HRA auditing

From GCWiki
Jump to: navigation, search

> Warning.png ***Warning: Please continue to refer to the Compliance Guidefor addtional current audit information!!!***

> Warning.png ***Warning: Do not make any changes under any of the headings, with the exception of the Audit Community Heading. If changes are required please contact [redacted]!!!***

This wiki has been created to assist staff in the HRA audit process. This wiki should be read in conjunction with the Compliance Guide

Contents

[edit] Purpose of Audit

Auditing is applied to Operations in order to assess and demonstrate the degree of compliance with policy standards. These standards are designed to meet the legal requirement to demonstrate necessity and proportionality and to show that GCHQ is acting in accordance with its authorisations and meeting its human rights obligations. The audit process is designed to achieve this aim.

For full details of the audit requirement please see

Compliance Guide

[edit] Audit Timetable

There is currently an audit requirement for a random sample of database records from BROAD OAK every quarter & HRA EVENTS Service every 6 months at the following intervals; however, this audit programme is currently under review and this may be subject to change at any time:

JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
UDAQ	BROAD OAK	None	None	BROAD OAK	EVENTS	UDAQ	BROAD OAK	None	None	BROAD OAK	EVENTS

[edit] OPP-LEG's Responsibility

OPP-LEG is responsible for overseeing the audit process and for providing guidance on how to complete an audit. It is OPP-LEG's responsibility to set the objective standards, using metrics, and which measure HRA compliance. The metrics used are Red - below 75% being unacceptable non-Compliance, Amber - 75% to below 94% being fairly Compliant but with room for improvement & Green - 95% and above being Compliant. It is for this that OPP-LEG provides training and guidance to all staff on the need to properly justify their work and to demonstrate compliance. OPP-LEG will:

- provide data samples for the UDAQ and events audits to the chief auditor or LPL at the start of each audit
- provide end of year reports to the Deputy Directors for Intelligence Production on the overall findings of the audits.
- work with IPTs/BUs, if requested, to help to raise compliance rates and will track key themes that are identified in audit reports, and will request changes to systems if necessary.

[edit] Analyst's Responsibility

All records of analysts' actions when conducting targeting, tasking, searching and examining intecept for communications content or metadata must demonstrate compliance with HRA. Some areas have produced local guidance to help staff how to demonstrate high standards of HRA compliance. Please speak to your Legal and Policy Lead to see if your area has this guidance and make sure that you are familiar with it as this is the standard that auditors will use to judge records as part of an audit.

You must ensure that your work:

- is conducted for one of GCHQ's Sigint purposes: **National Security**, **Economic Well-Being** of the UK or in support of the prevention or detection of **Serious Crime**
- supports an intelligence requirement (demonstrated by recording a relevant MIRANDA reference)
- contains a free-flow HRA justification stating why you are intruding an individual's privacy and what your expected outcome is in conducting this intrusion

- where necessary contains the Warrant or Copper reference for targets in the UK or targets overseas who are deemed sensitive on grounds of nationality or location

You must also comply with any requests made by an auditor to:

- ensure that any amendments required to records you own are made within a two-week deadline
- notify the auditor once amendments are made
- take responsibility for ensuring that you improve the standard of your HRA justifications for ad-hoc UDAQ and events queries if your your auditor highlights any shortcomings in queries that have already been run

Please see What are auditors looking for? for guidance on how auditors assess targeting and query records.

[edit] BROAD OAK HRA justifications in other tools

The BROAD OAK tool provides links to both content and events interfaces. The appropriate HRA justification fields in BROAD OAK are pulled through to these interfaces and populate the HRA justification fields in the interface. If you choose to work in this way, you must ensure that your HRA justification in BROAD OAK also justifies your intrusion into the communications of or associated with your target.

[edit] Auditor's Responsibility

Whilst the Legal and Policy Lead for each business unit has overall responsibility for audits, he or she may devolve responsibility for individual audits to a chief auditor (see ’audit community’ for full list). The LPL or other delegated person is responsible for ensuring recommendations for improving standards made by the auditors are followed up. The chief auditor is responsible for the following:

- pulling data for BROAD OAK audits using the Query Builder function of the BROAD OAK tool. The BROAD OAK *User Guide contains detailed instructions on how to create queries for auditing and adhoc spot-checks
- providing OPP-LEG with the audit report using the audit template
- ensuring that the report is sent to OPP-LEG by no later than the first week after the month in which the audit was completed (eg audit conducted in May, report must be with OPP-LEG by first week in June)
- either completing the audit him/herself or devolving the audit burden amongst a team of established auditors
- informing record owners or team leaders of changes required to records that do not meet the criteria or need to be improved
- confirming that the necessary changes have been implemented within the two-week deadline
- engaging with line managers or business unit heads if analysts fail to comply with requests for amendments, to ensure prompt action is taken
- advising analysts of shortcomings noted in records that cannot be amended (one-off queries) to assist with improvements in future queries
- making recommendations on how to improve standards of compliance
- advising OPP-LEG about potential improvements to the audit process or of changes to the systems

Please see What are auditors looking for? for guidance on how to assess targeting and query records.

[edit] Business Unit/IPT Head's Responsibility

Each BU/IPT Head is responsible for the legality of his/her team's activities and must ensure that auditing takes place to a standard that demonstrates compliance. This responsibility remains with the BU/IPT Head even if the control and reporting of the audit is delegated. Each BU/IPT audits its own activity. BU/IPT Heads must:

- ensure that resources are made available to meet audit requirements
- confirm that they have seen each audit report and noted the recommendations contained within
- conduct a light-touch spot-check of audit integrity of the **BROAD OAK** audit by examining a small sample of the **BROAD OAK** records that have been audited to make an objective assessment whether audit teams have carried out their role in a satisfactory manner
- provide a short report to OPP-LEG (email will suffice) on the results of the spot-check and on all plans to implement audit report recommendations, no later than a month after filing each audit report with OPP-LEG

The spot-check sits alongside existing responsibility to ensure that measures are in place to follow up on the recommendations in each audit report

[edit] What are auditors looking for?

The auditors must make a judgment on whether the information in the following fields demonstrates HRA compliance. Records must meet the standard required in all fields to pass the audit test:

Some areas have produced local guidance that helps staff to understand how to demonstrate high standards of HRA compliance. Auditors in these teams should use this guidance to help them to assess records.

- **Source Reference (BROAD OAK only) –** this should provide a clear and traceable reference indicating where the record-owner got the selector from, and the date of the source. #
    - A Telephone Call with a customer/partner that has led to the provision of selectors should not be used a source reference. The telephone call needs to be followed up with a formal record of the passing of the selector (e.g. An email). This is to ensure a traceable reference to the origin of the selector. It is up to local areas to decide how best to implement this requirement.
    - Any records in the system that pre-date 1 January 2006 may be given a pass if the source reference is vague or incomplete. Auditors should indicated in the audit report how many records fall into this category.
    - With effect from 20 May 2010, it is mandatory to record a source date as well as a source reference. Auditors can apply a waiver to any selectors that were targeted before 20 May 2010 that do not have a source date and should indicate in the quarterly audit report how many records fall into this category; however, auditors should encourage analysts to try to identify and record an accurate source date.
- A Telephone Call with a customer/partner that has led to the provision of selectors should not be used a source reference. The telephone call needs to be followed up with a formal record of the passing of the selector (e.g. an email). This is so that there is a traceable reference to the origin of the selector. It is up to local areas to decide how best to implement this requirement.

- **MIRANDA number –** this should be relevant to the intelligence requirement and JIC purpose.
    - If analysis is being carried out for target development eg targeting selectors linked to a known target from call records, the MIRANDA number that is relevant to intelligence requirement should be used, and the targeting period should be limited to 3 months.

    - If Sigint Development or even Target Development/Discovery is being conducted in a broader context the use of a Sigint Development MIRANDA number such as 20135 is appropriate with, again, the targeting period being limited to 3 months.
    - The Open Source MIRANDA number 20142 should only be used by those working in CK.
    - There was a change to MIRANDA numbers 01 October 2009 and, from then, there was a concessionary waiver to treat incorrect 'old' codes as an amendment required and not an audit failure; however, this concessionary waiver expired from 01 October 2010. Any incorrect codes found from now will be treated as a fail.
- **JIC Priority/Purpose** – this must be the correct underlying purpose ie NS, EWB or SC; however, records should not be failed if the priority has changed since the record was first entered, but should be noted as needing attention and the record should still be amended by the record-owner
- **HRA Justification** – this should provide clear explanation of why it is necessary to intrude upon an individual's privacy by targeting, or running a particular query to examine their communications (both content and events). The following principles should be applied:
    - it should add value to the intelligence requirement and NOT just repeat the intelligence topic
    - it should be clear to an uninformed observer why it is necessary and proportionate to intrude on that particular individual's right to privacy and what the expected intelligence outcome is.
    - use of acronyms and codewords is not encouraged as they may be clear to an analyst, but not necessarily to others. Only the most common abbreivations are acceptabnle; the test is whether or not the abbreviation would be understood by the Commissioner. Any lists of acronyms or abbreviations which have been agreed with OPP-LEG in the past as usable are no longer valid. If explanation of an acronym or codeword may result in the compromise of a sensitive operation then consult OPP-LEG to discuss a waiver
    - TD/SD, CT etc are NOT valid HRA justifications; neither is an operation name without some further comment to expand on this
- **HRA revalidation** - if the targeting of a selector has been renewed beyond the default limit (one year or three months) or a scheduled content query has been extended, a check that the HRA justification clearly explains why it is necessary to *continue* to intrude on an individual's right to privacy by targeting that selector or running the query.
- **Legal or policy authorisation for target** – If this is required (for selectors or queries that relate to targets in the UK or targets overseas who are sensitive on grounds of location or nationality), the correct warrant or COPPER reference and a valid expiry date are required. The HRA Review date must also reflect the expiry date of the warrant or authorisation. Any targeting or content queries that do not have a valid warrant or STA reference may constitute an offence under Section 1 of RIPA, a breach of RIPA safeguards or a breach of GCHQ policy. These records must be reported immediately to OPP-LEG.

OPP-LEG have had questions on Audit requirements in the past and some can be found at FAQ's

[edit] The Report Template

The report should be submitted in a word document using the templates found at the following links. Please note these links only work using **Internet Explorer**:

events or udaq audit template

targeting audit template

[edit] Audit Community

Here is a list of the main points of contact for each audit. **Please feel free to amend this list as roles**