.

Where changes are required by the NHS Systems Integration Team, such as fixes, an Amendment Request (AR) must be raised. If this involves a change to an already agreed client specification for a change, the NHS organisation to which it relates to must raise a corresponding SR to cover the necessary change. Where a corresponding SR exists, this is linked to the AR.

All SRs are reviewed by the NHS Systems Integration Team for appropriateness and clarity, and to perform initial diagnosis and validation checks. If the SR relates to an application enhancement, the NHS Systems Integration Team is responsible for routing the SR to the appropriate team member for additional validation.

Change design and build

All AR and SR change requests must be approved by the change requestor and validated by the NHS Systems Integration Team. No change will be made until an approved and validated AR and SR is received by the NHS Interface Development Team.

Developers obtain a copy of the production files and import these onto their individual desktop computers for development, using specified version numbers as agreed with the Development Controller.

Production GL Build and Supporting Perl script files are version controlled and each new release has a unique, consecutive version number. It is the responsibility of the Development Controller (who is a member of the NHS Systems Integration Team) to manage the version history.

Once a developer is satisfied that the change meets the requirement specified in the SR and AR, the developer uploads the change onto the NHS Hub development environment for testing. The development environment is a replica of the NHS Hub production environment.

Change Testing

Once a change has been uploaded onto the NHS Hub development environment, the developer sets up the development environment with the new code and data from the production source so that the developers can test and synchronise the new files in the development environment.

When the developer is satisfied with the results of their testing, they sign off the AR and inform the NHS Organisation change requestor. The requestor then performs user acceptance testing in the development environment by logging onto the NHS Development Hub using their development Web Service account. Once satisfied with the change, the change requestor provides signoff on the SR.

After testing is completed successfully, the developer assigns the change to the NHS Interface Production Control Team who are responsible for promoting the new file versions onto the NHS Production Hub.

Approval to move to production

On satisfactory completion of testing, approval to promote the change to the production environment is provided by the NHS Organisation change requestor via the SR. In addition, approval is provided by one of the three NHS Production Controllers who are responsible for promoting the change into the production environment.

When a change is initiated by the NHS Systems Integration Team, the approval to release the change to the production environment is provided by one of the three NHS Production Controllers only.

A Handover document is required to be completed by the NHS Interface Development Team before a change can be promoted into the production environment. This document is used to formalise the handover process from the NHS Interface Development Team to the NHS Production Control Team. The Handover document is used by the NHS Production Controllers to confirm that all required authorisations, change documentation, and ‘secondary items’ (e.g. site specific settings or lookup tables) that may be required to make the change, are present before a change is promoted to production.

Implementation process for releasing change into production

The implementation of changes into the production environment differs depending on the type of change and whether it relates to GL Build or supporting Perl scripts, as below:

GL Build Changes

When releasing GL Build changes into the production environment, the NHS Production Controller runs a ‘Proclive’ script, (a Perl script used to release changes into the production environment). The Proclive script promotes changes by copying the changed GL build/version and associated lookup tables for the specified NHS Organisation’s site from the NHS development Hub to the production Hub. The Proclive script helps to ensure that the relevant permissions required for running the code in the production environment are set. It also ensures that the NHS Organisation sites have access to the new build version after the change has been made.

A Proclive job log is available which produces system messages to warn the NHS Production Controller of any problems being encountered when releasing the change to production. These problems are investigated by the NHS Production Controller to help ensure that changes are successfully implemented. The Proclive log is available once the change has been implemented and contains change details and indicates whether the change has been successfully implemented.

Only members of the NHS Production Control Team have access to the Proclive script for the purpose of promoting changes to production.

Supporting Perl Script Changes

Supporting Perl script changes, and changes made to secondary items are not implemented to the production environment using the Proclive script. These changes are manually promoted by the NHS Production Controllers by copying the code from the development Hub to the relevant directory on the production Hub. Only the NHS Production Control Team has access to promote these changes to the production NHS Hub.

Implementation Documentation

The Production Controller implementing the change into the production environment completes a Handover Summary Log which requires the following information:

- GL Build name (or supporting Perl script name);
- Version number;
- Amendment change request number;
- SR number;
- Name of the NHS Production Control Team member promoting the change to production;
- Change description; and
- Change date.

The Summary Log is created and documented by running a Handover Check (Perl script) which automates the task of ensuring that the required documentation is correctly completed and cross-referenced with appropriate sign-offs:

Monthly Change Reconciliations

Each month the NHS Systems Integration Team Manager performs a reconciliation of changes that have been promoted to the NHS Hub Production environment with their corresponding SRs, Amendment Requests and Handover Requests. This is undertaken in order to reduce the risk of unauthorised changes being promoted to the production environment. Evidence of the review is maintained in a reconciliation log which the NHS Systems Integration Team Manager signs off.

1.2 ESR Service application changes

Application changes for the NHS General Ledger Interface are unique in nature and have been documented under section 1.1 above. The following section relates to the ESR Service only.

The ESR Change Management Team has processes in place for initiating, designing, building, testing, approving and implementing ESR application changes. The overall change management process is described below.

Change initiation

Requests for application changes (typically ‘enhancements’ or ‘fixes’) vary depending on the scope of the change required and can arise from any of the sources listed below:

- NHS and IBM Teams engaged on the ESR Programme;
- Live users of the ESR Service (NHS organisations);
- NHS User Groups (NHS ESR Central Team); and
- Oracle for database and statutory updates.

<u>ESR application enhancement changes</u>

Requests for enhancement to the ESR Application are raised through ESR Service Desk by creating a Service Request (SR). The SR can be submitted by users logging directly into the Customer Portal website or by calling the ESR Service Desk. Requestors put an initial priority on the SR which will usually be assessed by the ESR Support Team and may be adjusted accordingly.

The SRs are also reviewed by the ESR Support Team for appropriateness and clarity. They conduct an initial diagnosis and validation checks. If the SR highlights an application enhancement, the ESR Support Team is responsible for routing the SR to the IBM Design Team to confirm it is valid. If the request is valid, it is routed to the NHS Development Team to add the analysis results to the SR. The IBM teams must elaborate fully why the request is an enhancement stating clearly which project deliverables they have referenced.

Following review by the NHS Development Team, the change enhancement requirements will be assessed through a cost benefit process. This process is documented in procedure NHS0132 and involves:

- Special Interest Groups (SIGs) supporting the request and providing full business justifications including benefits;
- Discussion of the locally supported requests at the National SIGs;
- CCN costed Change Requests are sent to NSIG Chairs for a national support and prioritisation;
- Top SIG priorities are assessed against available development resource profile;
- Change Request (CR) for design team requirements;
- A formal CCN is created for detailed costing, and is contractually binding; and
- Review and approval of costing by the NHS Commercial Board.

<u>ESR application fixes</u>

The ESR Support Team will also identify requests for fixes in the same way as those for application enhancements. A SR is raised and reviewed by the ESR Support Team and the SR is routed to the relevant team which will try to replicate the issue that the customer has. Proposed changes will be assessed and scoped by the ESR Development – Solution Design Team (the ‘ESR Design Team’) or the ESR Application Support Team and queued accordingly.

Change design and build

When the SR is validated and requirements defined for an application enhancement or fix, a Change Request (CR) document will be raised by the ESR Application Support Team or ESR Design Team. The CR document is linked to the SR in ESR Service Desk, but remains an internal document for ESR Programme use only. The ESR Application Support Team or the ESR Design Team are not required to raise a CR for minor support type changes related to data fixes. These are coordinated directly with the ESR end users to validate the change requirements.

The following information is required to be completed as part of the CR:

- High level functional specification;
- Impact assessment;
- Estimated man days to build, test and implement;
- Target date (this date is agreed with the ESR Release Manager); and

- SR number.

After the impact assessment and high-level functional specification are complete, the CR is routed to the team that will be responsible for the development of the application change.

CR and SRs are discussed and approved by the CR Change Advisory Board (CAB) which included business and technical representation. Approved changes are placed in the CR Target queue and assigned a release number and target date. Development of a change begins according to the dates in the Release Plan; at this point the CR is placed in the developer queue. Change development is performed by the ESR Development – Technical Development Team. Specifications for each enhancement are developed, along with a suitable testing strategy.

Developers code changes in the development environment. Kintana provides a repository for source code and defines a workflow showing the progression of a change through the application change procedure. Developers check out the source code from the production environment into the development environment using Kintana.

The developer will perform testing in multiple testing environments to help ensure that the changes satisfy the requirement specified in the CR.

Change Testing

When the developer is satisfied with the result of the testing for application changes, the change will be assigned to the ESR Testing Team. The ESR Testing Team is experienced in various areas of the application and related processes. The assigned ESR Programme Tester tests the change to help ensure the change works in accordance with user requirements and it does not have an impact on other areas of the application. This simulation testing is the in-house project User Acceptance Testing (UAT) phase. The test results are recorded in the SR and 'Request For Change' (RFC) document.

End users are requested (where relevant) to perform testing on changes in a testing environment. Once the testing is completed, they confirm their satisfaction with the change within the SR prior to the change being released into production.

After testing is completed successfully, the ESR Database Analysts prepare the Kintana release package together with a Technical Release Note (TRN) developed by the Release Team which provides details of dependencies (such as Kintana package number and CR number) and the changes to be implemented as part of the package.

Approval to move to production

When application changes are ready to be implemented into the production environment, a member of the ESR Release Team creates a RFC document and has the RFC approved by the ESR Release Manager and the CAB, where applicable.

The process of raising an RFC for application change implementation into the production environment follows the same process as described for system software and hardware changes in section 1.3. RFCs for application changes reference the relevant SRs, CRs and Kintana packages. (Note that one RFC may cover more than one SR, CR or Kintana package depending on the nature of the change). A reference to the RFC number is included in the Technical Release Note (TRN).

Implementation

<u>Release management strategy</u>

The release management strategy is documented in EE-25455 Release Management Process and Procedures. This document is specific to the ESR Programme and is focused on the migration and release of application changes into the production environment.

There are several system environments involved in the configuration and deployment of changes. These can be categorised into three groups: (1) development environment, (2) test environment and (3) production environment. Code is promoted from the test environment to the production environment by the ESR Production DBA Support Team on the agreed date with the ESR Release Manager (as per the CR). The ESR Production DBA Support Team is part of the ESR Operations – Technical Infrastructure Team.

The ESR Production DBA Support Team will dry-run a release into a test environment to validate the TRN, Kintana release and associated processes to help ensure they function as planned without negative results. This test also provides timing information that is used to request the appropriate downtime.

Individual Kintana packages (incorporating system changes, patches and fixes) are implemented into production either immediately in the case of emergency changes (but more likely outside of core business hours), or are grouped with other changes to be implemented with the next planned release of the ESR Service.

Release numbering mechanism

Oracle patches, database packages, statutory packages and application changes are given a release number. The release number is categorised as follows:

> ***Major Release (e.g., 2) -*** This type of change is usually performed quarterly and it often ties to the Oracle family pack release. Major releases will be scheduled into the ESR development plan several months in advance. The NHS ESR Central Team is provided with the copy of the development plan.
>
> ***Planned Release including agile (e.g., 2.1) -*** This type of change will incorporate a group of changes supported by a SR or CCN and includes an accelerated cycle to support an agile development approach for mainly non-Oracle eBS changes and deliver low risk presentation layer changes faster.
>
> ***Urgent Release (e.g., 2.1.1) -*** This type of change is usually performed on a weekly basis, in most cases occurring on Thursday evenings. Included in the urgent release, for example, is an installation of a patch that is sent by Oracle.
>
> ***Emergency Release (e.g., 2.1.1.1) -*** This type of change could be performed any day of the week if considered urgent to maintain the operation of the system.

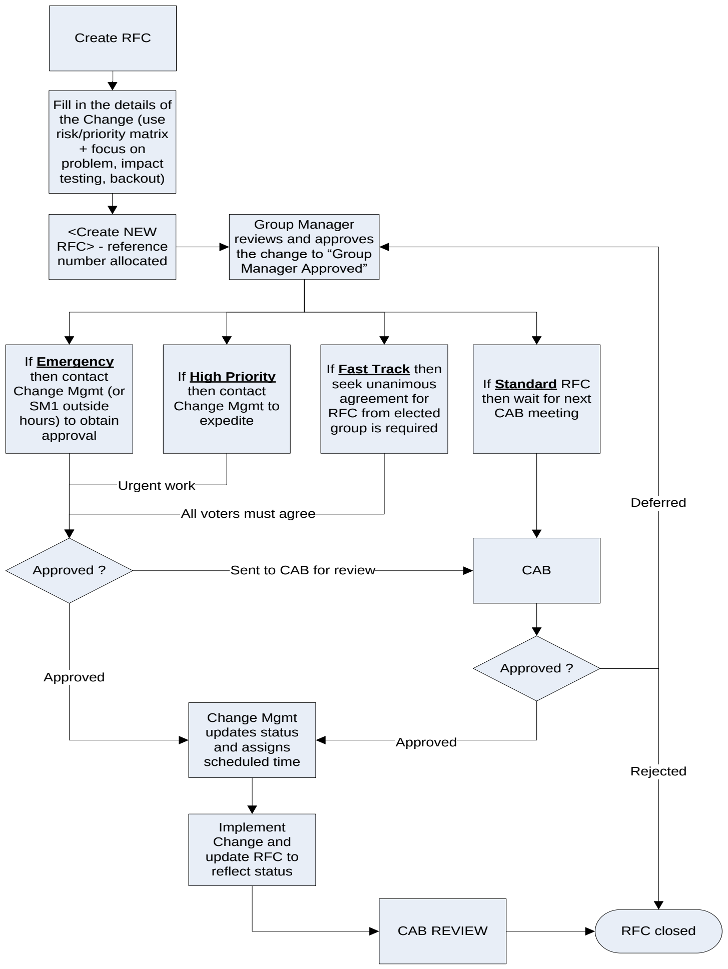
1.3 System software/hardware changes (applicable to the ESR Service and the NHS GL Interface)

The following control activities are common to both the ESR Service and NHS General Ledger Interface and will therefore be described once in this section.

An ESR Service Change Management process is in place which covers system hardware and software changes. It is designed to provide standard methods and procedures for prompt and efficient handling of changes, in order to minimise the negative impact of changes on IT service quality, and improve day-to-day IT operation. As system software and hardware changes are initiated by technical Teams working on the ESR service, the change management process is different to that typically followed for application changes.

System software and hardware changes follow the process set out in the ESR Service Change Management flowchart on the following page:

ESR Service Change Management flowchart:


Create RFC
Fill in the details of the Change (use risk/priority matrix + focus on problem, impact testing, backout)
<Create NEW RFC> - reference number allocated
Group Manager reviews and approves the change to "Group Manager Approved"
If Emergency then contact Change Mgmt (or SM1 outside hours) to obtain approval
If High Priority then contact Change Mgmt to expedite
If Fast Track then seek unanimous agreement for RFC from elected group is required
If Standard RFC then wait for next CAB meeting
Urgent work
All voters must agree
Deferred
Approved ?
Sent to CAB for review
CAB
Approved
Approved ?
Change Mgmt updates status and assigns scheduled time
Approved
Rejected
Implement Change and update RFC to reflect status
CAB REVIEW
RFC closed

Change initiation

An RFC is required for any proposed changes to the ESR system software and hardware which could affect the availability and integrity of IT services provided to NHS Organisations. Requests can be raised by any team member within the group where the actual work lies.

The Change Requestor must initiate the change request by creating an RFC through the bespoke Technical Service Database system (the 'Technical Portal'). They must provide a summary description of the change along with business justification, an initial assessment of the impact the change is likely to have on the ESR Service, a priority rating for the change, and the anticipated time required to complete the change which includes an allowance for contingency and back out. The requestor must also specify the potential impact should the change not be implemented.

The priority rating assigned to the RFCs by the Change Requestor is one of the following:

- Emergency – This is assigned when loss of service or severe usability problems to a large number of users or a mission critical system is expected. Immediate action is required;

- High – This is assigned when a severe effect is expected on some users, or when a large number of users is expected to be impacted;

- Medium – This priority rating is assigned to planned change that is project linked and/or date driven (required to meet a scheduled activity). No severe impact, but is required by a given date; or

- Low – Planned change with no or minimal date/time constraints.

Obtaining approval for initiated changes

After the RFC is created and prioritised, the Change Requestor is required to obtain approval from the Group or Team Manager and the Change Advisory Board (CAB), unless the change is on the Pre-Approved List (PAL) or is classified as Low; whereby the Change Manager acts on behalf of the CAB (this is to prevent excess RfCs being presented at the CAB and the meeting becoming unwieldy and inefficient).

Pre-Approved List (PAL)

From time to time, the CAB will consider some requests as being of low relevance/routine and as such deems the request as being suitable for the pre-approved list (PAL). All changes on the PAL are approved by the CAB and PAL changes are reviewed atleast annually by the CAB. Changes covered by an entry on the PAL are allowed to be implemented without Group or Team Manager or CAB approval. However, an RFC is still required, the completion of which reflects the PAL status of the change.

Each item in the PAL will include:

- ID Number (PAL ID Number) which must be quoted on the RFC;

- Description of the task;

- Where possible, a knowledge base article on how to complete the task;

- Scope, including restriction;

- Test criteria; and

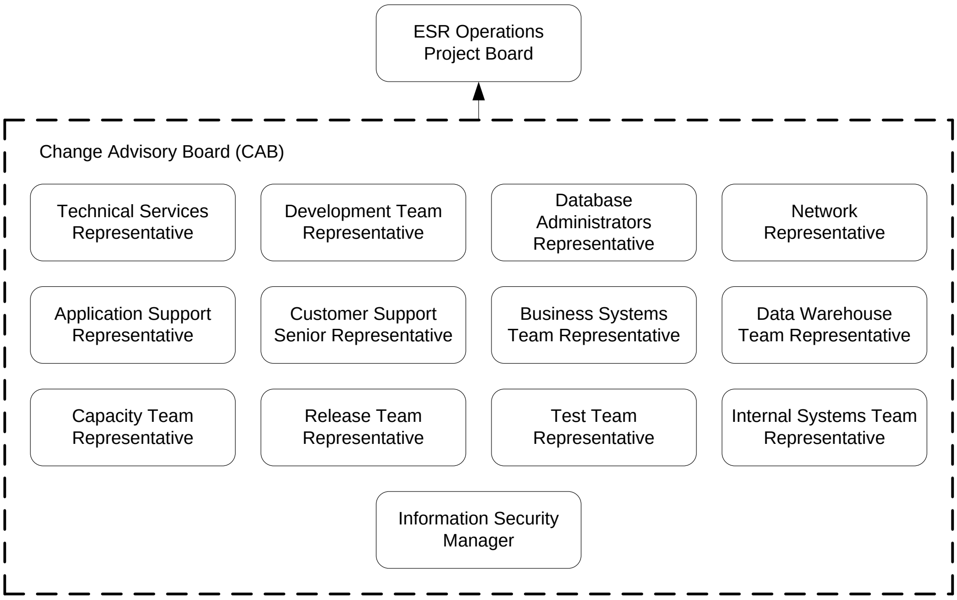
- Special consideration.

Group or Team Manager approval

Upon creation of an RFC, an e-mail is generated and sent to the Group or Team Manager to prompt them to review the change. The Group or Team Manager is responsible for reviewing the change requested by the Change Requestor to help ensure that appropriate testing, implementation and back out plans are available and to verify the justification. The Group or Team Manager must review changes assigned to them within two business days. They will either set the RFC status to 'Group Manager Approved' or 'Group Manager Rejected'. RFCs that require further information or subsequent update will be marked 'Group Manager Deferred'.

Change Advisory Board (CAB) approval

The CAB is made up of key representatives from various parts of the ESR Programme Team as follows:


ESR Operations Project Board
Change Advisory Board (CAB)
Technical Services Representative
Development Team Representative
Database Administrators Representative
Network Representative
Application Support Representative
Customer Support Senior Representative
Business Systems Team Representative
Data Warehouse Team Representative
Capacity Team Representative
Release Team Representative
Test Team Representative
Internal Systems Team Representative
Information Security Manager

The RfC CAB meets every Wednesday and includes members of the NHS central team. During the meeting, the CAB:

- Reviews and approves upcoming changes;
- Produces the Schedule of Changes where downtime is required; and
- Reviews past changes to assess whether:
  - the change was implemented successfully;
  - the change met its objectives; and
  - the change did not create an unwanted side effect.

A quorum for this meeting consists of three people plus a member of the ESR Operations Project Board. Changes that do not have representation at the CAB may be deferred to the following week or rejected in its current form.

Any Requests presented to the CAB will be discussed and a decision made. The decision will take one of the three forms:

- Approved - The change will be scheduled into a change window and the implementation must take place within that period. Failure to do so requires reporting back to the CAB for rescheduling;
- Deferred - The change request contains insufficient information or more details are required. This may also be used to give approval for more work to be carried out. A deferred decision will involve details of what is required and a deadline of when the RFC needs to be resubmitted to the CAB. The status will be changed to ‘Further information required’ and must have the status changed when it is ready for reconsideration; or

- Rejected - The change is considered to be inappropriate in its current form and must not be implemented. A rejected decision will often provide a justification for the decision. The database is configured to automatically close the rejected change request.

Scheduling of changes

Approved changes that involve downtime will be scheduled by the CAB into defined change windows in the Forward Schedule of Change (FSC) Calendar (maintained in the Microsoft Outlook Public Folder). Each change will obtain a slot which must be adhered to. No change must start earlier than its allotted slot and must complete within the time allocated.

Other changes will be implemented as and when deemed appropriate but cannot be carried out in core hours. Core hours are defined as 08:00 – 18:00 Monday to Friday (excluding Bank and Public holidays).

RFCs that are not scheduled in the CAB will be scheduled by the Change Manager or change requestor (for PAL changes).

Monitoring and Review of Changes

Changes that have been implemented need to have the appropriate RFC updated with details of the success and any outstanding issues. This must be completed within 24 hours so that the Group or Team Manager can represent the review at the next CAB meeting. If the CAB agrees with the change implementation and no more issues are raised by any Group or Team Managers, then the RFC is closed by the authorised individuals.

Emergency Changes

From time to time it is critical that changes are implemented as an emergency to fix either a system failure or to allow the system to continue to operate. In the event of system failure, changes may only require approval from the Change Manager (or the System Level Manager 1 (SM1) out of hours). If the system is not currently down or if implementing the change will cause additional disruption to the service an emergency RFC should be raised. The emergency change may mean that testing is not undertaken and the risk assessment is performed by the Change Manager (or SM1 out of hours). If a change is rejected, the request will be processed through the CAB and its priority will be automatically upgraded to high.

Network related changes

Changes to the firewall rule sets can only be made by the six authorised members of the IBM Network Support and Infrastructure Teams. Changes to firewall configurations and rule sets are logged to remote syslog servers, to which the teams do not have access to. All changes must be raised and approved through the Request for Change (RFC) process described in section 1.3 above.

1.4 Access to production

A tool named Kintana is used to control the migration of source code and changes within production. Kintana restricts developers from promoting changes into the production environment directly. There are only two security groups within Kintana that are granted access to release functional changes to the production environment: PROD Special Access (Limited) and Kintana Administrator. Each security group consists of a number of users who are members of the ESR Production DBA Support Team. A third security group (ESR Data Fix Management) provides access to release data changes into the production environment. The security group includes members of the Production DBA Support Team and ESR Application Support Team. Where custom configuration is required (formula changes), manual changes are implemented by the ESR Application Support Team. Manual custom changes are validated and tracked through Kintana.

At each stage within Kintana, authorisation is required to allow code to be implemented into test and development areas. Once full testing is complete, the ESR Release Team member is required to complete a TRN for the ESR Production DBA Support Team to promote code into the production environment. Upon receipt of the TRN, the ESR Production DBA Support Team performs the following steps in Kintana: (1) Check Release, (2) Process Release and (3) Auto task from Kintana. The auto task from Kintana only implements the non-configuration changes (including software upgrades and functionality changes). Configuration changes need manual intervention from the ESR Application Support Team who will implement the changes into the production environment. System Administrator level of access within the ESR Application is required to implement such manual configuration changes. This level of access is restricted to appropriate members of the ESR Application Support Team and ESR Production DBA Support Team. After the changes are implemented into the production environment, the ESR Application Support Team notifies the ESR Production DBA Support Team who will subsequently update the information in Kintana.

Access to the Kintana application is restricted via a user ID and password. Each user is assigned to a user group, and each user group is assigned the relevant access rights required to perform their duties within their team. Access is defined to key stages within a workflow that can vary depending on function. Each step throughout the creation of packages to promotion to production is logged by Kintana, with each user’s User ID, date and the action performed by the user.

Control Objective 2: Logical Security

Controls provide reasonable assurance that security configurations are created, implemented and maintained to prevent inappropriate access.

2.0 Introduction

IBM and ESR Programme users gain access to the ESR Service by first logging onto an internal Active Directory domain and then by logging onto the ESR Service via Internet Explorer (this type of access is required for support purposes, in case the Smart Card infrastructure becomes unavailable). IBM employees and ESR Programme Team members may also require remote access. Accounts for IBM and ESR Programme users are created by the IBM Application Support Team.

2.1 Security Policies and Procedures

The ESR Programme Team designs and delivers security solutions and services to NHS Organisations, both in response to contractual commitments for ESR security compliance and in the provision of additional negotiated security services.

The team maintains a comprehensive range of security policies, standards, guidelines and procedures which are applicable to the management and security of the ESR Service and underlying data. It also monitors compliance with the applicable security policies and regulations. The ESR Information Security Manager is accountable for establishing the ESR Security policies and procedures. The ESR Programme Management Office (PMO) is responsible for maintaining those documents. A central repository of the ESR policies and procedures, as applicable, is maintained and is available to relevant ESR Programme Team members

The ESR Security policy and procedure documents define security requirements for the ESR Service. These documents define the responsibility for security between the ESR Programme Team and IBM

Availability of Policies and Procedures

The ESR policies and security procedures are maintained by the Governance Manager responsible for ESR in a central repository and accessible online by the ESR Programme Team.

The policies and standards adopt a layered approach to the security model, which requires security measures to be in place at each of the following levels:

- Physical;
- Logical;
- Personnel (User); and
- Procedural controls to safeguard NHS Organisations' data.

The Governance Manager seeks to ensure that the ESR policies and procedures are developed and implemented in a consistent manner. During the appraisal process, IBM employees are required to sign that they have read and understand IBM's Cyber Code of Conduct, Code of Business Conduct and Ethics, Data Confidentiality Code of Conduct, Health and Safety Policy and Security Policy.

Among the ESR policies and procedures that are maintained and available to the ESR Programme Team, some have been outlined below. The NHS ESR Central Team have access to only some of those policies:

- **OO-3000 ESR Security Policy Manual** – outlines the security measures that have to be followed by Sub Service Providers, employees, sub-contractors and customers working on its sites. The document covers, among others, the security policy, risk analysis, data confidentiality and incident management;

- **P-2600 Access to ESR Environments** – details the procedure for requesting, authorising and granting access to ESR environments for Sub Service Providers and/or the ESR Programme users who need access for maintenance, support or other system-wide purposes, as opposed to those users who are set up by the NHS Organisations;

- **OO-2000 ESR Information Security Policy Statement** – contains a brief security policy statement that defines that the Sub service Provider has a fundamental responsibility to protect the data in the ESR Service from threats, whether internal or external, deliberate or accidental;

- **OO-0200 ESR Security Risk Assessment** – structured to satisfy NHS Organisations' concerns with the ESR Service, including potential security-related risks and should aim to provide confidence that the ESR Programme Team has addressed key risks;

- **HH-25006 Major Incident Management** – defines the main categories of incident and the procedures of managing the incidents through to the resolution; and

- **Acceptable Use Policy** – contains the policy and procedures for internet/e-mail usage.

The following policies and procedures are available to IBM and ESR Programme Team but not to the NHS ESR Central Team:

- **OO-25013 ESR Security Management Plan** – an IBM document which is equivalent to the ESR Programme document *O-0300 ESR Security Policy and Procedures*;

- **ZZ-25002 – ESR Operate Quality Plan** – provides policies relating to the Quality strategy, including project methodology, resource management and service management policies.

- **OO-30040 – ISMS Information Classification, Handling and Retention Policy** – provides information related to, among others, data classification and responsibility for data classification.

2.2 Application level access to the ESR Service

2.2.1 User administration responsibilities

Administrative User Account creation procedure

The IBM Application Support Team is responsible for creating the initial 'Administrative User Accounts' for nominated contacts in each NHS Organisation which uses ESR (it is recommended that each organisation restrict this to two users if possible). These nominated contacts in each NHS Organisation act as the local administrators, and have the capability to create/modify/revoke user accounts for their local NHS Organisation. They can also create/modify/revoke other local administrator IDs for their own NHS Organisation.

2.2.2 User administration responsibilities for Sub Service Provider employees and ESR Programme Team member user accounts

The ESR Application Support Team is responsible for creating and modifying ESR accounts for Sub Service provider employees and ESR Programme Team members who require access to the ESR

Service. They are also responsible for revoking those accounts when Sub Service Provider employees and ESR Programme Team members leave the company / project. These are referred to as ‘National user accounts’, as the users have access to the data for more all NHS Organisations. It should be noted that national user access is restricted access and is limited to an as needs basis to only those who require it on routine basis to carry out their job role. Sub Service Provider employees and members of the ESR Programme Team need such access to the system for fault investigation, global system administration and database administration.

The ESR Technical Support Team is responsible for helping to ensure that the AIX operating system that hosts the ESR Application is configured properly in line with the baseline standard.

Account creation, modification and revocation procedure

IBM adopts a principal of granting permanent and temporary user accounts for IBM Employees and the ESR Programme Team. Temporary account holders are limited to a defined period of time which cannot be extended without authorisation from the ESR Application Support Manager. The procedures in place are outlined below:

Granting and modifying user access rights – Sub Service Provider Employees and ESR Programme Team

Requests for user access to the ESR Service are initiated by the requestor (Group or Team Manager and/or members) by completing the P-2601 Environment Access Request Form. The request has to be approved by the Line/Project Manager and the Gatekeeper (the data owner) before being submitted to the ESR Application Support Team. The Line/Project Manager approval is optional where the Gatekeeper is also the Line/Project Manager. Upon receipt of the request form, a member of the ESR Application Support Team validates the request and creates the ESR account.

In order to modify a user’s ESR account, the Group or Team Manager submits a P-2601 Environment Access Request Form with the modified access requirement. This then follows the same process as the ESR account creation procedure.

Granting remote access– Sub Service Provider Employees and ESR Programme Team

Specific requests must be made for remote access. Such requests have to be authorised by a member of the ESR Sub Service Provider Senior Management Team prior to being submitted to the ESR Customer Support Team. At this point a risk assessment is undertaken to help ensure no risks are added to IBM’s Corporate Network.

Users connect remotely via a Virtual Private Network (VPN) client which requires two factor authentications to connect onto the Sub Service Provider’s Corporate Network. With this method of authentication, users have to enter the VPN ID, a PIN number followed by six-digit code that is shown on a physical RSA ID token, which changes every sixty seconds. Access to ESR production environments by ESR Sub Service Provider team members is only permissible via a VDI (Virtual Desktop). This VDI is only accessible with an Active Directory account. The VDI controls all the software available to the account holder, no applications or data can be downloaded to an individual PC or laptop. Once connectivity has been made, a second level of authentication is required to authenticate to the Active Directory Domain. For users who have access to the ESR Service, they are also required to enter the application ID and password if they need to access the ESR Service. The ESR Service does not assume authentication by trusting either the VPN or Active Directory connectivity.

Revoking access rights – Sub Service Provider Employees and ESR Programme Team

Line management and Human Resource (HR) use a Leaver Checklist to help ensure that leavers’ access to programmes and services is revoked upon their departure.

The leaver’s Group or Team Manager contacts HR to notify them of the leaver. HR end-dates the employee record which initiates the HR leaver email notifying the relevant Groups (including ESR Application Support) of the leaver. Upon receipt of this email the ESR Application Support Team end dates the ESR account with the leaver’s leaving date. The leaver’s Group or Team Manager then has to signoff and submit the checklist to HR.

2.3 Operating system access (AIX)

Access to the AIX Operating System

The ESR Application and Oracle database are hosted on the AIX operating system. Currently there are eleven production servers that host the ESR Application and another six production servers that host the Oracle database. These production servers balance the workload, and are located in the Warwick Data Centre.

There are a number of AIX default (vendor provided) and service or system accounts on both the ESR Application and Oracle database production servers. The ESR Technical Support Team Manager who reports directly to the ESR Technical Team Manager, functions as the AIX Administrator and he is responsible for creating and maintaining the AIX accounts. Only the ESR Technical Programme Manager (the Leader of the ESR Operations – Technical Infrastructure) and the members of the ESR Technical Team have the authority to use these AIX accounts.

A single AIX account is used to login to the ESR Application production servers and a separate AIX account is used to login to the Oracle database production servers. These accounts are shared by the AIX Administrators and the members of the ESR Technical Support Team. Use of the AIX accounts has to be via a technical portal which provides key stroke logging level data. The Technical Portal is automatically set to log logons, logoffs and transactions performed by recording keystrokes and output by each user. This audit log is reviewed only on an exception basis.

Manual procedures require AIX administrators to login through the Technical Portal when accessing the AIX servers to make changes. Before the AIX Administrators can login through the Technical Portal, they should have their user profiles created in the Technical Portal. This user profile in the Technical Portal authenticates the username against the user’s Active Directory username, user domain and user DNS domain.

Baseline Operating System Standards

Logical system security parameters are specified by the ESR Technical Support Team. The ESR Technical Support Team will use the relevant and current security standards to build and configure the hosted operating system to help ensure consistent configuration and security across AIX servers supporting the ESR Application. Alternative settings may be used where required for operational purposes or where the baseline settings are not applicable. Changes to operating system configurations are managed through the change management procedure.

Direct access to the AIX server is restricted to a small group of key users to guard against the Technical Support Team being ‘locked out’ of AIX should the Technical Portal become unavailable for some reason. If direct access is gained while the Technical Portal is running, a system generated alert is produced which is then escalated. The AIX log file is configured to record logon and logoff information. This audit log is reviewed only on an exception basis.

2.4 Database access (Oracle)

Overview

The ESR Application is based on the standard Oracle HRMS. The Oracle HRMS was configured and customised by the ESR Programme Team to help ensure it aligns with the NHS Organisations’ business objectives. The ESR Application runs on an Oracle 11g database.

There are six database servers and eight application servers that are located in IBM's Data Centre in Warwick, England which share the load. These are load balanced through both network layer technology for user connectivity as well as internally within the database technology.

The ESR Production DBA Support Team is responsible for managing the Oracle database. They are responsible for defining standards for the design and physical build of the databases, and for defining production standards that include processes for the administration of the security surrounding the databases. The Team also provides support to the development and test stream as well as production. No employee is permitted to work on production until they fulfil a security assessment and are deemed sufficiently skilled by the DBA management group. The Team reports directly to the ESR Technical Programme Manager who looks after the technical service function for the Oracle database and AIX operating system.

NHS Organisation users cannot access the ESR programs and data files directly. They access the database through the ESR front end application system using their own application IDs and passwords.

Accessing Oracle

The Oracle database that supports the ESR Application is hosted on six production servers which run on the AIX operating system. A single AIX account is used to login to the Oracle database production servers through Technical Portal. This account is shared among the ESR Production DBA Support Team, which comprises of approximately ten team members. Technical Portal is automatically set to log logons, logoffs and transactions performed by recording keystrokes and output by each user. This audit log is reviewed on an exception basis.

There are three system accounts with administration rights. The ESR Production DBA Support Team uses these accounts to administer the database. One is used for accessing the database locally, and the other two are used for indirect access.

Procedures require Database Administrators to login through the Technical Portal when accessing the Database servers to make changes. Before the DBA can login through the Technical Portal, they should have their user profiles created within it.

Database Security Configuration

The Oracle HRMS application, upon which ESR is based, has embedded access controls such as user profiles, passwords, account expiration dates and responsibility profiles.

Database passwords vary from server to server and are controlled using KeePass Password Safe. These password safes are limited to the ESR Production DBA Support Team. A KeePass password is then required to gain access to the safe. KeePass encrypts the database in which it stores the passwords under control.

Database Audit Logging

Audit logging on tables within the Oracle database is enabled. Failed logons, logoffs and changes made to ESR data records are logged at an application level.

Although ESR user activities are recorded in the audit log files, no active monitoring is performed on the logs by the Sub Service Providers and/or the ESR Programme Team. However, the Sub Service Providers and/or the ESR Programme Team can investigate exceptions in the log files, as required. These log files are kept indefinitely.

2.5 Accessing the Technical Portal to obtain access to the operating system and database servers (AIX and Oracle)

In order to access the AIX operating system and the Oracle database, users must log in via the Technical Portal. The procedures for creation, modification and revocation of Technical Portal accounts is as below:

Granting and modifying user access rights

Access through the Technical Portal requires a background authentication against the Active Directory username, user domain and user DNS domain. Therefore, users who request access to the Technical Portal should have an Active Directory account created for them as well.

Within the Technical Portal, users are assigned to a specific User Group based on the user's job functionality. Each user can only belong to one User Group.

If a member of the ESR Technical Support Team requires a change to the access rights on the Technical Portal, the Line or Team Manager contacts the Technical Portal Administrator who will perform the required amendments.

Revoking access rights

Line management and Human Resource (HR) use a Leaver Checklist Set to help ensure that leavers' access to programmes and services is revoked upon their departure.

The leaver's Group or Team Manager contacts the Technical Portal Administrator who will disable the Technical Portal account upon notification of the termination.

Since access through the Technical Portal requires a background authentication against the Active Directory username, user domain and user DNS domain; once the leaver is deactivated in Windows Active Directory, access cannot be gained through the Technical Portal using that account.

2.6 Networks: Access to firewall devices

Overview

The primary data centre in Warwick and the secondary DR centre located in Newcastle are each provided with a dual Primary/Secondary Gigabit circuit to the NHS HSCN network. Each circuit is diversely routed to help minimise risk of failure. Additional firewall load balancing is added as required, the whole infrastructure estate was refreshed in the past year, the service now runs on IBM P8 Processors and incorporates new network switches, routers and firewalls.

The NHS HSCN network connections are then terminated to a pair of firewalls configured in a primary/secondary design. Both firewalls actively monitor the traffic flows into the ESR network and automatically switch over in the event of failure. This can reduce the risk of unavailability due to events both inside the Sub Service Provider's Data Centre, and NHS HSCN network link failures. The secondary DR Data Centre located in Newcastle is configured to replicate the design of the primary Data Centre at Warwick.

The NHS Systems Integration Team based in Sheffield, South Yorkshire provides an additional service to NHS Organisations, enabling them to reformat GL interface files. This functionality is provided on the NHS Hub, a separate server to the ESR Core service servers. NHS Organisation users access the NHS Hub using the Web Service facility, which is a web based front-end system available on the NHS intranet via the NHS HSCN Network.

The firewall that resides between the NHS HSCN network and the NHS Hub is the same physical firewall that resides between the NHS HSCN network and the ESR Application. However, the physical firewall is logically segregated into different 'zones' to control access to the ESR application and access to the NHS Hub. The IBM Network Support and Infrastructure Teams manage the firewall ‘zones’. As a result, the controls and processes in place to manage access and changes to the firewall are common for the ESR Service and the NHS Hub.

A limited set of permitted services are identified and implemented in firewall configurations. Firewalls were initially configured with access denied to all traffic, and services accepting incoming and outgoing traffic were added later. This includes specific rules that were added during the infrastructure refresh during the year.

Key controls over the network firewall include:

- An SLA is in place with an outsourced third-party provider (IBM Security Operations Centre) who are responsible for managing intrusion detection devices that sit in-line with the firewall.

- Firewalls supporting the ESR application are configured and installed to prevent access unless specifically allowed.

  Firewall settings have been configured in line with best practice to ensure that only access is restricted to authorised traffic only.

- Access to update rule sets for firewalls in production is limited to six members from the Sub Service Provider Network Support and Infrastructure Teams.

  Changes to the firewall rule sets can only be made by the six authorised members from the IBM Network Support and Infrastructure Teams. Changes to firewall configurations and rule sets are logged to remote syslog servers, to which the teams do not have access to. All changes must be raised and approved through the Request for Change (RFC) process.

- Firewall activity is logged on an audit log and monitored.

  Firewall activity, including rule-set changes, are captured and monitored by the IBM SOC team. They receive a real-time stream of activity on the firewalls, ranging for internal support teams logging to external connections. They review the audit logs on an exception basis, if alerts are sent by the firewall and the Network Management System. If an exploitation attempt is identified, or a high volume of unknown traffic is found to be targeting a particular port or service on the firewall, the traffic will be blocked from targeting that port or service as a matter of priority. The logging is also extended to all the production and DR servers.

2.7 NHS General Ledger Interface

2.7.1 Security Policies and Procedures

The ESR policies, standards, guidelines and procedures noted in section 2.1 are applicable to the NHS Systems Integration Team and users. This is in addition to any local NHS Systems Integration Team policies and procedures for the management of security of the NHS General Ledger Interface service and its underlying data. All policies are held on a local file server which acts as a central repository for the team. Access to the file server is restricted to members of the NHS General Ledger Integration Team.

The NHS Systems Integration Team has in place a Support Processes and Security Policy document which defines security requirements and any related procedures. It provides a description of the responsibilities for the setup of NHS Interface account usernames and passwords (for both privileged and non-privileged user accounts). It lists the names of the Production Controllers who have access to the production user account, and also describes the process for requesting and granting of access for NHS Organisation User accounts.

The document and associated procedures are reviewed and updated as appropriate on an annual basis. The NHS Systems Integration Team Manager is accountable for establishing and maintaining security policies and procedures for the GL Interface.

Access Controls to Data Files and Programs

NHS Organisation users access the NHS Hub using a Web Service username and password. The NHS Systems Integration Team is responsible for creating one generic production Web Service user account and password for use in each NHS Organisation. A nominated contact in each NHS Organisation acts as the local administrator and has the capability to download target files and modify lookup tables on the NHS Hub via Web Service.

NHS organisations are responsible for ensuring that the Web Service user account created for their organisation is appropriately controlled. Dissemination of the user account and password details within the organisation is the organisation’s decision and responsibility.

Web Service users access the NHS Hub by first logging onto the NHS HSCN network, and then onto Web Service on the NHS Hub via Internet Explorer. Web Service users in NHS organisation can only access their own data. The Apache Service’ which runs on the NHS Hub restricts access as appropriate. Users’ credentials (username and password) are verified by the Apache Service when they log onto Web Service. The user is then mapped to the file location where their organisation’s files are stored.

The Sub Service Provider Technical Team is responsible for helping to ensure that the AIX operating system that hosts the NHS Hub is configured in line with the ESR baseline standard, as well as for user administration on the NHS Hub AIX operating system. Administrator access to the AIX servers is through the Technical Portal. User administration procedures for the AIX operating system hosting the NHS Hub are the same as those for any other AIX server for ESR. Refer to Section 2.5 for details.

Web Service user account management / administration

Account Creation

If an NHS organisation user requires access to the Web Service, they must raise a Service Request (SR) on the ESR Service Desk. The process for raising SRs incorporates who can legitimately raise and authorise an SR within NHS organisations.

SRs are validated by the NHS Integration Team before they create a master user account (username and password) for that NHS organisation. Where additional verification is required, the Team contact the requesting organisation. Once a master user account has been set up, the NHS organisation's master account user is able to, using the Web Service, change the password that is initially allocated to them by the NHS Systems Integration Team. The master user account can also create secondary user accounts, 'within' that NHS Organisation. Secondary user account holders cannot create further accounts, but can change their own account's password. The master account password holder can reset secondary account user's passwords, or delete their secondary user accounts. Thus, once issued by the NHS Systems Integration Team, responsibility for account management rests with the NHS organisation. However any issues concerning account usage and setup may be referred to the NHS Systems Integration Team via an SR.

To help ensure that the Web Service passwords allocated to NHS organisations are strong, the NHS Systems Integration Team use a script to generate a random password (using a combination of upper- & lower-case letters, numbers and 'special' characters) for the account. The random password has a minimum length of 8 characters in line with suggested good practice. The same complexity rules are applied whenever an account password is changed using the Web Service.

Account Modification

There is only one standard Web Service account profile which grants the same level and type of access to all NHS organisation users of the service, there is no requirement to request access modifications. However, within the standard profile, master and secondary accounts are recognised. The only functional difference is that only the master account has the ability to setup, change or delete secondary accounts.

Any account which has not been used for over 24 months is automatically inactivated as part of daily housekeeping for the Web Service. Normally, as there is only one master user account per organisation, but unlimited secondary user accounts, there is no subsequent need for the NHS Systems Integration Team to add or remove access unless an organisation changes its GL system.

Account Revocation

Since each NHS organisation is allocated one Web Service master user account, the organisation's master user account is responsible for access to their master and secondary accounts. As a result, when an individual who has had access to an account leaves the organisation, it is generally the responsibility of the NHS organisation's master user account to take appropriate steps. If this proves impossible (for instance if the master user account holder has left) the organisation must log an SR on the ESR Service Desk and request a Web Service master user account change. Additionally, as part of the daily Web Service housekeeping any user account (master or secondary) which has not been used for over 24 months is automatically inactivated.

NHS Hub (administrative, production and development user accounts)

In order for members of the NHS GL Integration Team to be able access the production and development areas of the NHS HUB, they are required to have a username and password. For continuity of business purposes and the technical limitations associated with setting up individual user accounts, there is only one user account and associated password for each area.

Access to the shared username and password for the development hub is available to all members of the Systems Integration Team. Since 7 June 2021 the production password is only accessible via the KeePass safe. Access to the shared user account for access to the production Hub is limited to three members of the Team, and must be approved by the Team Manager.

There are three members of the team with access to both production and live areas of the Hub. In mitigation, a monthly reconciliation of all changes made to the production environment is undertaken by the Team Manager, who does not have access to the production environment. Testing for this control will therefore be undertaken under control 1b (change management)

Access controls over data files

The NHS Hub receives source files from the ESR application via the IBM hub. The NHS Hub processes the source files using Supporting Perl script scripts and GL Build routines, and generates target files for each individual NHS Organisation. Since the NHS Hub uses scripts to process data files, there is no physical database management system in use on the NHS Hub to manage the Source and Target files.

NHS Organisations users who have access to the NHS Hub using their Web Service accounts have view only access to the Source and Target files. Three members of the NHS Production Control Team who have access to the NHS Production Hub, have access to make amendments to Source and Target files. NHS Systems Integration Team policies do not permit manual changes to Source and Target files, therefore changes to these files are not carried out by the NHS Systems Integration Team.

Since there is no database management system in use on the NHS Hub, access controls over databases are not applicable to it.

2.8 TRS security

TRS allows current and former NHS employees to view a reward statement that defines salary, pension and other financial benefits. The system also allows NHS employers to tailor what information is presented to users in terms of what other benefits they offer outside of those related to the Payroll, such as access cycle to work schemes.

The TRS system is based on an Oracle database that is refreshed on an annual basis with data from the live ESR database via an ETL (Extract, Transform, Load) process. Only those datasets which are relevant for TRS are held in the database and there is no linkage between the TRS and ESR databases.

The system is web-facing and can either be accessed through an individual’s main ESR user account or creating a user profile of the Government Gateway site. Using a number of key identifiers, the TRS system is able to determine what information is to be presented to each user.

There are three main types of user accounts:

- Current/former NHS employee – can only access own information;
- Employer - can update employer information and view the statements of employees in their organisation; and
- NHS BSA – 3 levels of administrator accounts to amend user responsibilities and allow problem resolution.

A number of business rules have been defined which allow a user to perform certain activities. Each user type has access to different business rules to ensure that only relevant parts of TRS are able to be utilised and employees can only access their own information.

Control Objective 3: Problem Management and Performance and Capacity Planning

Controls provide reasonable assurance that system and network processing issues are identified, reported and resolved in a timely manner, and that performance against the SLA/contractual requirements for the ESR service is monitored.

3.0 Introduction

An SLA is in place for the provision of the ESR Solution through the ESR Service between IBM and the DHSC. The SLA includes a number of Key and Subsidiary Performance indicators which measure performance, availability reporting requirements and associated processes. SLA performance is monitored by the ESR SLA Manager who generates a Performance Monitoring Report for the NHS ESR Central Team at the end of each month.

The system capacity and performance monitoring is managed by the ESR Operations and ESR Performance Monitoring Teams using IBM Netcool which sends alerts by automatically distributing an e-mail to the ESR Operations and ESR Performance Monitoring Teams on issues identified. An SR is automatically raised for the alerts that meet the predetermined scope as determined and configured by the Sub Service Provider Network Operations Team in IBM Netcool.

System Capacity and Performance is proactively managed by the ESR Capacity Management team, using a combination of reporting tools and IBM Netcool. The output of this predictive work is reviewed monthly with the operational teams to present the status quo, and to define the actions needed to address any impending issues. This is further reviewed quarterly with the senior management team to present a summary of the System Capacity and Performance, along with the issues and mitigating actions and activities which are ongoing.

3.1 Performance and Capacity Planning

Monitoring of Service Level Agreement (SLA)

The ESR SLA Manager and the NHS ESR Central Team are jointly responsible for reviewing the contractual weightings for performance and availability, the results of which form the monthly Service Management reports which are tabled at the monthly Service Review Meetings.

Currently the SLA obligations are:

- Availability (HR, Payroll, Self Service, Data Warehouse, E-Learning, TRS, NHS Hub, Call logging);
- Critical Processes and interfaces;
- Performance (payment accuracy, payment timeliness and pay notification timeliness);
- Service Desk Performance (calls answered within target time, call back within target);
- Application support (service call resolution);
- Response times;
- Security (correctness of security profile, security breaches); and
- Training.

System Capacity and Performance

System capacity and performance is monitored continuously by the ESR Operations and ESR Performance Monitoring Teams using Topaz, which benchmarks transactional performance and automatically raises alerts within IBM Netcool if the processing time is not within the predetermined guidelines. IBM Netcool automatically distributes alerts by e-mail to these nominated officers on issues identified.

3.2 Networks: Availability Monitoring

The network that supports the ESR Service consists of a fully resilient highly available set of firewalls, distribution switches, and access switches zoned to allow segregation between discreet services. The network design helps to ensure that no central point of failure exists within the ESR network to the boundary to the NHS HSCN network. Additionally, components are configured to automatically switch over in the event of failure.

Failover testing from primary to secondary sites is performed on a regular basis by the IBM Network Operations Team. These tests are generally performed when changes are made to the primary network, to ensure that the failover remains effective.

Bandwidth and capacity planning is performed by the Sub Service Provider’s Network Operations Team. The current levels of usage on the network are correlated against the ESR Programme’s Network Capacity Model. The correlation between the current usage and the estimation of bandwidth and capacity requirement of each NHS Organisation moving forward is also performed, therefore ensuring that the current level of network usage is aligned to the estimated levels of usage as defined by the ESR Programme’s Network Capacity Model. This proactive estimation of bandwidth has proven to be successful, causing no problems regarding the speed in which NHS Organisations can access the ESR Service.

Orion Solarwinds is used to monitor the bandwidth utilisation and interfaces across the ESR network, providing alerting mechanisms directly to the Sub Service Provider’s Network Operations Team, along with the response times of the ESR network. Response times are analysed against a set of rules that define the contractual response time requirements. Thresholds are also set within the rules such that response times that are close to falling outside contractual requirements are also highlighted. This allows pre-emptive action to be taken. Response times that do not fall within the thresholds cause an alert that is sent to the ESR Capacity Management Team and the ESR SLA Management Team.

In the event of a network failure and/or issues which are detected by the Orion Solarwinds tool, alerts are generated and sent automatically via a service request to the Sub Service Provider’s Network Operations Team. The procedure of resolving network problems follows the problem management procedure as described in Section 3.3.

3.3 ESR Service Calls

All Service Calls are logged in the ESR Service Desk system (ICD). There is an ESR Programme Staff ICD Request Procedure which is maintained by the ESR Programme Management Office (PMO).

ESR Service Calls are submitted in one of the following ways:

- Log in to the Customer Portal website and create a Service Request (SR); or
- Call the ESR Service Desk and have the ESR Service Desk create the SR.

Process:

Service Requests (SRs) are investigated for appropriateness, prioritised and assigned to the appropriate ESR Team for resolution by the ESR Support Team. There are five levels of priority which are linked to the SLA:

- **Priority 1 -** a Service Call which:

  a) constitutes a loss of the Service which prevents a large group of ESR Users from working;
  b) has a critical impact on the activities of the Authority;
  c) causes significant financial loss and/or disruption to the Authority; or
  d) results in any material loss or corruption of Authority Data;

- **Priority 2** - a Service Call which has the potential to:

  a) have a major (but not critical) adverse impact on the activities of the Authority and no workaround acceptable to the Authority is available; or
  b) cause a financial loss and/or disruption to the Authority which is more than trivial but less severe than the significant financial loss described in the definition of a Severity 1 Service Failure;

- **Priority 3 -** a Service Call which has the potential to:

  a) have a major adverse impact on the activities of the Authority which can be reduced to a moderate adverse impact due to the availability of a workaround acceptable to the Authority; or
  b) have a moderate adverse impact on the activities of the Authority;

- **Priority 4** - a Service Call which has the potential to have a minor adverse impact on the provision of the Services to ESR Users.

- **Priority 5** - A Service Call comprising

  a) either a flaw which is cosmetic and, as such, does not undermine the ESR User's confidence in the information being displayed;
  b) Or a request for service, change or enhancement

Problem resolution is reviewed and tracked by the ESR SLA Manager to help ensure they are closed within the contractual timeframes. ICD has the capability to monitor progress against the SLA targets by SR. If an SR relates to a critical incident, the Problem and Incident Manager also reviews and tracks the issue.

The ESR Application Support Team and/or the assigned ESR Team responsible for resolving the problem is responsible for changing the SR status to ‘Customer Closure’. At this stage, the customer is responsible for confirming that they are satisfied with the resolution by setting the status to ‘Resolved’ or instructing the ESR Application Team to do so. Should a response not be received from the customer within 60 days of the SR being set to ‘Customer closure’, the SR is closed by the ESR Support Team. This is known as the ‘60-day rule’

An Age Profile Analysis detailing reported problems and their status is included in the Monthly Service Management report. The ESR SLA Manager and Application Support Team also monitor the outstanding SRs to ensure these are being resolved.

3.4 NHS General Ledger Interface specific controls

Availability of the NHS Hub application which resides within the IBM network is not the responsibility of the IBM Network Operations Team. As such, the NHS General Ledger Integration Team undertakes monitoring of the availability and response times for the Hub. They monitor the progress of files being processed on an ad-hoc informal basis. If there are any issues, a call is logged with the IBM Service Desk, and an SR is raised. The Service Desk will deal with it in line with the Problem and Incident Management process (as per section 3.3. above).

Control objective 4: Physical Security and Environmental Controls

Controls provide reasonable assurance that physical access to controlled areas is restricted to authorised individuals, and that facilities are protected against environmental threats. (Warwick and Newcastle Data Centres)

4.0 Introduction

The physical IT infrastructure for ESR is located within secure data halls in Warwick and Newcastle. Printing and despatch of pay advices is managed by a third-party service provider OPUS (this is located approximately 40 miles from the data centre, for which a contract is in place with IBM).

The exterior of the building is continuously monitored and provides a highly secure facility for the ESR service. The physical security controls deployed for the exterior and interior of the Data Centre follow both Sub Service Provider’s global security standards which have been certified under the information security standard ISO/IEC 27001.

An offsite storage facility is in place which is managed by a third-party service provider (this is located approximately 40 miles from the data centre, for which a contract is in place with IBM). This also complies with the same global security standards as the main data centre.

The controls descriptions provided below relate to both Warwick and Newcastle data centres.

4.1 Physical Security

The following physical security related controls are in place:

Monitoring of the Data Centre

The building is monitored by fixed CCTV cameras that record 24 hours a day, seven days a week. There is a line of sight over all sides of the building, which includes the exterior doors.

The internal data halls are also monitored by dedicated CCTV cameras, and all video recordings are electronically recorded to hard disk.

Staff are present within the Operations Room at the Data Centre at all times during working hours, and monitor CCTV recordings being taken within the data halls. Out of Hours the Security staff undertake walkarounds at regular intervals and that includes the Data Centre.

Access to the Data Centre and the Production Services Centre

Exterior access to the data centre

The office building which houses the data centre has one main entrance which leads to a manned reception area which is manned 24/7. A second entrance is positioned at the rear of the building and is used for goods delivery only. Two further exit points are also positioned at the side of the building. These are mandatory fire exit doors which can only be opened from the inside.

Outside of working hours (before 8am and after 7pm), the main entrance to the building is locked (including barricaded access to the car park) and is only accessible to staff members with an access card. The Security team patrol the building to ensure that first floor windows are closed, and that the alarm is active when the building is unoccupied by staff

Interior access to the Data Centre

During working hours access to the Data Centre can only be gained by manually signing into the Operations Room, and then passing through a series of access-controlled doors which require the use of an electronic access card. Only staff members who are primarily based within the Data Centre are issued with electronic access cards. Physical access to the ESR Warwick Data Centre is managed and controlled through a centralised corporate IBM system. Physical access to the ESR Newcastle Data Centre is managed and controlled via a standalone IBM system.

Access to the data halls and the Production Services Centre within the Data Centre is further restricted to an as needs basis, and only to those individuals who require it on a regular basis for the performance of their job-related duties.

Permanent access to the data halls

Should a staff member require permanent access to the data halls they are required to submit a request using the ICD system, which must then be approved by the IBM ESR Technical Team Manager.

Permanent access to the Production Services Centre

If permanent access is required to the Production Services Centre, a User Access request form must be completed by the requesting staff member, which must then be approved by the Operational Services Manager who looks after the Production Services Centre.

Temporary access to the data halls and Production Services centre

Should a staff member or visitor need temporary access to the data halls, a defined process is in place:

All visitors are required to sign in at the reception area at the main entrance of the building, and are issued with temporary paper-based badges which they must keep on display throughout their visit. Without an electronic access card, visitors can only gain access to the reception area and the meeting rooms on the first floor.

When a visitor requires access to the data halls or the Production Services Centre within the Data Centre, they are required to sign in on a separate Data Centre Visitor Log in the presence of an employee who has permanent access. Visitors are accompanied within the data halls and Production Services Centre at all times.

Periodic review of access, and revocation of access rights to the Data Centre

Periodically, the Operations Support Manager obtains a listing from the access control system showing which employees have access cards granting them access to the Data Centre. This list provides detailed information showing who has access to the data halls, the Production Services Centre, and to other sensitive areas such as data control facilities.

The list is circulated to each of the managers responsible for those areas for review and confirmation that the individuals listed still require access. If an employee has access that they no longer require, the manager responsible for that area is expected to request for that access to be revoked immediately.

For the Newcastle Data Centre, this was performed every 6 months. For the Warwick Data Centre this was performed quarterly thereafter.

Employee termination follows the standard ESR account process. This involves ESR Resource Management sending an email to the distribution group 'UK Leaver Notification' detailing the employee's name and final working day. Access card administrators are members of the UK Leavers distribution group. Therefore, ordinarily leavers' access cards which grant then access to the data centre should be revoked on their last day of work. It is the leaver's line manager's responsibility to retrieve Sub Service provider property which includes their physical access card. If for any reason the access card is not retrieved, the card should not work in any case due to their access rights being revoked by an access card administrator, as per the notification from ESR Resource Management.

4.2 Environmental Controls

The Data Centre is supported by an infrastructure configured as N+1 (individual components have at least one independent backup component such that a single point of failure does not exist) including an Uninterruptible Power Supply (UPS), two backup generators, VESDA smoke detection systems and fire suppression systems to protect the Data Centre from damage by natural disaster and/or environmental hazards. The equipment is regularly serviced by the appropriate vendors

The following environment related controls are in place:

Fire Suppression

Smoke detectors which are linked to a Red Care fire alarm system are located throughout the data halls in the Data Centre. This system automatically notifies the fire service when a fire is detected. The main building is split into 12 zones, and the alarm box is accompanied by a wall chart showing the location of the 12 zones. There is also a weekly fire alarm test, performed by the building maintenance staff.

The Data Centre is protected by an Inergen gas fire suppression system and a VESDA smoke detection system. It is set to the default setting of manual/automatic, so that it will automatically release gas when a fire is detected. It can also be manually released if required.

A mixture of CO_2 powder and water fire extinguishers are strategically located throughout the building.

Maintenance and Monitoring of Equipment

Maintenance agreements are in place for the regular servicing and repair of the following equipment in place at both Data Centres:

- UPS;
- Generators;
- Fire Alarm;
- Smoke Detection System;
- Fire Suppression;
- Cooling and Environment Monitoring; and
- Access Control Systems.

The Data Centre temperature and humidity is controlled by Airedale down flow units and condensers and the temperature in these rooms is set to 22°C. Detected changes in temperature or humidity result in an alert being triggered in the data control room, and the temperature is changed accordingly.

Under floor air conditioning is utilised and the air supplies are positioned to primarily cool the back of the server cabinets thereby creating hot and cold aisles.

Power Supply Protection

Two diesel generators are in place and are used to support and provide power to the Data Centre in the event of a prolonged power failure. A single generator has the capacity to provide power for up to 96 hours, with its own 21,000 litre diesel tank.

The Data Centre is also supported by a UPS (of which there are three), in the event of a short-term power failure. The UPS is supported by approximately 360 YUASA Endurance batteries. The UPS has the capacity to supply power to the building for at least 20-30 minutes. However, the diesel generator will automatically take over supplying power from the UPS after 2-3 minutes when it is at full power. The UPS and batteries are located in a separate room inside the building that can only be accessed through three access-controlled doors.

The UPS room is cooled by an Airedale cooling system and the battery room also has a Daikin split air conditioning unit. The temperature in these rooms is set to 22°C and is monitored on a regular basis throughout the day by IT staff.

Both the UPS and generator are tested ‘offline’ for approximately 20 minutes on a weekly basis. Three monthly full load generator tests are also undertaken.

4.3 Disposal of media

In line with the Secure Disposal policy, all magnetic media, such as back-up tapes and hard disks, are degaussed by Data Centre operators before being passed to a third party for disposal.

When a media item has been identified for disposal due to being taken out of service, the ESR Technical Team, remove the disk or tape and pass to the Data Centre operators for disposal. The item should be accompanied by a ‘Disposal Request Form’ to evidence that the item has been degaussed.

Currently there are two degaussers deployed within the UK located at each Data Centre. These are Verity Systems SV91 M certified to UK CESG Degaussing Standard and approved for disposal of UK Government Restricted protectively marked data.

Following degaussing, the items are passed to a third party for shredding in line with WEEE regulations.

Control Objective 5: Computer Operations

Controls provide reasonable assurance that standardised operating procedures are being followed, processing is appropriately scheduled, authorised and completed, and backups are performed and securely stored.

5.1 Computer Processing

Key payroll scheduling dates were configured on the ESR Application during the initial implementation of the system. Subsequently, every March prior to the beginning of each financial year, the ESR Programme requires NHS Organisation payroll users to supply scheduling information to the Sub Service Provider for the forthcoming 12 months. These jobs are manually invoked by NHS Organisation payroll users. For example, when a NHS Organisation needs to print payslips for its employees, the job must be submitted by an appropriate payroll user within that NHS Organisation. The submitted jobs are queued and processed according to predetermined priority levels in the Concurrent Manager System, which is part of the Oracle HRMS application and is used to run reports at various stages.

Additional automated processes used for routine data maintenance and data extracts and inbound and outbound interface files (e.g., pensions and national insurance data that is updated from ESR) are also executed at regular scheduled intervals within the Concurrent Manager system.

A national request set document listing jobs scheduled to run for the ESR application is maintained. Data extracts from the ESR application are used to support the HR and payroll processes for NHS Organisations.

Scheduled processes are monitored to ensure that they run to schedule and complete normally:

- The Concurrent Manager system automatically generates email daily following the completion of scheduled jobs showing the status of the jobs (success/failure); and

- The Monitoring Team also checks all ‘National’ processes every morning in the daily checks, and hourly using Netcool..

Any schedule related incidents are managed through the problem management process (refer to section 3.3).

If changes are required to the schedule of automated processes, these must be raised, authorised, tested and implemented through the application change process as outlined in (section 1). Issues or failures related to scheduled automated processes are identified by the Monitoring Team using the daily scheduled job completion status email, and are managed through the problem management process.

5.2 Data Backup

The ESR Technical Team is responsible for managing the backup of the hardware and software components for the ESR Service. This includes the operating system, Oracle 11g database, and the ESR Application which are all hosted at the IBM Data Centres.

The ESR Tape Operators perform tape library administration for the backups. Tapes are transported, stored and catalogued offsite by third party Iron Mountain. Iron Mountain are responsible for collecting and delivering backup tapes on a daily basis.

Tivoli Storage Management (TSM) is used for the management and storage of tapes. The TSM server is located in the Sub Service Provider Data Centre in Warwick, and the backup tapes are stored in an

This report is intended solely for use by the management of ESR, its user entities, and the independent auditors of its user entities, and is not intended and should not be used by anyone other than these specified parties.

off-site building which is located approximately 40 miles from the Data Centre. Both locations are subject to physical security controls and environmental security controls.

Backup Schedule

The frequency of backups has been agreed by NHS ESR Central Team and the Sub Service Provider. TSM is used to schedule, perform and monitor tape backups for the systems hosted at the Data Centre in Warwick.

- Full backups of ESR application files, log files and databases and the NHS Hub are performed daily and are retained for a month;

- Monthly backups are also performed every first Sunday of each month and are retained for 370 days. These backups also include the backup of the TSM system and records; and

- Separate backups of the AIX operating system (including configuration settings) are performed on a daily basis.

Backup Monitoring

The IBM Netcool tool raises an event with the system which is then assessed by the ESR Technical Team to determine whether or not a Service Request needs to be manually raised. Because the Netcool tool provides information about each event, only those errors that require action to be taken have Service Requests raised. Outside of normal working hours, the system is monitored by Data Centre operators who have been briefed about which events need further action.

Tape Storage

One set of backups is stored in an automated library located in the Warwick Data Centre and another set of backup tapes is collected and stored by third party Iron Mountain.

A ‘Log Shipping’ Mechanism is also in place which moves the Oracle 11g archive logs to the Disaster Recovery site located in Newcastle, England. The logs list the recent transactions that have been committed to the database and are transferred to the Newcastle site over a secure FTP connection. At any one time, the data in the Disaster Recovery site is approximately one hour behind the live environment.

The Disaster Recovery site is used as the primary method of recovery in the event of data loss.

Offsite Storage Facility

The Sub Service Provider stores backup media at a storage facility situated approximately 40 miles from the Warwick Data Centre. The tape storage area used has a single entrance accessible from the inside of the building, which is alarmed. The room used to store the backup media has a locked door with PAC ID Key access and an air conditioning unit which also covers humidity protection. A standalone CO2 powder fire extinguisher is positioned outside the storage room.

The building has a fire detection system, which automatically notifies the fire service when a fire is detected.

Backup media is kept on shelving racks within the tape storage area.

All backup media marked as exceeding its natural life is degaussed within the Data Centre and shredded before being disposed of.

Testing of Backup Tapes

The disaster recovery (DR) plan is regularly tested as part of the major release schedule as the production environment is required to be restored onto the test servers to allow for testing of changes and rehearsals of the upgrade process.

Where required as part of major releases, backup tapes are restored at the DR site.

Control objective 6: Payslip Distribution

Controls provide reasonable assurance that system output is complete, produced on a timely basis and properly distributed to NHS Organisations.

Introduction

The ESR Programme Team provides a service to NHS Organisations for printing payroll related outputs (including payslips, P45 and P60 forms).

Until May 2018, the Production Services Team (working on behalf of the ESR Programme Team) was responsible for helping to ensure and monitor that the payslips, P45 and P60 forms are complete, produced on a timely basis and despatched to the relevant NHS Organisation. From May 2018 this responsibility was transferred to OPUS under contract with IBM and is covered by a SLA and performance monitored periodically against agreed KPIs. The payslips are printed on a weekly or monthly basis, depending on the agreement between the ESR Service Management Team and the NHS Organisations payroll customers. The Production Services Team/OPUS follows a number of procedures and checks to help ensure the completeness of output.

Payroll related outputs are despatched to the relevant NHS Organisation for onward distribution to employees and it is the responsibility of the NHS Organisations to initiate the payroll print process (this is performed through the ESR application over a secure internet connection).

The OPUS solution operates on 24/7 operation based in a secure location in Leicester with access restricted to authorised staff through the use of access cards. OPUS's own controls are not in scope for this report, but there are monitoring controls in place over OPUS which are tested.

Payslip Distribution

The initiation of the printing jobs is the responsibility of the NHS Organisations who initiate printing through the ESR application.

The payslip process initiated by the NHS Organisations results in payslip files being sent to the Production Services Team/OPUS for printing. The Production Services Team/OPUS activates the printing of the payslips and the client print operators monitor, on a continuous basis, the print jobs on the consoles within the printing room during payslip production. The printers automatically generate a print log file detailing the date and time the file was received and printing was activated.

If problems occur during printing, the print operators are responsible for resolving the errors. This may include adding more paper to the printer, aligning the payslip paper correctly in the printer, reprinting a single payslip, a series of payslips or the entire batch of payslips. Printer related problems are logged within the print log and include details for re-prints that were initiated. Printing problems that impact NHS Organisations and contracted service level agreements (SLA), such as an incomplete or late printing of payslips, are logged as a service request (SR) via the standard problem management procedure.

The print process incorporates closed loop technology which prints a unique barcode on each payslip. Once the print job is complete, the payslips are passed through a payslip sealing device which also scans each payslip. The Production Services Team used a pressure sealer whereas the OPUS uses a Zip Dox' sealing solution. The sealer detects duplicate or missing payslips within the batch. Duplicate payslips are removed from the batch and missing payslips are reprinted by the client Print Operators. Duplicate or missing payslips and reprints initiated are automatically consolidated within the Infoprint Workflow (IPW) log.

When a complete batch of payslips is printed, under the Production Services Team they were consolidated where relevant, and sent to the Despatch Controller who gathered and sorted print jobs received within a one-hour period by NHS Organisation. With the exception of P45's, OPUS uses a fully automated sorting solution. The print jobs are gathered so that they can be despatched as part of one consignment and are packaged in bundles of 200 payslips. The consignments are then sent to the Despatch Operators within the despatch areas for consignments of 1600 or less; consignments with more than 1600 payslips are retained and packed in the print room for efficiency. Please note; although consignments are now packed in both the print room and dispatch room the same process (detailed in the paragraph below) is followed in both rooms.

The Packing Operator updates a control sheet with the number of payslip files received making up the consignment and the NHS Organisation for which the payslips have been printed. The payslips included in the consignment are automatically scanned to confirm that the payslips have the correct NHS Organisation number printed on them and that they are for the same payroll name. Finally the Packing Operator checks that the delivery labels that will be attached to the consignment have the correct Organisation number allocated. Once the checks have been completed, the control sheet is signed off by the Packing Operator. A Verification Operator in the despatch area repeats the check process and also signs the control sheet as evidence of the review performed.

At the end of the day, parcels are gathered as the courier arrives to collect the payslips for distribution and delivery before 10.30am the following working day (as per the agreed SLA in place with the DHSC). The courier driver scans each package while the Despatch Team performs a manual count. The totals from the driver's scan and the Despatch Team count are compared with the End of Day manifest generated and the results are updated in the End of Day Reconciliation control sheet, this is signed by both the courier driver and the Despatch Operator. If the totals correspond, the packages are despatched from the main Production Services Centre for delivery to the NHS Organisations.

The courier takes the parcels to the national hub where they are sorted for onward journeys to enable local drivers to deliver before 10.30am. The courier company provides access to online reports regarding the status of the packages to the Production Service Team the next working day after collection. It is the responsibility of the Production Services Administration Team to monitor and reconcile the reports to maintain visibility of all despatched parcels and to ensure a proof of delivery signature has been received. The courier company reports include:

- 9:30am – Report automatically generated from the courier systems providing details of every parcel dispatched the previous working day and the current delivery status, and who has signed for the delivery;

- 10:30am – Report providing details regarding exceptions noted during the distribution process. This report does not list a status on each package. The Production Service Team will use this report to notify the NHS Organisations of expected delays or problems being experienced by the courier company; and

- 11:00am-11:30am – Report containing details of the outcome of the delivery of each parcel that was despatched the previous evening. The report will detail whether there was no-one available to receive the parcel or the name of the person who has received the parcel and the time that it was delivered.

All parcels are required to be signed for and the electronic proof of delivery is scanned into the courier company's delivery and tracking system. The Production Service Administration Team has access to the parcel tracking system and is able to view the proof of delivery signature should it require the information.

The Production Services Team maintains internal incident logs in which detected deviations from the existing payslip printing and distribution process are logged.

Payslip related incidents that result in security related issues (e.g. payslip parcels have been delivered to an incorrect address or a damaged package) are logged and managed through the problem and incident management process as documented in sections 3.1 to 3.3. These incidents, along with payslip related incidents that breach SLA, are also reported on in the monthly SLA management report as documented under control objective 3. If payslips are not received within a timely basis, NHS Organisations are encouraged to log incidents through the standard ESR problem management procedures as documented in section 3.3

6. Detailed control objectives and testing performed

Control Objective 1: Change Management

Controls provide reasonable assurance that changes to the system software, hardware, and network components are documented an d approved.

Control ref:	ESR Programme control	PwC Testing Performed	Exceptions noted
1.1 a	Segregation of duties are in place all for application changes to the NHS General Ledger interface. Changes must be tested first by a developer and then approved by the change requestor or production controller, as appropriate, before going live.	For a sample of application changes applied to the NHS General Ledger interface, inspected the corresponding Service Request and/or Amendment Request ticket to determine whether the changes were tested by a developer and then approved by either the change requestor or production controller before going live.	None.
1.1 b	There is a monthly report of all application changes made to the NHS general ledger interface. The report reconciles all changes made in the NHS Hub production environment to the required forms and sign off at each stage the corresponding service amendment and handover requests. Unusual or unauthorised changes which may not be in line with standard process are flagged and a review of report is completed by the team manager with any issues investigated. The monthly report is signed off by NHS team Manager.	For a sample of months, inspected the monthly change reconciliation report to determine whether any unusual or unauthorised changes had been flagged and a review had been undertaken and signed off by the NHS team Manager.	None.
1.1 c	NHS General Ledger Interface application change policies and procedures have been established and are reviewed and updated annually by the head of integration team. The following policies are in use and are reviewed and updated as appropriate on an on-going basis: ESR-NHS0018 – NHS Systems Integration Team Change Control Process.	Inspected the 'ESR-NHS0018 – NHS Systems Integration Team Change Control Process' policy to determine whether it had been reviewed and approved within the year by the head of the integration team.	None.

1.2 a	Application changes to the ESR services are requested by raising a Service Request on the ICD helpdesk system. This is reviewed and approved by the ESR Service Change Advisory Board (CAB) prior to development. Change development can either be done by the Development team or the Design Configuration Team or the Database Administrator Team. Once approved by the CAB, this is then tested by the Testing team prior to live deployment. Once the change has been tested and is ready for release, it is then approved by a Group Manager and the Change Manager or by a Senior Manager (for out of hours). For changes that are impact rated medium or above, CAB approval is also required prior to live deployment.	For a sample of changes applied to ESR, inspected: ● evidence that the change had been tested prior to deployment; and ● the Request For Change ticket change to determine whether it had been reviewed and approved by a Group Manager, Change Manager or Senior Manager or by CAB (if impact rated medium or above) prior to deployment.	None.
1.2 b	ESR Change Process policy and Agile Change policy have been established and are maintained by the ESR Change Management Team. The ESR Change Process policy is reviewed on an annual basis by the Change Manager. The Agile Change policy is reviewed and updated as required by the Change Manager.	Inspected the 'S-2500 Service Change Management policy' to determine whether this had been reviewed by the Change Manager. Inspected the 'EE-25454 – ESR Agile Change Process' document to determine whether this was reviewed by the Change Manager.	None.

1.3 a	System changes to the ESR services are requested by raising a Request For Change (RFC) on Techne. Changes are developed and tested, where applicable, by the supporting teams. This is then be reviewed and approved by the Group Manager and the ESR Change Advisory Board (CAB) or the Change Manger (for low impact changes) or by a Senior Manager (for out of office hours) prior to implementation.	For a sample of changes applied to the ESR services, inspected the completed Request for Change ticket on Techne to determine whether: ● if relevant, these had been tested by the ESR Support team prior to implementation; and ● these have been approved by the Group Manager and the ESR Change Advisory Board (CAB) or the Change Manger (for low impact changes) or by a Senior Manager (for out of office hours) prior to implementation.	None.
1.3 b	Techne is used to manage the authorisation of RFCs and restricts the ability to authorise changes to Senior members of the ESR Programme Team in line with their job responsibility. Segregation of duties are followed whereby no users are allowed to request and approve their own change request.	For a sample of employees that have the ability to authorise and request changes on Techne, inspected their employee records to determine whether access was appropriate and in line with their job responsibilities. For a sample of change request raised on Techne, inspected the RFC ticket to determine whether: ● it was authorised by an appropriate Senior member of the ESR Programme Team; and ● the RFC had been requested and approved by different individuals as appropriate.	None.
1.3 c	Emergency system changes to the ESR services are requested by raising a Request For Change (RFC) on Techne. Emergency Changes are developed and tested, where applicable, by the supporting teams prior to implementation. This will then be reviewed and approved by the Group Manager and the ESR Change Advisory Board (CAB) or by a Senior Manager (for out of office hours) prior to implementation. Where formal authorisation on Techne cannot be obtained prior to implementation, (e.g., when the system is unavailable and immediate action is required to restore availability of the ESR Service), approvals are granted retrospectively.	For a sample of emergency changes applied to the ESR services, inspected the completed Request for Change ticket on Techne to determine whether: ● if relevant, these had been tested by the ESR Support team prior to implementation; ● these have been approved by the Group Manager and the ESR Change Advisory Board (CAB) or the Change Manger (for low impact changes) or by a Senior Manager (for out of office hours) prior to implementation; and ● where authorisation could not be obtained in time, approvals were sought and obtained following the change.	None.

1.3 d	All changes on the Pre-Approved List (PAL) are approved by the ESR Service Change Advisory Board (CAB). A PAL form is completed and signed off by the CAB as evidence of approval. All PAL changes are reviewed at least annually by the CAB.	For a sample of change on the Pre-Approved List (PAL), inspected the PAL form to confirm that it had been completed, signed off by the CAB and reviewed during the year by the CAB.	None.
1.4 a	Access to configure changes in the production environment is restricted to members of the ESR Application Support Team and ESR Production DBA Support Team. No developers have accessed to promote change to the production environment.	Inspected the access configuration on the production environment and confirmed that no developers have privilege access to promote change to the production environment. Observed a development trying to make a change to the prodcution environment unsuccessfully. For a sample of users who can configure changes in the production environment, inspected their employee records to determine whether they are a member of the ESR Application Support Team or the ESR Production DBA Support Team and not a developer.	None.

Control Objective 2: Logical Security

Controls provide reasonable assurance that security configurations are created, implemented and maintained to prevent inappro priate access.

Control Ref:	ESR Programme control	PwC Testing performed	Exceptions noted
2.1 a	The ESR Security Management Plan defines both the security requirements for the ESR Service and the responsibility for security held by the ESR Programme Team and IBM. This document is reviewed on an annual basis by the ESR Information Security Manager and updated as required. A central repository of the ESR policies and procedures is maintained and made available to relevant members of the ESR Programme Team	Inspected the ESR Security Management Plan to determine whether: ● it contained the relevant security policies and procedures; and ● it had been reviewed by the Information Security Manager during the year. Inspected the central repository to determine whether it contained the reviewed ESR Security Management Plan and that relevant members of the ESR Programme Team have accessed to it.	None.
2.2 a	New access to the network, active directory user group, production environment and firewall are approved by the line manager and if applicable by the Gatekeeper (the data owner) prior to access being granted.	For a sample of new/modified ESR application user accounts created in the period under review, inspected: ● the starter approval form to determine whether it was approved by the line manager; and ● the service request ticket raised to provision access to determine whether it was approved by the line manager and if applicable by the Gatekeeper (the data owner) prior to access being granted.	None.
2.2b	The leavers' access to the network, active directory user group, production environment and firewall are revoked on their final day of employment.	For a sample of leavers from the HR listing, inspected: ● the service request ticket to determine whether access was revoked on their final day of employment; and ● the system access log to determine whether no leavers remained had access to the system.	We noted for a sample of leavers that one individual's access was not removed on the final day of their employment. There was a three week delay between the employee leaving and the service request being raised to be removed from the system.

2.3 a	The AIX privilege account passwords are stored and encrypted via the KeePass Safe in a secure network location. The AIX passwords within KeePass cannot be viewed by the user outside of the ESR Technical team.	Inspected the KeePass safe to determine whether passwords to the AIX privilege accounts cannot be viewed by a user outside of the ESR Technical team. .	None.
2.3 b	The password to access the KeePass network location is only known by the ESR Technical Programme Manager (the Leader of the ESR Operations – Technical Infrastructure) and the members of the ESR Technical Team and are updated on a quarterly basis by the ESR Technical Programme Manage	For a sample of quarters, inspected the service request ticket completed to determine whether the password to access the KeePass network location has been updated	None.
2.3 c	Operating system and network password controls are in place and define requirements around the minimum length, periodic expiry and history in line with IBM password policy.	Inspected that AIX Operating system and network password configuration around the minimum length, periodic expiry and history to determine whether they are in line with IBM password policy	We noted that the password configuration in place within the operating systems was not in line with IBM password policy.
2.4 a	Database passwords (including SYS, SYSTEM and APPS passwords) are stored and encrypted via the KeePass Safe in a secure network location. The database passwords within KeePass cannot be viewed by the user outside of the DBA team.	Inspected the KeePass safe to determine whether passwords to the Database passwords (including SYS, SYSTEM and APPS passwords) cannot be viewed by the user.	None
2.4e	The Production database credentials are stored in KeePass. Access to the secure network location where KeePass is stored is reviewed on a quarterly basis against the Resource notifications for 'Leavers and Role Transfers'. Any differences result in a Service Request for Internal Systems to remove access	For a sample of quarters, inspected the review along with the service now tickets to remove any access post the review taking place.	None
2.4 b	The password to access the KeePass network location is only known by the ESR DBA team and are updated on a quarterly basis by the DBA Support Lead.	For a sample of quarters, inspected the service request ticket completed to determine whether the password to access the KeePass network location has been updated	None.

2.4 c	The ESR Production DBA Support Team track patches released quarterly by Oracle. This allows patches that have been applied to be assigned service and changes requests in order to gain assurance that the patch has been applied correctly in line with business processes.	For sample of quarters, inspected: ● the quarterly patched review log to determine whether the review performed by the ESR Production DBA support team had been performed; and ● the service and change request ticket to determine whether the DBA Support team had tracked and applied patches released by Oracle in line with business processes.	None.
2.6 a	On an annual basis, penetration testing is performed to determine whether the firewall ruleset appropriately restricts access. Any issues from the annual penetration testing are recorded and tracked through to resolution. A monthly meeting is held with the Security Privacy and Review Board to discuss and monitor these issues.	Inspected the penetration testing report to determine whether this had been performed during the year and had identified relating any issues related to the firewall configuration. For any issues found, inspected the Security Issues tracker to confirm that it had been logged, investigated and tracked to resolution. For a sample of months, inspected the Security Privacy and Review Board agenda and minutes to determine whether the findings and issues related to the Penetration testing results are discussed and monitored.	None.
2.7 a	GL Interface security policies and procedures have been established and are reviewed and updated annually by the head of the integration team. An NHS Systems Integration Team Support Processes and Security Policy is in existence and defines the security requirements and related procedures for the NHS General Ledger Interface Service. The Policy and associated procedures are reviewed and refreshed as appropriate.	Inspected the following interface policies to determine whether these had been reviewed during the year and defines the security requirements and related procedures for the NHS General Ledger Interface Service: ● ESR-NHS0017 – NHS Systems Integration Team Support Processes and Security Policy. ● ESR-NHS0024 – NHS Hub Security. Inspected the central repository to determine whether it contained the reviewed policies and that relevant members of the NHS ESR Integration team have accessed to them.	None.
2.7 b	If an NHS organisation requires a web service account, a request for user access will need to be raised on the ESR Service desk. All new user access requests to the web service must be validated by a member of the NHS Systems Integration Team.	For a sample of new Web Service user accounts, inspected the Service Request and completed handover form to determine whether it had been reviewed and approved by a member of the NHS Systems Integration Team before access had been granted.	None.

2.7 c (i)	**Applicable for the period of 1 April 2021 - 6 June 2021** Access to the Production area is restricted to a single user account and password. The password is stored on a shared drive within a password protected spreadsheet.	Observed an attempt to access the production account using the access credential of the development account to determine whether the production account cannot be accessed using the development account access credential. Observed an attempt to make a change to the production environment using the share development account to determine whether that it was unsuccessful and that the development and production environment are segregated.	We noted that for the period of 1 April 2021 - 6 June 2021, the shared username and password to the development and production area were stored on password protected Excel files on the ESR team's shared drive. These excel files were unencrypted and hence it was possible for members who had accessed to the team's share drive to brute force the excel password protection and gain access to both the production and development areas' credentials.
2.7 c (ii)	**Applicable for the period of 7 June 2021 - 31 March 2022** Access to the Production area is restricted to a single user account and password. The password is stored and encrypted via a KeePass Safe and cannot be viewed by the user.	Inspected the KeePass safe to determine whether passwords to the Production area cannot be viewed by the user. Observed an attempt to access the production account using the access credential of the development account to determine whether the production account cannot be accessed using the development account access credential. Observed an attempt to make a change to the production environment using the share development account to determine whether that it was unsuccessful and that the development and production environment are segregated.	None.
2.7 d	A report is run annually detailing the last active date of all accounts by the integration team. The report uses a traffic light system highlighting active accounts in green, inactive accounts which they are committed to keeping in orange and accounts that have been inactive for over 24 months in red. All red accounts are investigated by the integration team and any accounts that are no longer in use are removed.	Inspected the annual accounts review report to determine whether all "red accounts" had been investigated during the year. For accounts that are no longer in use, inspected the service request ticket completed to remove these accounts to confirm that it was correctly actioned.	None.
2.8 a	Sophos Sophos Anti-Virus is installed on each part of the TRS infrastructure to protect from malicious software. Relevant Microsoft Security updates and patches are reviewed quarterly and applied to address any weaknesses in the operating system security.	Inspected the TRS servers to determine whether Sophos Anti-Virus was installed. Inspected the TRS servers to determine whether they were covered by Microsoft Windows Server Update Service. For a sample of quarters, inspected the Change Request ticket to determine whether the IBM technical team had tracked and applied patches to operating system security.	None.

2.9 a	New access to the network, active directory user group and the NHS System Integration team network drive are approved by the line manager prior to access being granted. (NHS System Integration team).	For a sample of new/modified NHS System Integration application user accounts created in the period under review, inspected: ● the starter approval form to determine whether it was approved by the line manager; and ● the service request ticket raised to provision access to determine whether it was approved by the line manager prior to access being granted.	None.
2.9 b	Leavers' access to the network, active directory user group and the NHS System Integration team network drive are revoked on their final day of employment. (NHS System Integration team).	For a sample of leavers from the HR listing, inspected the service request ticket to determine whether access was revoked on their final day of employment	None.

Control Objective 3: Problem Management and Performance and Capacity Planning

Controls provide reasonable assurance that system and network processing issues are identified, reported and resolved in a timely manner, and that performance against the SLA/contractual requirements for the ESR service is monitored.

Control Ref:	ESR Programme control	PwC Testing performed	Exceptions noted
3.1 a	Service Level Agreement (SLA) for performance and availability of the ESR Service and network are monitored as part of the monthly SLA meetings held by the NHS Central team to discuss ESR performance against SLA obligations. This review is supported by a Monthly Performance Report prepared by the ESR SLA Manager which is then reviewed and discussed by the NHS Central team during the monthly SLA meeting.	For a sample of months, inspected: ● the monthly Service Management Report to determine whether it provided details of ESR service and network performance against SLA obligations; and ● the SLA meeting minutes to confirm that the Service Management Report was reviewed and discussed by the NHS central team during the meeting.	None.
3.1b	System capacity and performance is monitored (ESR Service). Thresholds for system capacity and performance are in operation and automated alerts are produced where performance below these thresholds is identified. The alert will also trigger within Netcool and a Service Request (SR) will be raised if appropriate for resolution.	Observed for one instance related to system capacity that an automated alert is produced on Netcool if performance fell below a threshold. For a sample of Netcool alerts inspected that these had been invesigtaed to appropriate resolution.	None.
3.2 a	Network capacity and performance is monitored (ESR Service). Thresholds for system and network capacity and performance are in operation and automated alerts are produced where performance below those thresholds is identified. The alert will also trigger within Netcool and a Service Request (SR) will be raised if appropriate for resolution.	Management confirmed that there were no instances of network capacity and performance breach that required a Service Request to be raised and follow up action during the reporting period. Nonetheless, inspected the Network software configurations to determine whether: ● network Monitoring Software are utilised to monitor each server for performance; and ● automated alerts are raised where network thresholds are breached. Inspected the event log from the Network Software to confirm that there were no network capacity and performance breach that required a Service Request to be raised and follow up action during the reporting period.	None.

3.3 a	Incidents are prioritised, investigated and tracked to completion in the ESR Service Desk system (ICD).	Observed that the ICD system was used to log all incidents and problems, including those raised internally and externally and that each was assigned a unique Service Request. For a sample of incidents raised on ICD, inspected the incident ticket to confirm that it had been reviewed and resolved in a timely manner.	None.
3.3 b	Problem tracking and resolution are monitored as part of the monthly SLA meetings held by the NHS Central team to discuss ESR performance against SLA obligations. This review is supported by a Monthly Performance Report prepared by the ESR SLA Manager which is then reviewed and discussed by the NHS Central team during the monthly SLA meeting.	For a sample of months, inspected: ● the monthly Service Management Report to confirm that it provided details of ESR performance against SLA obligations; and ● the SLA meeting minutes to confirm that Problem tracking is monitored and that the Service Management Report was reviewed and discussed by the NHS central team during the meeting.	None.
3.4 a	The availability of the NHS Hub is monitored by the Integration Team, through the use of live admin dashboard during working hours. Issues that cannot be resolved immediately are tracked and resolved via the ESR Service Desk application.	Observed the operation of the NHS GL Hub dashboard to determine whether it monitors progress of files being processed within the Hub. For a sample of issues raised by the Integration team as a result of their monitoring, inspected the Service Request ticket raised on the ESR Service Desk application to confirm that it was tracked and resolved.	None.

Control Objective 4: Physical Security and Environmental Controls

Controls provide reasonable assurance that physical access to controlled areas is restricted to authorised individuals, and that facilities are protected against environmental threats (Warwick & Newcastle Data Centres).

Control Ref:	ESR Programme control	PwC Testing performed	Exceptions noted
4.1 a	Access to the Data Centres can only be gained by passing through a series of access-controlled doors which require the use of an electronic access card.	For both the Warwick and Newcastle data centres, observed that: ● an access card system was in place which was configured so only appropriate staff can access the Data Centres. ● access to the Data Centres could only be obtained using an access card.	None.
4.1 b	New access to the data centres is required to be approved by the data centre door owner or deputy prior to the access being granted.	For a sample of new users requiring access to the data centres, inspected the service request ticket raised and determine whether it had been approved by the data centre door owner or deputy prior to the access being granted	None.
4.1 c	Reviews of access rights to the Data Centre are performed by the data centre door owner to check that only appropriate persons have access to the facility and that their level of access is suitable. Any users found to have inappropriate access to the Data Centre will have their access revoked. For the Warwick data centre this control operates on a quarterly basis. For the Newcastle data centre this control operates twice a year.	Warwick data centre For a sample of quarters, inspected access review evidence to determine whether the access review was performed. For any users found to have inappropriate access, inspected the updated access data centre access list determine whether their access was removed. Newcastle data centre For a sample of bi-annual review, inspected access review report to determine whether the access review was performed. For any users found to have inappropriate access, inspected the updated access data centre access list to determine whether their access was removed.	None.

4.1 d	Leavers' access rights to the data centres are revoked on the final day of employment.	Management confirmed there have been no leavers with access to the data center who had their rights revoked in the period. Nonetheless, inspected a listing of leavers in the period and compared this to access review listings from CO4.1C validate there were no instances in the period.	None.
4.2 a	Maintenance of data centres' equipment and infrastructures are performed in line with the Maintenance agreement and calendar schedule agreed with the third-party Maintenance provider, Apleona.	Inspected maintenance agreements with Apleona to determine whether they are in place for maintenance of the Warwick and Newcastle data centres' equipment and infrastructure. For a sample of planned maintenance work from the agreed maintenance calendar schedule with Apleona, inspected the signed worksheets to confirm that maintenance work over the data centres equipment and infrastructures had taken place.	None.
4.2 b	The backup systems for the power generators within the data centres are tested offline on a monthly basis. They are also tested full load on a quarterly basis.	For a sample of months, inspected the signed engineer worksheets to confirm that power generators were tested offline. For a sample of quarters, inspected the signed engineer worksheets to confirm that full load tests were performed on the data centres power generators.	None.
4.2 c	The Airedale system that controls the temperature within the data centre is checked once a day by the Newcastle Data Centre Operation team and twice a day by the Warwick Data Centre Operator.	Observed on site the temperature and humidity monitoring devices to determine whether they were in place for both the Warwick and Newcastle data centre. For a sample of days, inspected the Operation team daily check sheet to determine whether temperature checks were performed twice a day at the Warwick data centre and daily at the Newcastle data centre.	None.
4.2 d	The Airedale systems are set to trigger an alarm in the data control room if any unexpected changes in temperature or humidity is detected. Priority 1 Issues that cannot be resolved immediately are tracked and resolved via the ICD Service Desk application where it will be passed to the relevant IBM teams for resolution.	Management confirmed that there were no instances temperature or humidity Priority 1 issues raised during the reporting period. Nonetheless, observed the monitoring management where automated alerts would be raised if temperature and humidity thresholds are breached. Inspected the P1 alert log from the monitoring management system to confirm that there were no instances temperature or humidity Priority 1 issues during the reporting period.	None.

4.3 a	Hardware is disposed of in a secure manner to ensure that data loss does not occur. A documented procedure is in place which outlines the process to follow to dispose of media (either hard disks or tapes) when it has been removed from service. All assets that are disposed have all data removed before being passed to a third party for destruction.	Inspected the disposal policy to determine whether a documented procedure is in place which outlines the process to follow to dispose of media (either hard disks or tapes) when it has been removed from service. For a sample of disposed assets, inspected the service request ticket for disposal to confirm that all data removed before being passed to a third party for destruction.	None.

Control Objective 5: Computer Operations

Controls provide reasonable assurance that standardised operating procedures are being followed, processing is appropriately scheduled, authorised and completed, and backups are performed and securely stored.

Control Ref:	ESR Programme control	PwC testing performed	Exceptions noted
5.1 a	Scheduled processes are monitored to ensure that they run to schedule and complete normally. The Concurrent Manager system sends an automatically generated e-mail daily to the Monitoring Team following the completion of scheduled jobs showing the status of the jobs (success/failure). The Monitoring Team also checks all 'National' processes every morning in the daily checks, and hourly using a Netcool patrol metric. Any schedule process failures are investigated by the Monitoring Team or passed to the relevant IBM support team for resolution.	For a sample of days, inspected the daily automated email sent by the Concurrent Manager system to determine whether the completion status of scheduled jobs had been monitored. For any scheduled process failures found, inspected the Service Request raised by the Monitoring Team to confirm that they were investigated or passed on to the relevant IBM support team for resolution.	None.
5.2 a	Backup processes are monitored by staff through the use of the IBM Netcool tool, with failures and errors resulting in an alert. When a new alert is created, staff will assess whether further action is required and, if so, a new Service Request will be raised on the ICD system and assigned to the appropriate team for further investigation and remediation.	For a sample of backup failures from Netcool, inspected these had been assigned to the appropriate team, investigated and resolved as appropriated .	None.
5.2 b	The disaster recovery (DR) plan is tested in a continuous three-monthly performance testing cycle. Within this cycle the DR recovery mechanism is invoked (including recovery from tape backups) and tested multiple times at the DR site in the North East of England.	Inspected the DR Plan to determine whether it exists and contains ESR disaster recovery policies and procedures. For a sample of quarters, inspected the DR testing plan and Baseline Performance Tests report to determine whether DR testing (including recovery from tape backups) had been conducted.	None.

Control Objective 6: Payslip Distribution

Controls provide reasonable assurance that system output is complete, produced on a timely basis and properly distributed to NHS Organisations.

Control Ref:	ESR Programme control	PwC Testing performed	Exceptions noted
6.1 a	All payslip incidents relating to security and timeliness issues raised by the NHS payroll department are logged and managed through the ICD Service Desk application. This involves raising a Service Request with the Service Desk via ICD, which is then investigated and passed to the relevant Support team for resolution.	For a sample of payslip incidents, inspected the Service Request ticket raised on ICD to confirm that the incident had been investigated and resolved.	None
6.1 b	Payslip production & distribution (outsourced to a third party, OPUS) are monitored as part of the monthly SLA meetings held by the ESR SLA Manager with OPUS to discuss performance against agreed KPIs per the SLA with OPUS. The output of these meetings are included with the Monthly Performance Report prepared by the ESR SLA Manager which is also reviewed and discussed by the NHS Central team during the monthly ESR SLA meeting.	Inspected the OPUS contract to confirm that SLAs and Key Performance Indicators (KPIs) had been agreed. For a sample of months, inspected: ● the monthly Service Management Report to confirm that it provided details of OPUS service performance against SLA obligations; and ● the SLA meeting minutes to confirm that the Service Management Report was reviewed and discussed by the NHS central team during the meeting.	None.
6.1 c	On a daily basis, the Production Service Manager performs a reconciliation between the payslip requested for printout and payslip delivered to the recipients. Any discrepancies are investigated by the Production Service Manager or passed to the relevant Support team for resolution.	For a sample of days, inspected evidence to confirm that a reconciliation had been carried out by the Production Service Manager. For any discrepancies found, inspected the Service Request ticket raised to determine whether they were investigated or passed on to the relevant support team for resolution.	None.

7. Additional information provided by ESR

The information contained within this section of the report is out of the scope of the ISAE 3000 controls audit. It has been provided by the management of the ESR Programme, as additional information for NHS organisations users of the ESR Service to provide further context.

Overview

The ESR Service is delivered from a Production Data Centre in Warwick, England. This is backed up by a second Disaster Recovery (DR), Data Centre in Newcastle, England.

To help ensure that the DR solution can be implemented promptly, transactions that are carried out on the ESR Service are recorded in a transaction log. Every 15 minutes, or whenever this log becomes full (whichever is the earlier), the transactions are copied to an archive log which is automatically transferred over the network to the DR Data Centre. At this point the archive logs are then replayed back against the DR System. This approach will result in the DR System being up to approximately one hour behind the main ESR Service.

To facilitate data transmission to the DR Data Centre, Virtual Private Network Tunnels exist over the Sub Service Provider's corporate infrastructure interconnecting the boundaries of the ESR network to form a single virtual ESR Network.

Management consider that a live ESR service could be restored within a matter of hours, should the Production Data Centre become unavailable.

DR Procedures

The principles and procedures around declaring a disaster and invoking the DR solution have been established, documented and rehearsed. The NHS tested both the procedures and the resulting ESR Service during final acceptance testing of the ESR service in November 2008. The following sections expand some principles and established processes to assist a general understanding of the DR solution.

Calling a DR

There are a number of potential incidents that would warrant a DR to be invoked; fire or flooding for example. There are many other possibilities where it will not be clear if the problem can be resolved and service resumed from the Production Data Centre in an acceptable period, therefore informed judgment and agreement are required. A DR will only be invoked with the agreement of both the NHS ESR Programme Director and the Sub Service Provider Programme Director. In the event that a major incident occurs, which is likely to cause the ESR Service or material part of the Service is likely to be unavailable for a period of more than 24 hours, a service will be provided from the DR Data Centre.

If the ESR Service delivered from the Production Data Centre is still operating in some reduced form, consideration will be given to allowing certain payroll activities to complete at the Production Data Centre before invoking a DR. Once a DR has been invoked and DR Cutover has occurred, the ESR Service delivered from the Production Data Centre will be stopped (if it has not already stopped), because further updates would not be included on the transaction archive logs sent to the DR Data Centre and would therefore be 'lost' when the ESR Service is resumed at DR Data Centre.

Dual Path

At the same time as invoking the DR solution the Sub Service Provider will endeavour to recover the ESR Service at the Production Centre. In some circumstances it may be possible to resume service from the Production Data Centre before the DR system has been put into live service.

Resources and Documentation

To enable a Disaster Recovery to be undertaken a team of individuals with appropriate skills and authority needs to be assembled. Suitable individuals and standbys have been identified and contact details documented. In addition, the appropriate documentation has been secured to enable a Disaster Recovery to take place and also for the eventual re-instatement of the ESR Service at the Production Data Centre.

Communications

If a 'disaster' is declared end users will be informed via an e-mail sent to the main contacts at each NHS Organisation and status updates will be provided as regularly as possible. Notifications of this type are also communicated to end users via Twitter and the MyESR App.

The Service Desk will be kept fully up-to-date on the current status so that they can provide relevant information to users contacting them by telephone.

Implications of a DR

The SLA document contains the details of the effect of invoking DR on the restricted service that is offered whilst maintaining the KPIs.

In the event of a local failure at the main production side of the HSCN connection, the Sub Service Provider and the NHS will agree an estimate of the likely duration of the outage. If it is likely that the outage will be longer than 10 core service hours, the Sub Service Provider will invoke the DR process, so as to be 'ahead of the game' if the DR is agreed as the best solution to resume the ESR Service. However, it must be noted that the Sub Service Provider have no responsibility for the availability of HSCN or any of the NHS Organisations' infrastructure; therefore any such failure will not adversely impact the SLA.

ESR Data Warehouse

Overview

In tandem with ESR the ESR Data Warehouse (Warehouse) has been implemented across England and Wales. The Warehouse is a separate database populated by monthly extracts from ESR. The Warehouse has been developed to meet central and strategic reporting requirements and the database contains data to aid strategic decision-making; it is structured to support reporting rather than transactional operations with read only access.

The requirements for the Warehouse were determined through consultation with the DHSC, NHS Digital, NHS Employers, Welsh Assembly, Health Solution Wales, SHAs and Deaneries. Both RoWIN (Review of Workforce Information Needs) and RoBIN (Review of Business Information Needs) were significant contributors to the design. The Warehouse was built to allow for central collection of the following reports, which were current at the time of design:

- Medical and Dental workforce census;
- Non-Medical workforce census;
- NHS Earnings survey;
- Nursing campaign return;
- Vacancy survey of NHS Organisations;

- Planning Extract (Deanery data on Specialist registrars);

- Junior Doctors Hours return (partially); and

- Monitoring Executive Board Member Gender and Ethnicity and staff PDPs.

The Data Warehouse User Group was consulted during the design and development stage of the warehouse and the user group participated in the testing of the Warehouse before it went live.

The Warehouse offers huge strategic benefits. Now that all NHS Organisations are using the ESR Service (with the exception of two organisations) Trusts no longer need to provide certain workforce related data themselves.

For instance from 2010 data for the Medical and Non-Medical Workforce Censuses was extracted directly from the Warehouse; this decision was made by NHS Digital on the basis of ongoing data quality processes and their ability to run monthly reports enabling more timely analysis of significant data changes or quality issues. This new approach to the Census has brought about significant cost benefits along with more timely publication of data and a reduced burden on the source organisation.

Using the one system provides a greater consistency of information across NHS Organisations. Benefits include:

- Access at national and supra-Trust level to a single database designed to meet central and strategic reporting requirements for statistical reporting and planning purposes;

- Streamlined reporting arrangements in which data is input once in the ESR Service and then used to populate the Warehouse to cater for multiple reporting purposes; and

- Improved accuracy, timeliness and consistency of data and provision of a rich data set for reporting:

    - Reduced effort is required to meet the national and supra-Trust reporting requirements. Direct central production of consolidated workforce returns currently requested from individual NHS Organisations from national and supra-Trust organisations.

    - Direct production of the Medical and Non-Medical Workforce censuses previously requested from individual NHS Organisations.

One benefit of an integrated workforce solution is that employee information related to payroll has to be available and correct for staff to be paid accurately. As with all databases the data in the Warehouse relies on people entering the correct details into ESR in the first place. The use of managed List of Values, Validation Masks, and a process for data quality reporting on key data items however, does help to ensure that the Warehouse remains fit for purpose.

Rollout

Full implementation and population of the Warehouse was achieved in June 2008. Those NHS Organisations that are able to access the Warehouse are:

- The Health and Social Care Information Centre;

- NHS Wales Informatics Service (Following the April 2013 restructuring this will be the NHS Wales Shared Services Partnership (NWSSP));

- NHS Employers;

- Health Education England;

- Deaneries;
- Department of Health and Social Care;
- Welsh Government;
- Skills Academy for Health - Core Learning Unit (restricted to summary level data access); and
- Care Quality Commission.

Security of Access

Access to the Warehouse, and the security profile allocated to users is based on individual business requirements. The type of data held in the Warehouse was originally derived from reporting requirements identified through ROWIN (Review of Workforce Information Needs) and ROBIN (Review of Business Information Needs) reviews carried out by the NHS in conjunction with the DHSC with subsequent changes agreed by the Data Warehouse User Group.

The organisations and data items which any user has access to is restricted by the User Profile allocated to their Warehouse account; for instance:

- Up to 31 March 2013, Strategic Health Authorities (SHAs) could view workforce data for England for all staff groups. From 1 April 2013, this role will be transferred to Health Education England (HEE), when the SHAs cease to exist.
- At National level. NHS Digital and NHS Wales Informatics Service (NWIS) have two security profiles; medical and non-medical (note that from 1 April 2013, NWIS will be replaced by NHS Wales Shared Services Partnership (NWSSP)). The non-medical security profile for NHS Digital enables a view of workforce data for England for non-medical staff groups. For person items, they have the same view as SHAs (or HEE from 1 April 2013); date of birth and national insurance number only. They cannot view surname and forename. The Medical and Dental security profile is allocated to the appropriate teams within NHS Digital and NWIS/NWSSP (from April 2013) in line with Data Protection Requirements. The profile enables a view of workforce data for England (NHS Digital) or Wales (NWIS/NWSSP from April 2013) for medical and dental staff group only. This view includes person items, date of birth, national insurance number, forename and surname. This replicates current workforce collection for the Medical and Dental census. Two security profiles were recently added to allow organisations that do not report to the DHSC or Welsh Assembly to have their data excluded from the DW views that can be accessed centrally.
- The Deanery security profile limits the view to the medical training grades, for these grades they can view person items; date of birth, national insurance number, forename and surname. This view replicates their current data collection.

Applicability of other information in this report to the Data Warehouse

The Warehouse is maintained at the Warwick Data Centre. Data is ‘fed’ into the Warehouse directly from the ESR Production Environment according to a published schedule.

The Data Warehouse does not fall within the scope of this report.

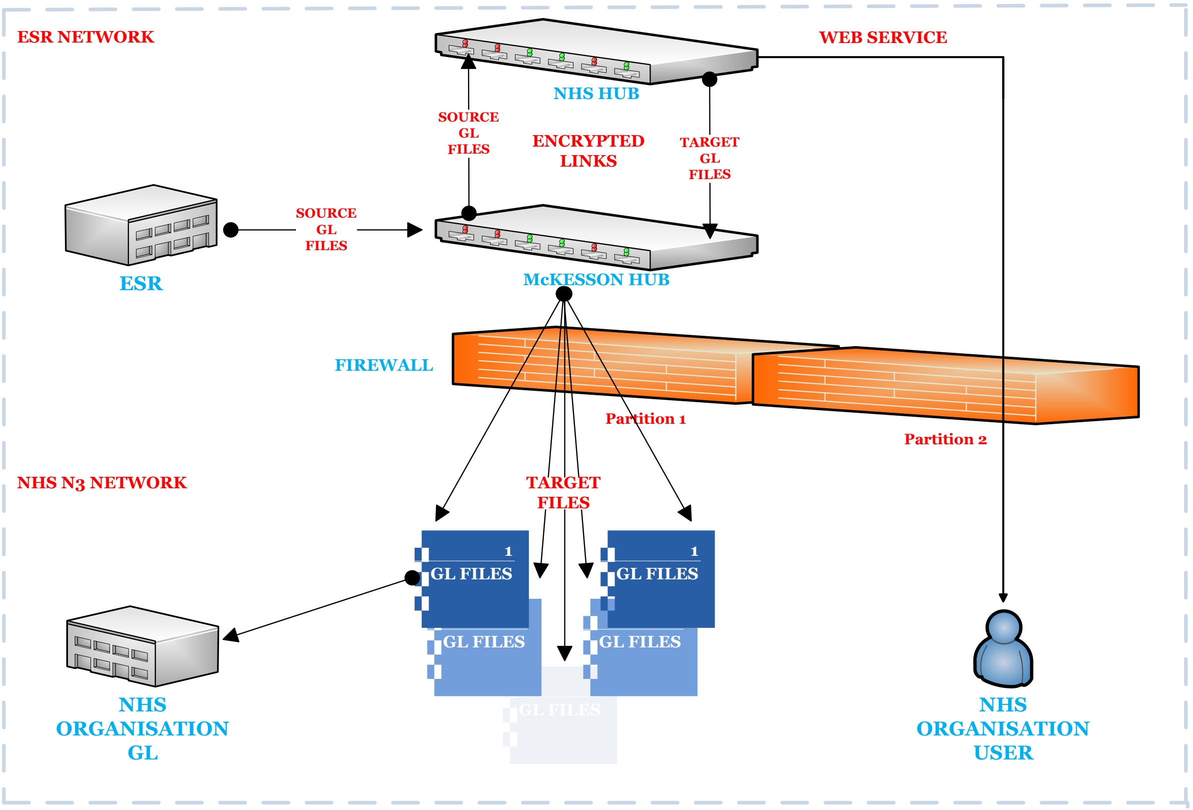
Overview of the General Ledger (GL) Interface

The NHS Systems Integration Team provides an additional service to NHS organisations in relation to reformatting of GL Interface files from within ESR, so that they can be imported into individual GL applications. This functionality is known as ‘NHS GL Interface Processing’. Functionality to reformat GL interface files is available within the ESR application, and is referred to as ‘ESR Mapping’. This functionality is available to all

NHS Organisations; however some organisations choose to perform this reformatting outside of the ESR application.

Both the ESR Mapping functionality and the NHS GL Interface Processing functionality allow NHS organisation users to make changes to the account mapping of the GL balance sheet account codes produced by the ESR application, to the NHS Organisation's specific chart of accounts within their GL systems. The diagram overleaf provides an illustration of the NHS GL Interface Processing process.

NHS GL Interface Processing process:



NHS GL Interface Processing is initiated by NHS organisation users through the ESR application as part of payroll processing. This initiates an automated job to send Source files (containing ESR GL data for that particular organisation) from ESR to the NHS Hub (a separate computer in the ESR network).

Data is transferred to and from the NHS Hub via a network device known as the Hub. The Hub transfers source files from ESR to the NHS Hub for processing, and transfers processed files (target files) from the NHS Hub to the relevant NHS organisations. The transfer of files between ESR, the Hub and the NHS Hub occurs over a secure encrypted link.

Upon receipt of source files by the NHS Hub, the files are processed and converted from source files to target files that meet the particular NHS organisation's requirements. Processed target files are collected by the Hub regularly during the day via secure and encrypted links and are then transferred to the relevant NHS organisations for import into their GL system.

7.1 Exceptions and Management Response

The purpose of this section is to provide an overview of the relevant exceptions noted and also to document the responses to these exceptions by management. The controls presented in Section 5 and Section 6 are those that NHS BSA believes are relevant controls and do not extend to controls in effect at user organisations. It is each interested party's responsibility to evaluate this information in relation to the internal controls in place for user entities.

Control ref:	ESR Programme control	Exceptions noted	Management Response
2.7 c (i)	**Applicable for the period of 1 April 2021 - 6 June 2021** **Access to the Production area is restricted to a single user account and password. The password is stored on a shared drive within a password protected spreadsheet.**	We noted that for the period of 1 April 2021 - 6 June 2021, the shared username and password to the development and production area were stored on password protected Excel files on the ESR team's shared drive. These excel files were unencrypted and hence it was possible for members who had accessed to the team's share drive to brute force the excel password protection and gain access to both the production and development areas' credentials.	This exception was raised late April 2021 and noted in FY20/21 ISAE report. The Authority Central Team subsequentially carried out a procurement exercise to obtain a password protection solution. The procurement exercise was completed during May 2021 and the solution was implemented and went live on 7th June 2021.
2.2b	**The leavers' access to the network, active directory user group, production environment and firewall are revoked on their final day of employment.**	We noted for a sample of leavers that one individual's access was not removed on the final day of their employment. There was a three week delay between the employee leaving and the service request being raised to be removed from the system.	This was a sub-contractor from the Security Business Unit, who support ESR. The resource had no access to ESR and only worked on the QRadar system for DCT project work. The delay in this case was due to leave over the Christmas period but there was no ESR access to remove.
2.3c	**Operating system and network password controls are in place and define requirements around the minimum length, periodic expiry and history in line with IBM password policy**	We noted that the password configuration in place within the operating systems was not in line with IBM password policy.	The AIX and Linux systems have a password limitation, however access to these systems is via a system that is has the compliant password length. There is an account level risk to manage the AIX/Linux system settings, these are being tracked with the vendors, and there are plans to change in the future.

8. Other Information Provided by the Service Auditor

This report on the controls surrounding ESR is intended to provide interested parties with information sufficient to understand the controls in place at ESR and its subservice provider IBM UK Ltd.

This report, when combined with an understanding of the internal controls in place at client locations and at other clients' agents, such as custodians, is intended to permit an evaluation of the controls surrounding the ITGC services in place for ESR's customers.

The review of ESR's controls was restricted to the overview in Sections 4 and5 and the control objectives and the controls set forth by ESR in Section 6 of this report that PwC believes are the relevant control objectives and controls, and was not extended to procedures in effect at customer or other service or subservice organisation locations. It is each interested party's responsibility to evaluate this information in conjunction with user controls in place for each client and other client controls to assess the overall internal control. If an effective client internal control is not in place, ESR's controls may not compensate for its absence.

The objectives of internal controls are to provide reasonable, but not absolute, assurance as to the reliability of financial records for maintaining accountability for assets. The concept of reasonable assurance recognises that the cost of a control should not exceed the benefits derived and also recognizes that the evaluation of these factors necessarily requires estimates and judgments by management.

As part of the review of ESR's controls, a variety of tests were performed, each of which provided different levels of audit satisfaction. The combined results of these tests provided the basis for understanding the controls and whether the controls surrounding the ESR process that ESR represented as placed in operation were actually designed, in place and operating effectively for the period from 1 April 2021 to 31 March 2022.

The control environment represents the collective effect of various factors on establishing, enhancing or mitigating the effectiveness of specific controls. In addition to the specific tests described below, our procedures included tests of, or considered the relevant elements of ESR's environment including:

- NHS BSA ESR's organisational structure and approach to segregation of duties;
- Management control methods;
- Personnel policies and practices; and
- Departments with oversight functions

The tests of the control environment included the following procedures, to the extent considered necessary: (1) a review of ESR's organisational structure, including the segregation of functional responsibilities, policy statements, accounting and processing manuals and personnel policies; (2) discussions with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying control activities; and (3) observations of personnel in the performance of their assigned duties.

The control environment was considered in determining the nature, timing and extent of the testing of controls relevant to the achievement of the assessment criteria.

The tests of the operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls and the extent of compliance with them, are sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period from 1 April 2021 to 31 March 2022. The testing of the operating effectiveness of controls was designed to cover a representative number of transactions and controls throughout the period from 1 April 2021 to 31 March 2022, for each of the controls listed in the matrices in Section IV, which are designed to achieve the specified control objectives.

In selecting particular tests of the operating effectiveness of controls, the following were considered: (a) the nature of the items being tested; (b) the types and availability of evidential matter; (c) the nature of the control objectives to be achieved; (d) the assessed level of control risk; and (e) the expected efficiency and effectiveness of the test.

Tests performed over the operating effectiveness of the control activities were performed on a judgmental basis and are described below:

Tests	Description
Inquiry (Corroboration)	Inquired of appropriate personnel. Inquiries seeking relevant information or representation from personnel were conducted to obtain, among other factors: **a.** Knowledge and additional information regarding the control, policy or procedure; and **b.** Corroborating evidence of the control, policy or procedure. As inquiries were performed for substantially all controls, the test was not listed individually for every control shown in the matrices in Section IV.
Observation	Observed the application or existence of specific controls as represented.
Inspection / Examination	Inspected documents and records indicating performance of the control. This may include: • Examination of source documentation and authorizations to verify propriety. • Examination of documents or records for evidence of performance, such as existence of initials or signatures. • Examination of documentation, such as operations manuals, flow charts, job descriptions and user profiles.
Reperformance	Reperformed the control or processing to determine the accuracy of its operation, including obtaining evidence of the arithmetical accuracy and correct processing of transactions by recomputing the application computation.

The sample sizes that have been applied in testing control procedures, depending on the frequency the control is applied and the assessed level of control risk are set out in the table below:

Frequency of control	Number of items tested
Annual	1
Quarterly	2
Monthly	2, 4, 5
Weekly	5, 10,15
Daily	20, 30, 40
Multiple times per day	25, 45, 60

The report in Section II includes the following statement:

‘While the controls and related control objectives may be informed by the Service Organisation’s need to satisfy legal or regulatory requirements, our scope of work and our conclusions do not constitute assurance over compliance with those laws and regulations.’

In addition, while the controls and related control objectives in this report may include some aspects of measures taken by management to protect operations supporting ESR against cyber-attacks, the scope of the work and the conclusions do not constitute general assurance over the adequacy of the cybersecurity or resiliency measures implemented.

Had we performed additional procedures or had PwC performed an assurance engagement specifically in respect of the Service Organisation’s compliance with specific regulations (for example, CASS, AML, KYC etc), or the adequacy of cybersecurity or resiliency measures implemented, other matters might have come to the attention that would have been reported.