

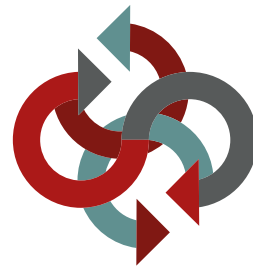


GIG
CYMRU
NHS
WALES

Iechyd a Gofal
Digidol Cymru
Digital Health
and Care Wales



Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government



Cytundeb Rhannu Gwybodaeth
Bersonol Cymru
Wales Accord on the
Sharing of Personal Information

Code of Conduct

Governance & Information Risk Assurance (Gira) Procedure

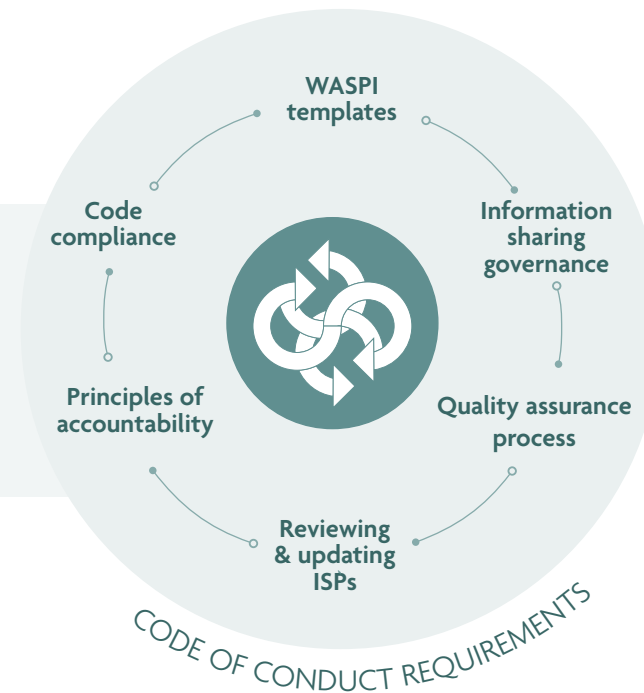


INTRODUCTION

The Governance and Information Risk Assurance (GIRA) is a required annual assessment which will be reviewed by the monitoring body in respect of each code member to ensure that the organisation meets a set of minimum requirements to continue to be an approved code of conduct member.

The GIRA focuses on monitoring and measuring that a code member continues to meet standards expected and to enable a code member to provide evidence of its organisational controls aligned to the WASPI code of conduct requirements.

The GIRA is the annual self-assessment that each code member will complete to evidence how they continue to meet the requirements of the Code of Conduct, specifically those relevant to requirements 2-5 of the WASPI Code of Conduct, with requirements 1 and 6 continually assessed as part of code member engagement with WASPI.



Complying with the GIRA process is part of the evidence of compliance set out within requirement 6 of the Code of Conduct and will support the 3-year audit programme that each code member would be required to undertake.

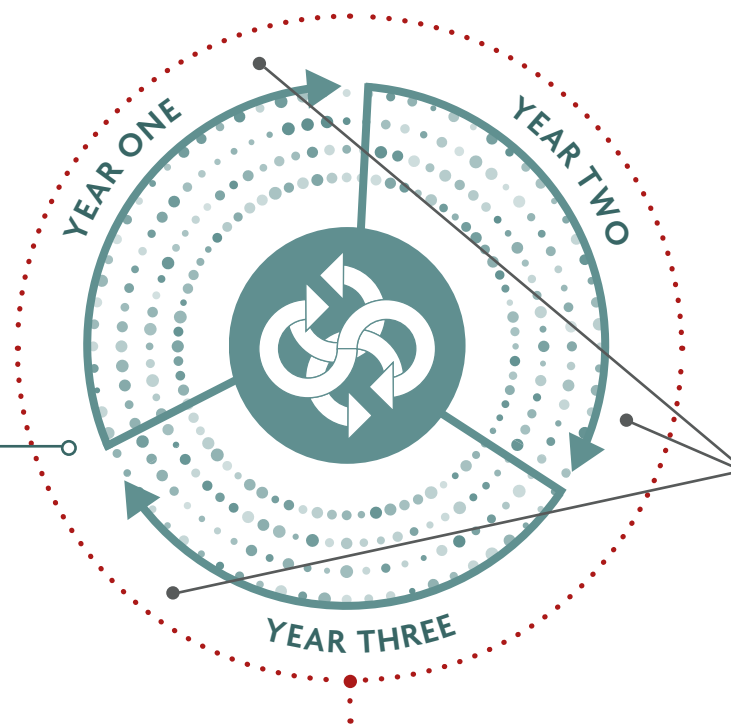
The diagram below shows the 3-year Code of Conduct cycle, showing how the GIRA and the Audit Programme interact.

WASPI CODE OF CONDUCT – 3 YEAR CYCLE FOR CODE MEMBERS

START

Prospective Code Member complete and submit the application form to the Monitoring Body. The Monitoring Body reviews and approves the application for Code Membership.

Application is only completed once.



GOVERNANCE & INFORMATION RISK

ASSURANCE (GIRA)

The GIRA will need to be completed by the Code Member in **advance of annual membership expiring.**

This is due a minimum of 8 weeks prior to expiration of membership but no sooner than 12 weeks before expiration.

AUDIT PROGRAMME

To supplement the assessment of the GIRA, the monitoring body will undertake a comprehensive audit programme. Code Members commit to be subject to a **audit a minimum of once every three years.**

Process

The GIRA must be completed in advance of annual membership expiring. To ensure the accuracy of review this must be issued to the monitoring body at least 8 weeks prior to expiration of membership but no sooner than 12 weeks before expiration.




As a self-assessment the GIRA will be considered by the monitoring body to determine if appropriate evidence has been provided that demonstrates that the code member remains compliant with the code of conduct requirements.

Each area of the assessment will be rated:

 **RED**

 **AMBER**

 **GREEN**

RAG	Assessment Explanation
RED 	Area of assessment determined by the monitoring body to have failed to meet evidence to demonstrate compliance with the control requirement for code membership.
AMBER 	Area of assessment determined by the monitoring body to have supplied sufficient evidence to demonstrate compliance with the control requirement for code membership, with areas to improve assessment rating suggested.
GREEN 	Area of assessment determined by the monitoring body to have supplied more than sufficient evidence to demonstrate compliance with the control requirement for code membership.

Where a code members' assessment has identified any areas which fail to meet, or where insufficient evidence has not been submitted to demonstrate meeting, essential requirements of the Code of Conduct, the code member will have 3 weeks to evaluate the response from the date of the assessment being issued by the monitoring body and to resubmit assurance, evidence and/or commitment of improvements to be implemented.

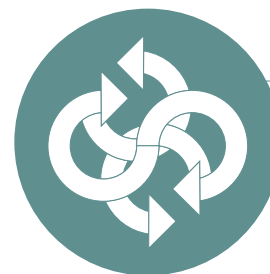
A re-evaluation will be completed within 2 weeks by the monitoring body and determination of this communicated back to the code member to enable a code members' membership with the Code of Conduct to continue before expiration.

Where this timeframe is not followed by the code member, or evidence/resubmission is not received, or reassessed as

meeting the required criteria, the code member will be notified of their suspension from the Code of Conduct and have the rights of appeal/complaint as set out within the WASPI Code of Conduct Appeals and Complaints Procedure.

The monitoring body will maintain a record of GIRA assessments and evidence provided and this may be considered as part of future assessments, or to consider any complaints made against a code member. This information may also be shared with any other regulatory bodies as part of audits and inspections obligations they may be subject to, including inspectors such as Audit Wales and Care Inspectorate Wales.

The annual Governance & Information Risk Assurance assessment is attached to this procedure.



**AELOD COD YMDDYGIAD
CODE OF CONDUCT MEMBER**

Cytundeb Rhannu Gwybodaeth
Bersonol Cymru
Wales Accord on the
Sharing of Personal Information

Versions

Amended	Version	Status	Date	Purpose of change
D. Parsons	0.1	Draft	November 2022	Initial Draft

This document has been written and produced by:

WASPI Monitoring Body

Tŷ Glan-yr-Afon
21 Cowbridge Road East
Cardiff
CF11 9AD



This document is also available in Welsh

Section A – Code Member Information Sharing Governance (RQ2)			
Overarching Control Objectives	Control Question	Y/N	Code member response
Management direction for information sharing: To provide management direction and support for information governance and data sharing requirements and relevant laws and regulations.	A.1 Do you have a SIRO/DPO/ Caldicott Guardian/ Lead or Chief Officer (or equivalent Board level member) that manages the organisation's information risk management framework and information sharing responsibilities? Please explain your response.		
WASPI Monitoring Body comments/observations			
RAG Rating			
	A.2 Does your senior responsible officer (as outlined above) have visibility of and sign off your organisations Information Sharing Protocols?		
WASPI Monitoring Body comments/observations			
RAG Rating			

	A.3 Does your organisation have access to information protocols such as Freedom of Information and Subject Access, in place which align to any Information Sharing Protocols?		
WASPI Monitoring Body comments/observations			
RAG Rating			
	A.4 Please provide details of all systems used to securely share personal data with partners as part of active Information Sharing Protocols. This section should list all systems used to securely share data.		
WASPI Monitoring Body comments/observations			
RAG Rating			

Section B – The principles of accountability (RQ5)			
Overarching Control Objectives	Control Question	Y/N	Code member response
Data protection & data sharing awareness, education & training: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.	B.1 Please confirm what training arrangements you have in place to support officers with understanding their requirements of data sharing activities and use of personal/special category data.		
WASPI Monitoring Body comments/observations			
RAG Rating			
	B.2 Please provide details of staff your organisation have to support Information Sharing Protocols		
WASPI Monitoring Body comments/observations			
RAG Rating			

	B.3 Please provide details of how your organisation offers support/training/guidance to staff on the development of Information Sharing Protocols and the WASPI code of conduct.		
WASPI Monitoring Body comments/observations			
RAG Rating			
	B.4 Please provide evidence of any privacy notices/policies you have in place which represent data sharing activities with current Information Sharing Protocols		
WASPI Monitoring Body comments/observations			
RAG Rating			

Section C – Information Sharing Protocols and a commitment to review and update agreements (RQ4)			
Overarching Control Objectives	Control Question	Y/N	Code member response
Appropriate contact with relevant authorities and special interest groups shall be maintained and existing Information Sharing Protocols compliance.	C.1 Please confirm how your organisation engages with and regularly communicates with its information sharing partners. Examples may include relevant partnership boards/groups, cluster hubs, regional quality assurance groups or others, where information sharing is regularly discussed.		
WASPI Monitoring Body comments/observations			
RAG Rating			
	C.2 Please provide details of any Information Sharing Protocols created or reviewed over the past 12 months and evidence of the process followed to ensure these have followed WASPI processes including quality assurance mechanisms		

WASPI Monitoring Body comments/observations			
RAG Rating			
	C.3 Does your organisation have any Information Sharing Protocols for which you are the lead organisation which have not been reviewed for over 2 years? Please detail these ISPs and detail any planned or ongoing measures in place to ensure these are reviewed		
WASPI Monitoring Body comments/observations			
RAG Rating			

Section D – A commitment to the quality assurance process (RQ3)			
Overarching Control Objectives	Control Question	Y/N	Code member response
Supporting quality assurance processes to ensure to maintain the integrity of the standard templates.	D.1 Does your organisation attend and contribute to any of the five Regional Quality Assurance Groups? If you are a standing member of one of the Regional Quality Assurance Groups, please provide details of attendance by your organisation during the past 12 months.		
WASPI Monitoring Body comments/observations			
RAG Rating			
	D.2 Please provide details of any Regional Groups your organisations staff may have attended or engaged with during the past 12 months through the development of ISPs.		
WASPI Monitoring Body comments/observations			

RAG Rating			
	D.3 Please provide details of ISPs which your organisation have issued for initial quality assurance and successfully agreed and signed off with partner organisations over the past 12 months.		
WASPI Monitoring Body comments/observations			
RAG Rating			

Section E – Code Member Commitment Declaration

I confirm that my organisation meets its obligation to deliver the control outcomes of the Governance and Information Risk Assessment and to actively resolve areas where shortfalls are identified; and that I am able and agree to commit the resources of my organisation towards maintenance and continuous improvement against these obligations.

I accept that the WASPI Code of Conduct Monitoring Body has the right to audit my organisation and to request supporting information to gain assurance in respect of my organisation's Governance and Information Risk Assessment.

Name of Organisation	
Name of Senior Information Risk Owner/Caldicott Guardian or equivalent	
Signature	
Date	
Name of Information Governance / Data Protection lead / Designated person	
Signature	
Date	
WASPI Monitoring Body overall comments/assessment	
Name of WASPI Member completing assessment	
Signature	
Date	