The Regulation and Quality Improvement Authority

Independent Safeguarding Authority

Memorandum of Understanding

between the

Independent Safeguarding Authority

and

The Regulation and Quality Improvement Authority (RQIA) Northern Ireland

on the sharing of information under SVG (NI) Order 2007

The Regulation and Quality Improvement Authority

Independent Safeguarding Authority

TABLE OF CONTENTS

1. PARTIES TO THE MoU

The partners to this agreement are:

Independent Safeguarding Authority (ISA)
PO Box 181
Darlington
DL1 9FA

and

The Regulation and Quality Improvement Authority (RQIA)
9th Floor
Riverside Tower
5 Lanyon Place Belfast
BT1 3BT

This document is jointly owned by Adrian McAllister, Chief Executive of the ISA and Glenn Houston, Chief Executive of the RQIA.

2. TERM OF AGREEMENT

The agreement incorporates the duties and principles of information sharing between the ISA and RQIA that took effect from 12 October 2009. Any future changes in policies will be reflected when appropriate in this agreement and will follow the agreed change process as detailed below.

The agreement will be reviewed on an annual cycle from the last date of approval to negotiate any required changes or confirm the agreement is still valid. A significant change to VBS policy or legislation impacting on the Memorandum of Understanding (MoU) will also trigger a review. The review will be conducted jointly by the ISA and RQIA officers named in the MoU as responsible for the MoU.

If following review, no changes are required this will be confirmed by the ISA and RQIA officers responsible for the MoU. A review date will be set for a further year's time.

If following review, only minor changes are required, the changes will be agreed by the ISA and RQIA officers responsible for the MoU. The MoU will be amended and a review date set for a further year's time.

If following review, major or significant changes are required, for example to the information flows, then the changes will be agreed by the ISA and RQIA

officers responsible for the MoU and confirmed by the Chief Executive (or officer nominated by the Chief Executive) of the respective organisations. The MoU will be amended and a review date set for a further year's time.

The frequency of reviews may be altered by agreement of the ISA and RQIA

3. PURPOSE OF MoU

This Memorandum of Understanding (MoU) provides a framework for sharing information between the ISA and RQIA.
The overall aim of the MoU is to ensure that information is legally and appropriately shared in the interests of safeguarding children and vulnerable adults. In particular to:

- Promote co-operation between the ISA and the RQIA staff at an operational level and in the conduct of their respective statutory duties;
- Facilitate an effective and efficient sharing of information within existing legal powers and constraints concerning safeguarding children and vulnerable adults; and to
- Promote consultation on matters of mutual interest to improve ISA and the RQIA performance in meeting their respective statutory duties and corporate objectives.

4. SCOPE OF MoU

This MoU covers the means by which data will be transferred and the agreed process around that duty in accordance with the phased implementation of the VBS.

5. BACKGROUND

The Independent Safeguarding Authority (ISA) is a Non Departmental Public Body established under Section 1 of the Safeguarding Vulnerable Groups Act 2006. The core purpose of the ISA is to prevent unsuitable people from gaining access to children or vulnerable adults through work or volunteering opportunities.

In 2004 Sir Michael Bichard produced a report that looked at the events leading up to the murder of Holly Wells and Jessica Chapman. In all, Sir Michael made 31 recommendations, mainly around information retention and sharing. Recommendation 19 of that report led to the creation of the VBS and stated "*New arrangements should be introduced requiring those who wish to work with children, or vulnerable adults, to be registered. This register [...] would confirm that there is no known reason why an individual should not work with these client groups. The new register would be administered by a central body, which would take the decision, subject to published criteria, to approve*

or refuse registration on the basis of all the information made available to them by the police and other agencies."[1]

The Regulation and Quality Improvement Authority (RQIA) is the independent body responsible for monitoring and inspecting the availability and quality of health and social care services in Northern Ireland, and encouraging improvements in the quality of those services. Our role is to ensure that health and social care services in Northern Ireland are accessible, well managed and meet the required standards. We will work to ensure that there is openness, clarity and accountability in the management and delivery of all these services. RQIA was established under The Health and Personal Social Services (Quality, Improvement and Regulation) (Northern Ireland) Order 2003. The Order also places a statutory duty of quality upon health and social care organisations, and requires the DHSSPS to develop standards against which the quality of services can be measured.

What the RQIA do:

RQIA registers and inspects a wide range of health and social care services. Our inspections are based on minimum care standards which will ensure that both the public and the service providers know what quality of services is expected.

Our inspectors visit a range of services including nursing, residential care and children's homes to examine all aspects of the care provided, to assure the comfort and dignity of those using the facilities, and ensure public confidence in these services. We are also responsible for the regulation day care settings, domiciliary care agencies, nursing agencies and a range of independent health care services.

RQIA also has a role in assuring the quality of services provided by Health and Social Care (HSC) Board, HSC trusts and agencies, to ensure that every aspect of care reaches the standards laid down by the Department of Health, Social Services and Public Safety and expected by the public.
Under the Health and Social Care (Reform) Act (NI) 2009, RQIA undertakes a range of responsibilities for people with a mental illness and those with a learning disability. These include: preventing ill treatment; remedying any deficiency in care or treatment; terminating improper detention in a hospital or guardianship; and preventing or redressing loss or damage to a patient's property.

Click here to view www.opsi.gov.uk/si/si2003/20030431.htm and www.rqia.org.uk to view more information about RQIA and its functions.

[1] The Bichard enquiry 2004

6. PHASING

12 October 2009

From 12 October 2009 all regulated activity providers; personnel suppliers; local authorities; HSC bodies; education and library boards; keepers of registers and supervisory authorities as set out in the 2007 Order[2] are under a duty to provide information to the ISA in certain circumstances. There is also a power for local authorities; HSS bodies; education and library boards; keepers of registers and supervisory authorities to provide information where relevant conduct occurred prior to 12 October 2009. For more information on these duties and powers see the ISA's website guidance http://www.isa-gov.org.uk

These information sharing protocols will ensure that relevant information will be held and available where it can best be used to protect children and vulnerable adults.

7. INFORMATION SHARING

The responsibilities relating to the duties and powers are defined within legislation and as such must be adhered to. This section provides, in detail, the requirements for information flows that will be undertaken between both parties and proposed future information flows.

Where there is a duty to disclose information section 35 of the Data Protection Act 1998 becomes relevant. This provides that "Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment".

7.1. Transitional Arrangements from 12 October 2009

The ISA will, at the request of the RQIA, inform the RQIA if an individual, for whom they have a legitimate interest, is included on the PoCA list, PoVA list, List 99 or the ISA barred lists. The requirement is RQIA must have a legitimate interest in knowing. The RQIA will have a legitimate interest where:

- The RQIA has made a referral and asked to be informed of the outcome;
- The RQIA has asked for a person's barred status and the person is engaged in, or was engaged in an activity for which the RQIA has responsibility;
- The RQIA has asked for a person's barred status and that person is or was engaged by an organisation for which the RQIA has sector responsibility.

[2] Keepers of registers are listed in the 2007 Order art 43(7) and supervisory authorities at art 47(7) of the Order

- The RQIA has asked for a person's barred status and the person is on their register, or under consideration for their register

Where the request has been made by the RQIA ISA will:

- If the case is concluded and a decision is taken to include the person in a barred list, provide barred status and the date of the decision
- If the case is concluded and a decision is taken not to include the person in a barred list provide barred status and the date of the decision
- If the case is under consideration we will confirm their legitimate interest has been linked to the individual and confirm will be in contact once a decision is available
- If ISA have no information about the named person we will confirm the person is not barred but provide no date of decision

The Department of Health, Social Services and Public Safety (DHSSPSNI) may, at the request of a person with a legitimate interest inform that person if an individual is included in the Disqualification from Working with Children (DWC) (NI) List or the Disqualification from Working with Vulnerable Adults (DWVA) (NI) List

The Department of Education (DENI) may, at the request of a person with a legitimate interest, inform that person if an individual is included in the Unsuitable Persons list.

8. RESPONSIBILITIES & GUIDANCE

8.1. Duty to provide information on request

Article 48 SVG (NI) Order 2007

If the ISA is considering whether to bar an individual or remove an individual from a barred list it may require RQIA to provide it with any prescribed information it may hold on an individual. RQIA must provide this information.

The information to be referred is outlined in paragraphs 1, 2, 3, 5, 6, 9 and 10 of the Schedule to the Safeguarding Vulnerable Groups (Prescribed Information) Regulations (Northern Ireland) 2009 (See Appendix 2: Prescribed Information).

8.2. Duty to Make Referrals to the ISA

Article 47 SVG (NI) Order 2007

Introduction

1. This guidance for the RQIA is intended to provide further clarification in relation to the duty on the RQIA to refer information to the Independent Safeguarding Authority (the ISA) under article 47 of the SVGO.

2. This guidance is designed to assist the RQIA to interpret the provisions of article 47 of the SVGO and to clarify the ISA's expectations in relation to the duty to refer.

Historical cases

3. Article 47(5) of the SVGO confers a power, rather than a legal duty, for the RQIA to refer any cases of 'relevant conduct' occurring prior to the commencement of the new referral duties on 12 October 2009. The RQIA may, in the interests of safeguarding children or vulnerable adults, refer information to the ISA in relation to 'relevant conduct' occurring prior to 12 October 2009.

4. While it is up to the RQIA as to how they may wish to exercise the power in article 47(5), the ISA provides the following non-mandatory guidance to assist the RQIA in considering the application of this power:

a. The ISA does not expect the RQIA to conduct a lengthy or onerous 'trawl' of previous cases to identify 'relevant conduct' cases for referral to the ISA under these provisions.

b. The RQIA should consider for referral, current cases that involve conduct prior to 12 October 2009 that would be considered 'relevant conduct' if the conduct occurred after 12 October 2009.

c. For completed cases with extant sanctions, the RQIA should focus on high risk cases involving harm or risk of harm to a child or a vulnerable adult where the RQIA thinks the ISA may consider barring the person. This includes old cases with sanctions that are re-considered and a decision taken to leave the sanctions in place, where there are safeguarding risks for a vulnerable group.

d. The ISA would not expect the RQIA to consider closed cases with no extant sanctions for referral to the ISA under this provision, unless there are exceptional circumstances involving risk of harm to a vulnerable group.

e. The RQIA should also consider the following criteria in determining the 'appropriateness' of making a referral to the ISA:

i. What specifically is the person deemed to be at risk of doing (i.e. what behaviour?) and how does this link to harm or risk of harm to a child or vulnerable adult?

ii. What impact does the sanction imposed by the RQIA have on the risk of harm outside the regulated setting? Does the action taken by the RQIA remove the risk of harm to children and vulnerable adults, or is there an ongoing risk?

iii. What are the chances of the behaviour being repeated against a vulnerable group and/or is the behaviour likely to escalate?

iv. What is the likely level of harm if it does?

8.3. Article 47 – duty to refer

Referral trigger points – the first condition criteria

Auto Bar

5. For autobar cases, the legal duty to refer information to the ISA arises at the point at which the RQIA receives formal notice of a conviction or caution in relation to an autobar (or connected) offence. A full list of Autobar offences can be downloaded from the ISA website

Relevant conduct

6. For relevant conduct cases, the ISA wish to receive RQIA referrals after one of the following actions has been taken by the RQIA, **and** where the RQIA considers that the relevant conduct criteria within article 47 are met:

a. the RQIA has made a substantive adverse finding of fact;

b. where a person for whom the RQIA hold relevant information has accepted a warning or undertakings;

c. the RQIA has made a decision not to permit an individual to undertake regulated activity.

7. If a referral is made earlier than these points, unless the ISA holds other relevant safeguarding information, the ISA may not be able to progress the case until the RQIA can provide further information following one of the above actions being taken.

The Harm Test

8. In relation to the Harm Test, the first condition of the referral duty arises when the RQIA has sufficient compelling evidence that the registrant poses a risk of harm to children and vulnerable adults such that ISA may bar the person from working with children and vulnerable adults. For clarity sufficient compelling evidence may include (but is not limited to) the following information:

a. Evidence from a foreign court or police service of a criminal conviction or caution in relation to a criminal offence;

b. A determination received from an overseas organisation; or

c. An outcome of an investigation completed by a reputable employer or any other similarly authoritative substantiated evidence from a reputable source.

9. In relation to the endangerment component of the Harm Test limb of the first condition, the endangerment, or risk of endangerment must relate specifically to children and or vulnerable adults as defined by the SVGO. For clarity, the Harm Test criteria will not be met where there is only general endangerment (or risk of endangerment) to persons other than children and or vulnerable adults as defined by the SVGO.

10. Referrals made to ISA should be double wrapped and sent by Registered Mail to the ISA address in section 9 Contact Points – COST

11. It is agreed that the Harm Test should only be used for cases which do not meet the relevant conduct or relevant offence criteria. Normally, the Harm Test is likely to be applied where a person has communicated something in his/her thoughts, beliefs or attitudes that indicate a future risk of harm directly in relation to children and/or vulnerable adults. For example, a person who tells a colleague that he/she is sexually attracted to children but there is nothing in the person's conduct that meets the relevant conduct referral criteria and they have not been cautioned or convicted for a relevant offence.

12. The Harm Test will only be satisfied where there is sufficient compelling evidence to suggest a person poses a direct risk of harm to children or vulnerable adults. The Harm Test will not be met in cases where there is only a general risk of harm – for instance a case of football violence where one adult harms another, indicating risk of harm to people in general rather than a direct risk of harm to vulnerable groups.

13. The RQIA should also consider the following criteria in determining the 'appropriateness' of making a referral to the ISA:

a. What specifically is the person deemed to be at risk of doing (i.e. what behaviour?) and how does this link to harm or risk of harm to a child or vulnerable adult?

b. What impact does the sanction imposed by the RQIA have on the risk of harm outside the regulated setting? Does the action taken by the RQIA remove the risk of harm to children and vulnerable adults, or is there an ongoing risk?

c. What are the chances of the behaviour being repeated against a vulnerable group and/or is the behaviour likely to escalate?

d. What is the likely level of harm if it does?

Application of the second condition criterion

The first limb of the second condition

14. The first limb of the second condition, at article 47(4)(a) of the SVGO requires the RQIA to consider whether the person is engaged or may engage in regulated or controlled activity. The first limb of the second condition will also be satisfied if the person was engaged in regulated or controlled activity at the time the relevant conduct occurred.

15. For clarity, the first limb of the second condition will be satisfied even if at the point the RQIA establishes that the relevant conduct occurred, the person has been removed from regulated activity by virtue of a sanction imposed by the RQIA.

The second limb of the second condition

16. The second limb of the second condition, at article 47(4)(b) requires the RQIA to consider whether the ISA may consider it appropriate to bar the individual. The second condition will not be met in cases solely concerning professional issues which do not raise wider safeguarding issues for vulnerable groups.

17. The second limb of the second condition will be met where 'non-professional' safeguarding concerns for vulnerable groups are present (such as sexual or violent behaviour) or where the individual may be unsuitable to work with children or vulnerable adults in the future because they have demonstrated such a callous disregard for procedure that if repeated outside a professional setting would put children or vulnerable adults at risk.

18. The duty to refer as specified in art. 47 of the SVGO do not apply if the RQIA is satisfied that the ISA already has the information.

9. CONTACT POINTS

ISA CONTACT POINTS

The ISA Central Operations Support Team (COST) will be the principal point of contact regarding the day to day operation of the content of this agreement.

Contact type	Job Role	Name	Contact method
General day to day queries and postal contact for all correspondence	Central Operations Support Team	COST	Central Operations Support Team Independent Safeguarding Authority Post Office Box 181 Darlington DL1 9FA isadispatchteam@homeoffice.gsi.gov.uk 01325 953759
Officer Responsible for MoU	Policy & Partnerships Manager	Scott Postlethwaite	scott.postlethwaite@isa.gsi.gov.uk 01325 953748
Escalation contact	Head of Operations	Anne Hunter	Anne.hunter16@homeoffice.gsi.gov.uk 01325 953875
Security contact	Security Manager	Samuel Hehir	Samuel.hehir@isa.gsi.gov.uk 01325 953744
Data protection & Freedom of information contact	DP & FOI officer	Haydn Rees Jones	Haydn.reesjones@isa.gsi.gov.uk 01325 953743

RQIA CONTACT POINTS

John Black will be the principal point of contact regarding the day-to-day operation of the content of this agreement.

Contact Type	Job Role	Name	Contact method
General day-to-day queries and Postal contact for all correspondence	Head of Programme	John Black	028 905 17450 John.Black@rqia.org.uk
Officer Responsible for MoU	Director of Operations	Phelim Quinn	028 905 17440 Phelim.Quinn@rqia.org.uk
Escalation contact	Director of Operations	Phelim Quinn	028 905 17440 Phelim.Quinn@rqia.org.uk
Security contact	Director of Corporate Services	Maurice Atkinson	028 905 17480 Maurice.Atkinson@rqia.org.uk
Data protection & Freedom of information contact	Head of Information	Sandra McElhinney	028 905 17486 Sandra.McElhinney@rqia.org.uk

The Regulation and Quality Improvement Authority

Independent Safeguarding Authority

10. AUTHORISATIONS

On behalf of the ISA

Name Adrian McAllister

Role within organisation Chief Executive Officer

Signature _____

Date 20/2/12

On behalf of the RQIA

Name Glenn Houston

Role within organisation Chief Executive

Signature _____

Date 20/2/12

Appendix 1: Security and Risk Audit assurance

Introduction

The Independent Safeguarding Authority is committed to protecting children and vulnerable adults, across the whole of the UK in terms of information sharing, but specifically within the English, Welsh and Northern Ireland framework in compliance with the Safeguarding Vulnerable Groups Act 2006 and Safeguarding Vulnerable Groups (NI) Order 2007. It seeks to implement fast and fair decisions; and in achieving these Strategic Objectives it will be heavily reliant on its information.

The ISA's information is its corporate memory, providing evidence of actions and decisions and representing a vital asset in support of its daily functions and operations. Information supports policy formulation and managerial decision-making, protects the ISA's interests and the rights of stakeholders including applicants, staff and those members of the public who have dealings with it. It supports consistency, continuity, efficiency and productivity and helps us and our partners deliver services in consistent and equitable ways.

Being a corporate and not a personal asset, information needs to be properly managed and maintained as it has a value that changes over time. The Home Office has devised a set of 6 Information Management principles which set out how its integrity and value are to be protected; these are: Corporate Responsibility, Quality, Skills, Access, Value for Money and Security, and they form an overarching framework for the formulation of policies by the Home Office's executive agencies and non-departmental public bodies such as the ISA.

The Home Office and its Agencies create, use and store large amounts of information in both paper and electronic formats - although the clear trend now is towards the greater use of electronic working (e.g. email, file-sharing etc) for the conduct of business, resulting in growing volumes of important information being held electronically; however, all material which is disclosable under the Data Protection and Freedom of Information Acts needs to be properly managed to ensure its maximum utility to the Agency as well as safeguarded from loss, unauthorised disclosure or alteration.

Information created or used by the ISA are Public Records under the Public Records Acts (notwithstanding data exempt under the Data Protection Act 1998) and must be compliant with the relevant legislation and guidelines (see point 4 of this section) and managed in accordance with the relevant information management principles.

Objectives, Aim and Scope

Objectives

The objectives of the controls in this section are to preserve:

- **Confidentiality** - Access to Data must be confined to those with specific authority to view the data on a need to know basis.
- **Integrity** – Information is to be complete and accurate. All systems, assets and networks must operate correctly, according to management approved specification.
- **Availability** - Information must be available and delivered to the right person and/or system, at the time when it is needed.

Aim

The aim of this section is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the organisations receiving ISA data by:

Ensuring that organisations are aware of and fully comply with the relevant legislation.

- Describing the principals of security and explaining how they must be implemented in the organisation.
- Introducing a consistent approach to security across the safeguarding community, ensuring that all organisations fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for information security as an integral part of the day to day business.
- Protecting information assets within the organisation that support ISA data.

Scope

This section applies to all ISA information and organisations' information systems, networks, applications, locations and users accessing and/or processing ISA information.

Responsibilities for Security

Ultimate responsibility for security rests with the Chief Executive of the organisation.

- The organisation should appoint an ISA Data Guardian (IGD) who must be responsible for the security of day to day handling of ISA data within the organisation and safeguarding information received from and/or sent to the ISA.

- The organisation must ensure that their permanent and temporary staff and contractors are aware of:-
- The information security policies applicable in their work areas, roles and responsibilities
- Their personal responsibilities for information security
- How to access advice on information security matters
- How security incidents must be reported and managed

- All applicable staff must comply with security procedures supporting this section, including the maintenance of data confidentiality and data integrity

Legislation

The organisation is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation must be devolved to employees and agents of the organisation, who may be held personally accountable for any breaches of security for which they may be held responsible. The organisation should comply with the following legislation and other legislation as appropriate:

The Data Protection Act (1998)

The Copyright, Designs and Patents Act (1988)

The Computer Misuse Act (1990)

Human Rights Act (1998)

Regulation of Investigatory Powers Act 2000

Freedom of Information Act 2000

In terms of security requirements for information, the main areas which organisations should comply with are:

HSC ICT Security Policy and has signed up to its Code of Connection.

HMG Security Policy Framework www.cabinetoffice.gov.uk/spf

CESG InfoSec Memoranda www.cpni.gov.uk/docs/re-20050804-00653.pdf

The above is for government departments and public services; however, some partners may not follow these standards and hence ISO 27001 should be adhered to as the minimum level required for security management.

Whether or not a partner has adopted the HMG Security Policy Framework, partners would still be expected to ensure that the level of security would comply with the protective marking and not downgrade information to favour a lesser level of security.

VBS Security Policy Framework

Management of Security

- At board level, responsibility for Information Security must reside with the appropriate director as detailed in appendix 1.
- The organisations Information Security Officer must be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

Information Security Awareness Training

- Information security awareness training should be included in the staff induction process.
- An ongoing awareness programme should be established in order to ensure that staff awareness is refreshed and updated as necessary.

Contracts of Employment

- Security requirements must be addressed at the recruitment stage and all contracts of employment should contain security obligations and a confidentiality clause.
- Security Requirements should be included in job definitions.

Access Controls

Only authorised personnel who have a management approved business need must be given access to restricted areas containing ISA data or information systems handling ISA data.

User Access Controls

Access to ISA information must be restricted to authorised users who have a management approved business need to access the information.

Computer Access Control

Access to computer facilities containing ISA data must be restricted to authorised users who have a management approved business need to use the facilities.

Equipment Security

In order to minimise loss of, or damage to, all assets and equipment must be physically protected from security threats and environmental hazards.

Computer and Network Procedures

Management of computers and networks should be controlled by standard procedures that have been authorised by the Information Governance or Security officer.

Security Incidents and weaknesses

All security incidents and weaknesses are to be reported to the security manager identified in Annex 1. All security incidents must be investigated to establish their cause, operational impact, and business outcome. All security incidents and weaknesses involving ISA data must be reported to the ISA as soon as discovered.

Protection from Malicious Software

The organisation must use software countermeasures and management procedures to protect information systems -- where ISA information resides -- against the threat of malicious software. All staff must be expected to co-operate fully with this policy. Users must not install software on the organisation's property without permission from the appropriate security manager as agreed in Annex 1. Users breaching this requirement are likely to be subject to disciplinary action.

User Disks

Disks containing software or data from external sources, or that have been used in external equipment, must be fully virus checked before being used on the organisation's equipment. Users breaching this requirement must be subject to disciplinary action.

Monitoring System Access and Use

An audit trail of system access and use must be maintained and reviewed on a regular basis.

Accreditation/Approval of Information Systems

The organisation must ensure that all new information systems that hold ISA data, applications and networks include a security plan and are approved by the appropriate security manager before they commence operation.

System Change Control

Changes to information systems, applications or networks that contain ISA data must be reviewed and approved by the security manager.

Business Continuity and Disaster Recovery Plans

The organisation must ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks that may impact on the ISA's ability to function.

Reporting

The Information Security Officer and the IDG must keep the appropriate Boards informed of the information security status of the organisation by means of regular reports.

Policy Audit

This policy must be subject to audit, at least annually, by an appropriate auditor as stated in Appendix 1. The audit should include the review of access control arrangements, information disclosure, data storage and retention, IT systems audits (if ISA data or data provisioned by the ISA will be held electronically), physical security arrangements, personnel security and the vetting of persons with access to ISA data, and other applicable data handling arrangements.

This audit will be commissioned by the appropriately agreed individual within the organisation (typically the security manager) and based on the resource capability of the organisation. Each partner detailed in this agreement has the authority to decide whether to perform an in-house exercise or to outsource to a third party security audit specialist.

The primary assurance is that the principle of independence for scope, performance and reporting of the audit is preserved. Ultimately it is the responsibility of the agreed individual to determine the scope, schedule and performance etc. of the audit.

Risk Log

The information Security Officer must maintain a list of potential risks and any mitigation to reduce such risks. Where appropriate the Information Security Officer will share this list with ISA to discuss possible mitigation.

Further Information

Further information and advice on this section can be obtained from the ISA security manager, Samuel Hehir 01325 953744

APPENDIX 2: PRESCRIBED INFORMATION FOR SUPERVISORY AUTHORITIES

Section 45 of the Safeguarding Vulnerable Groups Act (SVGA) 2006 and Article 47 of Safeguarding Vulnerable Groups (Northern Ireland) Order (SVGO) 2007 sets out the duty for a Supervisory Authority (SA) to refer prescribed information to the Independent Safeguarding Authority (ISA) in certain circumstances.

Section 46 of the SVGA and Article 48 of the SVGO place a duty on a SA to provide prescribed information on request to do so by the ISA.

The information to be provided in a referral or on request is outlined in Articles 10 or 11 and Paragraphs 1, 2, 3, 5, 6, 9 and 10 of the Schedule to:

- The Safeguarding Vulnerable Groups Act 2006 (Prescribed Information) Regulations 2008 (No. 3265 of 2008); and
- The Safeguarding Vulnerable Groups (Prescribed Information) Regulations (Northern Ireland) 2009 (No. 40 of 2009).

The information is as follows:

Articles 10 or 11

In addition to the information requested in the following paragraphs of the Schedule, Articles 10 or 11 also require the SA to provide any other information relating to the person's conduct which is likely to, or may, be relevant in considering whether the person should be included in (or if relevant, removed from) a barred list including information relating to any decisions made, actions taken, complaints received or inspections undertaken by the SA in relation to the person.

Paragraph 1 requires the provision of personal information about the person being referred namely:

a) full name and title;
b) any other name or names by which the person may be known e.g. maiden name, aliases;
c) date of birth;
d) national insurance number;
e) gender;
f) last known address (including postcode); and
g) ISA registration number [Note: ISA registration has now been scrapped]

Paragraph 2 requires a description of the regulated or controlled activity that the person is, or was, engaged in.

Paragraph 3 requires information as to whether or not the person is included in a register maintained by a keeper of a register or a supervisory authority.

Paragraph 5 requires the SA to provide the following information relating to the persons conduct, (including copies of relevant documents):

a) a summary of the conduct including details of the setting and location in which such conduct occurred;
b) details of any harm suffered by any child or vulnerable adult resulting from or arising from the conduct or any risk of harm that a child or vulnerable adult was, or may have been, exposed to as a result of such conduct;
c) the following details of any child or vulnerable adult referred to above;
    I. the name and date of birth of the child or vulnerable adult;
    II. details of the relationship between the person and the child or vulnerable adult;
    III. information relating to the vulnerability of the child or vulnerable adult that may be relevant to ISA's consideration of whether to include or remove the person in or from a barred list including any emotional, behavioural, medical or physical condition;
d) whether the person has accepted responsibility for or admitted the conduct or any part of it;
e) any explanation offered by the person for the conduct or any remorse or insight demonstrated by the person in relation to the conduct;
f) any information other than that relating to the persons conduct which is likely to, or may, be relevant in considering whether the person should be included in or removed from a barred list including information relating to any previous offences, allegations, incidents, behaviour or other acts or omissions.

Paragraph 6 requires information relating to the reason why the referring party considers that the harm test is satisfied in relation to the person (if referring on the basis of satisfying the harm test).

Paragraph 9 requires details of any other proceedings before any court, tribunal or any other person taken or to be taken in relation to the person's conduct including the outcome of any such proceedings.

Paragraph 10 requires details of any action taken, or to be taken, by the person referring or providing information under the Act to the ISA in relation to the person's conduct including whether or not the matter has been referred to the police or to any other person.

Version 2.0 issued December 2011