SCI v2 How-to

This guidance is intended to assist those implementing SCI and, as such, is not primarily scoped to ‘end users’ - members of collections of users. Infrastructure managers, service operators, security officers, the responsibles of collections of users, and others invested in the security of an infrastructure and its services, are the intended audience.

Related documents:

https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf
https://indico.nikhef.nl/event/2146/contribution/13/material/0/

Contents:

Operational Security [OS]

OS1 - Security Person/Team

Each of the collaborating infrastructures has:

What:	*"A person or team mandated to represent the interests of security for the infrastructure."*
Why:	To ensure that implementing infrastructure security policy is clearly defined as an individual or group core responsibility, giving it appropriate priority and authority within the organisation for necessary actions to be carried out. To prevent confusion and delay in the event of a reported incident.
How:	Designate an individual, or team, with responsibility for the development and oversight of activities required to implement security policy, including those to address and mitigate security risks. Provide, or delegate to, a clear point of contact within the infrastructure for all matters related to security, including incident handling.
Checks:	- The person or team is appointed with clear responsibility and authority. - Contact details for the above are published internally and externally.

OS2 - Risk Management Process

Each of the collaborating infrastructures has:

What:	*"A process to identify and manage security risks on a regular basis."*
Why:	In order to reduce the likelihood and impact of security incidents.
How:	A process for the identification, assessment and appropriate mitigation of risk must be a core function of Infrastructure Management.The scope and comprehensiveness of the procedure depends on the size and purpose of the Infrastructure. The procedure may encompass the following: ● Data theft or loss (potential impact of data loss, personal data involved, protection of personal data, protection of users' data) ● Denial of service ● Intrusion detection ● Phishing/hacking/ransomware attacks ● Unauthorized use of resources (botnets, cryptocurrency mining) ● Detection of unauthorized/illegal data (adult material, illegal data) Periodic review of such a risk register and mitigations should be part of the ongoing management process which should also coordinate with the IR2 procedure, since some functionalities may overlap.
Checks:	- Risks and mitigations have been identified and documented - Reviews of the risks and mitigations take place on a regular basis - Actions resulting from the review are given appropriate priority and resources.

OS3 - Security plan

Each of the collaborating infrastructures has:

What:	*"A security plan (e.g., architecture, requirements, controls, policies, processes) addressing issues, such as, authentication, authorisation, access control, physical and network security, risk mitigation, confidentiality, integrity and availability, disaster recovery, together with compliance mechanisms ensuring its implementation."*
Why:	In order to ensure that critical steps and decisions are not forgotten in the event of an incident, and to facilitate knowledge transfer given staffing changes.
How:	Infrastructure must document a plan detailing the questions of access control (who and for which purpose can access resources), security, and reliability (all the aforementioned points must be addressed) together with creating policies and procedures to implement the plan. This point requires a substantial effort. As such, it may be fulfilled with multiple documents (a policy framework) that addresses the points in question. Procedures from other points of the SCI (not just from OS) can be used to address this requirement. The security plan may

	take the form of a “live” document that is subject to regular updates to reflect changes decided by OS1.
Checks:	

OS4 - Security Patching

Each of the collaborating infrastructures has:

What:	*“A process to ensure that security patches are applied to operating systems, application software and firmware in a timely manner, and that patch application is recorded and communicated to the appropriate contacts.”*
Why:	In order to maintain the security of a system to the fullest extent possible. Failure to apply security patches in a timely manner is one of the major causes of system compromise.
How:	Patching procedures should address the question of how the state of a system (e.g. has a security patch been applied?) is monitored and when and how required patches are applied. Procedures should also document the responsible persons and which actions must be taken. The investment of time in the deployment of software configuration management systems (https://en.wikipedia.org/wiki/Comparison_of_open-source_configuration_management_software) is highly recommended.
Checks:	- A system is in place to track the installed state of all systems - Subscription or other means is available to receive update notices - A process or frequent review is in place to correlate and act on the above

OS5 - Vulnerability Management

Each of the collaborating infrastructures has:

What:	*“A process to manage vulnerabilities (including reporting and disclosure) in any software recommended for use within the infrastructure. This process must be sufficiently dynamic to respond to changing threat environments.”*
Why:	It is likely that during the operation of an Infrastructure, vulnerabilities in software being used at resources will be discovered or made public. The ability of the operational security team to handle such events, on an ongoing basis, is critical to maintaining the security of the Infrastructure.
How:	Vulnerability management procedures must be documented, including the responsible persons and their actions. A communications channel to receive

	reports of vulnerabilities should be established and its details published. The channel should be open for anybody to post to but with a restricted recipient list. A process to assess the risk a vulnerability poses to the infrastructure and to action an appropriate response should be agreed, together with a policy on how and when to disclose details of confirmed vulnerabilities. It is important to have access to experts in the various software packages used to enable an accurate assessment of the impact of a vulnerability on the operational status of the infrastructure: can the risk be accepted, for how long, or should services be immediately shut down?
Checks:	- A system is in place to track the installed state of systems - A channel is available to receive vulnerability reports - Subscription or other means are in place to track vulnerability reports - Channels are available to report vulnerabilities to participants - A process for the timely assessment of vulnerability impact is in place - A process is in place to act in the event of a report detecting vulnerabilities

OS6 - Intrusion Detection

Each of the collaborating infrastructures has:

What:	*“Tools and techniques to detect intrusions and protect against significant and immediate threats to the infrastructure.”*
Why:	Security is a highly dynamic environment and no mitigations or other measures will prevent the success of some attacks. Timely detection of intrusions is necessary to limit their impact, and having the ability to trace ongoing or past intrusions through logged information will assist in preventing recurrence.
How:	Depending on the size of the Infrastructure, detection techniques may encompass deploying simple tools (e.g. logwatch, Tripwire) to more extensive measures (e.g. usage patterns monitoring). As a minimum it is recommended that all systems are configured to log network connections (successful or otherwise) and, to prevent attackers destroying or modifying logged information, that these logs are propagated to a central logging service for secure storage, in line with a log retention policy. As well as deploying active detection mechanisms, subscription to sources of threat intelligence (containing malware signatures and other indicators of compromise), together with tools to match published indicators against local activity, can help to both proactively detect and prevent compromises..
Checks:	- Appropriate tools are configured to control, monitor and log activity. - A centralised log storage and retention policy is implemented.

OS7 - Regulate Access

Each of the collaborating infrastructures has:

What:	*"The capability to regulate the access of authenticated users, including emergency suspension during the handling of security incidents."*
Why:	Access control is a primary means of protecting systems from misuse. Ensuring that only those authorised to access information or take actions are able to do so is critical to maintaining the integrity of data and systems. During the investigation of a security incident evidence of malicious, or otherwise harmful, activity associated with user accounts may be uncovered or suspected. Temporary suspension of such accounts may be necessary to prevent further damage or disruption to the infrastructure while investigations continue.
How:	Depending on the authentication and authorisation technology used, controlling access may entail blocking accounts, revoking certificates and refresh tokens, etc. If possible, and appropriate in the particular circumstances of the investigation, users should be contacted and informed of any actions taken.
Checks:	- Technology to regulate access is understood and tested. - Prior authority and process is in place to effect action in a timely manner.

OS8 - Contact Information

Each of the collaborating infrastructures has:

What:	*"The capability to identify and contact authorised users and service providers."*
Why:	Contact information of users is necessary to contact the user for security related reasons e.g. should malicious activity be found associated with a user's account to investigate if their credential has been stolen. Similarly, contact information of service providers is vital should, for instance, security investigations indicate that a service has been compromised e.g. is part of a botnet generating spam emails.
How:	As a minimum, it is recommended that the name and a validated email address for all users is gathered at registration and this information is available, where necessary, to authorised parties for the investigation of security incidents. The Infrastructure operations team should gather and maintain contact information for the service administrators. Periodic testing that service contact email addresses remain valid can help ensure smooth communications flow

	when needed. A generic contact email for the service team, rather than any personal email, is likely to be more appropriate in these cases.
Checks:	- user contact information is available and maintained - system administrator contact information is available and maintained

OS9 - Policy Enforcement

Each of the collaborating infrastructures has:

What:	*"The capability to enforce the implementation of applicable security policies, including an escalation procedure, and the authority to require actions necessary to protect assets from, or contain the spread of, security incidents."*
Why:	Security policies will likely have little or negative impact unless there are effective means to enforce them. Particularly, during an active security incident, valuable time and information may be lost if authority and actions are not clearly defined and understood by all parties beforehand.
How:	Mechanisms that enforce the policies can be organisational (i.e. everyone is aware of the policies, and that they will be enforced) and technical (i.e. using the measures that can suspend users, contain the spread of incidents, coordination, etc.). It is important that the relevant policy clearly establishes the authority of a body (e.g. security operations team or management) or individual (e.g. security officer) to take necessary enforcement action, and a process to adjudicate over any resulting disputes. Defining sanctions together with an escalation process to apply them in the event of non-compliance is an important tool in policy enforcement.
Checks:	- All participants are made aware of relevant policies and their responsibilities - Enforcement mechanisms and the authority to effect them are clearly defined

OS10 - Security Assessment of Services

Each of the collaborating infrastructures has:

What:	*"Processes that include security considerations in the design and deployment of services or software, reviewed by the responsible individual or team identified in [OS1] above, or their representative."*
Why:	Inadequate security design or implementation can introduce security vulnerabilities which put not only the service in question but also, particularly in federated environments, the Infrastructure as a whole at risk. Whenever a new service, software or significant configuration changes are introduced to the

	infrastructure, the risk of introducing vulnerabilities must be minimised.
How:	The processes of service deployment, onboarding to the infrastructure, and change control should include, as an integral part of service delivery, a stage where security implications for the service and Infrastructure are considered. A simple checklist including items such as software patching, network firewall hole checks and system dependencies can assist in operational aspects of safe deployment. The decommissioning of services, when they are no longer required, should also be part of the deployment lifecycle process to, for instance, ensure that unmanaged machines with open firewall access do not remain attached to the network.
Checks:	- Onboarding and deployment processes include assessment of security - Change management processes include assessment of security - Service decommissioning is included in management processes - Regular reviews of services, focussed on security, are scheduled

Incident Response [IR]

IR1 - Contact Information

Each infrastructure has the following:

What:	*"A process to maintain security contact information for all service providers and communities."*
Why:	Accurate and up to date contact information enables participants to exchange information quickly and efficiently with affected parties in the event of a security incident.
How:	This is generally seen as mandatory information to be provided when joining an infrastructure. The security contact information is usually an email used to contact service providers and communities in case of security incidents. The methods to obtain this lists are multifold, such as from the metadata (in the case of the federation participants that support Sirtfi[1]), or directly from the service operators and communities during the Infrastructure onboarding process. The up-to-dateness of the information can be ensured via periodic email verification procedures (tools for this exist).
Checks:	- there is an onboarding process which gathers security contact information - service security contact information is available and maintained

[1] https://refeds.org/sirtfi

	- community security contact information is available and maintained

IR2 - Incident Response Procedure

Each infrastructure has the following:

What:	*“A documented Incident Response procedure. This must address: roles and responsibilities of individuals and teams, identification and assessment of incidents, minimisation of damage to the infrastructure, response and recovery strategies to restore services, communication and tracking tools and procedures, and a post-mortem review to capture lessons learned.“*
Why:	Having a prepared and tested incident response procedure, agreed by all participants, allows for rapid and well coordinated response when an incident occurs. Valuable information may be lost or additional damage occur if time is lost during the response to an incident.
How:	The required effort depends on the size and the purpose of the Infrastructure. As a rule of thumb, the bigger the Infrastructure (in terms of users, communities, and services), or the more valuable or sensitive the data being processed is, the more comprehensive the procedure should be. Accordingly, for a smaller Infrastructure, the required effort may be more limited. As mentioned, the documented Incident Response procedure must (at the very least) address the points above. The diagram below is an example of step-by-step guidance on how to proceed in cases of security incidents.
Checks:	- a procedure covering the points listed is documented - all relevant parties are aware of the procedure

More information can be found also in the PDK Incident Response Procedure[2].

[2] https://docs.google.com/document/d/1V4YKQH3ha_odLBg6eZLT_VcD5JotHNL47UTLq5Ps6vg/edit

Incident Response Procedure Example

Version 2020

1 – (Suspected) Discovery

1. ☐ Local Security Team ——— *If applicable: INFORM **WITHIN 4 HOURS***.
2. ☐ Infrastructure Security Contact ——— *INFORM **WITHIN 4 HOURS***.

2 – Containment

1. ☐ Affected Hosts ——— *If feasible: ISOLATE as soon as possible **WITHIN 1 DAY***.
2. ☐ Affected VMs/Dockers ——— *SNAPSHOT and/or SUSPEND **WITHIN 4 HOURS***.
3. ☐ Affected Appliances ——— *DISABLE **WITHIN 4 HOURS***.

3 – Confirmation

1. ☐ Incident — *CONFIRM WITH YOUR LOCAL SECURITY TEAM AND/OR Infrastructure CSIRT*.

4 – Downtime Announcement

1. ☐ Service Downtime ——— *If applicable: ANNOUNCE WITH REASON "SECURITY OPERATIONS IN PROGRESS" **WITHIN 1 DAY***.

5 – Analysis

1. ☐ Evidence ——— *COLLECT AS APPROPRIATE*.
2. ☐ Incident Analysis ——— *PERFORM AS APPROPRIATE*.
3. ☐ Requests From Infrastructure CSIRT ——— *FOLLOW UP **WITHIN 4 HOURS***.

6 – Debriefing

1. ☐ Post-Mortem Incident Report ——— *PREPARE AND SEND to Infrastructure SCIRT **WITHIN 1 MONTH***.

7 – Normal Operation Restoration

1. ☐ Normal Service Operation ——— *RESTORE AS PER RESOURCE CENTRE STANDARDS **AFTER INCIDENT HANDLING IS COMPLETE***.
2. ☐ Procedures and Documentation ——— *UPDATE as appropriate to reflect analysis results*.

IR3 - Incident Response Collaboration

Each infrastructure has the following:

What:	*"The capability to collaborate in the handling of security incidents with affected service providers, communities, and infrastructures, together with processes to ensure the regular testing of this capability."*
Why:	Security incidents often extend across organisational boundaries and the handling of such multi-domain incidents requires communication and collaboration with other participants.
How:	Infrastructure management must ensure that adequate authority, priority and resources are given to be able to cooperate in security incidents with all affected (and potentially affected) entities. All parties must be aware of their responsibility to, and willing to participate, in the sharing of information. This generally implies the existence of a dedicated security officer with backup from a security team, and appropriate policy agreements in place to enable collaboration with other security teams. The effectiveness of the capability should be tested, i.e. "mock-up" incident scenarios, rehearsed on a regular basis. This activity is valuable, not only in revealing problems in communications and procedures, but also in building contacts and trust between the participants in the exercise..
Checks:	- resources and responsibilities are clearly allocated to security collaboration - engagement in multi-domain testing for incident response

IR4 - Information Sharing Controls

Each infrastructure has the following:

What:	*"Policies and procedures to ensure compliance with information sharing restrictions on incident data exchanged during collaborative investigations. If no information sharing guidelines are specified, incident data will only be shared with other security teams on a need to know basis, and will not be redistributed further without prior approval."*
Why:	Information, such as affected identities or hosts addresses, which might be invaluable in protecting from or helping in the response to a security incident, will only be shared by the owners of the information if they trust that you will handle the information appropriately. Demonstrating that those handling such information within the infrastructure will do so appropriately, by strict adherence to agreed policies and procedures, is key to building this trust. Similarly,

	information arising from an incident within an infrastructure should be shared with collaborators where possible and appropriate, and sharing policies should be put in place beforehand.
How:	This point requires the Infrastructure to create policies and procedures for the receipt and sharing of incident information. These policies should outline how this information should be shared (in a proper manner, through secure channels), preferably to whom (how "wide" the required and authorized audience is), and which channels for communication and information dissemination are available. All of these functionalities should be tested as defined in IR3. If such policies do not exist, the information should still be shared on a need to know basis. The Traffic Light Protocol (TLP) is widely used as a basis for information exchange classification.
Checks:	- an information sharing policy is agreed and known to collaborators

Traceability [TR]

TR1 - Traceability (who, what, where, when, how)

Each infrastructure has the following:

What:	*"Traceability of service usage, by the production and retention of appropriate logging data, sufficient to be able to answer the basic questions – who? what? where? when? and how? concerning any security incident."*
Why:	Log data is the primary source of authoritative information on service events, such as failed and successful network connections and logins, the import and export of data, vital to understanding and tracing the origins and progression of a security incident by asking the questions posed above.
How:	This point is more comprehensive than initially may seem, as it involves not only logs but the information necessary to produce those logs. That means that in addition to information the Infrastructure generates itself, it may need to receive enough information in order to be able to produce such information. For example, in a proxy scenario, the information received from the IdP must be

	verbose enough to generate and assign proper “uniqueness” to the user. One example of such standard that Infrastructure may follow is R&S[3]. In addition to receiving the information, generated logs should also be verbose enough to easily answer aforementioned questions. An infrastructure should also possess tools to properly parse the logs. To reduce the possibility that logs can be destroyed or tampered with during an incident, it is strongly recommended that all logs records are securely forwarded, on generation, to a suitably secured central logging service. For infrastructures sharing common services or service provider organisations, it is relevant to share personal information within the R&S attribute set (name of the person, email address) in order to correlate incidents across services and infrastructures that share cross-community users. In that context, the only service-provider correlatable information is user-bound, and this information should be sufficient to - with a high probability - identify the ultimate end-entity.
Checks:	- services are configured to receive and log all the necessary information - where possible, logs are securely stored on a central service

TR2 - Data Retention Period

Each infrastructure has the following:

What:	*“A specification of the data retention period, consistent with local, national and international regulations and policies.”*
Why:	The availability of log data, sufficient to trace historical incident reports, is vital in understanding an incident and protecting an infrastructure from future attack. However, log data often contains information directly or indirectly associated with an individual, such as an identifier or location. While such data may be essential evidence when the individual is involved in a security incident, blanket gathering and storage of the usage data of all individuals, for an extended period, not knowing whether or not they are associated with an incident, is often restricted by laws, such as the European General Data Protection Regulation (GDPR). A policy balance must be sought between the benefits of retaining the data for incident tracing, how long this data really remains useful, and the negative risk posed by invasion of privacy or the possibility of the exposure of data (data breach).
How:	The logs generated in the TR1 should be kept for as long as they are necessary, but not longer. This period is not necessarily short, and proper reasons for keeping the logs are for security purposes, accounting, incident response, legal requirements. The logs, naturally, should be properly protected

[3] https://refeds.org/category/research-and-scholarship

	and only available to authorized personnel. Users should be made aware of which of their data is kept and for how long.
Checks:	- a log retention policy is agreed and users are aware of it - logs are stored in a suitably secured manner

TR3 - Traceability Control

Each infrastructure has the following:

What:	*“A specification of the controls that a service provider implements to achieve the goals of [TR1].”*
Why:	Whenever a user passes a control point (authentication, authorization checks) the system should log sufficient information (identifier and attributes checked) to enable a unique path to be constructed back to the user, together with their associated actions, in the event of a security incident.
How:	In order to achieve TR1 (and TR2, for that matter) proper specification of how the logs are generated and accessed should be in place. It should outline the generation of logs, information contained in them, the retention time, access to logs. In addition, Infrastructure may force service providers to specify how such logs will be generated on the service provider side. Most commonly used AAI and logging tools have options to generate and manage the storage of this information in the appropriate format, and the configuration should be checked to ensure completeness of the logs. Service providers are also bound by Infrastructure policies, and the information generated on a service provider’s side is vital to proper functioning of the Infrastructure.
Checks:	- the configuration of tools has been checked against requirements of TR1

Participant Responsibilities [PR]

PRU1 - AUP (Individual Users)

Each infrastructure has:

What:	*“An Acceptable Use Policy (AUP) addressing at least the following areas: defined acceptable and non-acceptable use, user registration, protection and use of authentication and authorisation credentials, data protection and privacy, disclaimers, liability and sanctions.”*

Why:	An AUP brings together all the policy information that a user needs to understand about their use of the infrastructure, including limitations to use and the authority of others to restrict their use, before they are granted access.
How:	A recommended starting point is the WISE Baseline Acceptable Use Policy template available on the WISE website <here>. Guidance on using the WISE Baseline AUP in common scenarios, published by the AARC project, is available here - https://aarc-community.org/guidelines/aarc-i044/
Checks:	- Have an Acceptable Use Policy (AUP) - Check that the AUP covers the areas listed in PRU1 - Copy and augment the WISE Baseline AUP if useful.

PRU2 - User Awareness & Agreement (Individual Users)

Each infrastructure has:

What:	*"A process to ensure that all users are aware of, and accept the requirement to abide by, the AUP. "*
Why:	A user's acceptance of limits to their use of resources, and of the consequences of actions outside of these limits, acknowledges the authority of infrastructure operators to take actions which may affect the user's access to use resources. Knowledge of users' commitment to abide by a published AUP also helps services trust a collection of users across Infrastructure boundaries in a federated environment.
How:	Before a user is granted access to any resources, they must be shown the AUP (see PRU1 above) and required to agree to its terms. This might, for instance, be via a dedicated web page as part of a registration process supported by the membership management software being used, such as SP-IdP-Proxies.
Checks:	- Set up a user registration process in which users accept the AUP - Keep a record of users' registration and agreement to the AUP

PRU3 - Communication of extra requirements (Individual Users)

Each infrastructure has:

What:	*"A process to communicate changes to the AUP to their users that, for example, might arise out of new collaborative partnerships."*

Why:	Ensuring that all users are aware of current AUP requirements is important to ensure that their expectations are aligned with infrastructure requirements and the possibility of inadvertent misuse is avoided.
How:	Significant changes to the AUP must trigger a repeat of the process, or equivalent, described in PRU2 above, which inform users of the new requirements. Implicit in this requirement is that contact information must be recorded and maintained for all users. It is also recommended that the process of AUP acceptance is repeated periodically (recommended as annually) to ensure that all users remain aware of their responsibilities. This repeat also serves to ensure that users remain contactable by removing those who do not respond to the repeat request or whose email is undeliverable
Checks:	- Able to contact users and repeat the PRU2 process if required

PRC1 - Policy Awareness (Collections of Users)

Each infrastructure has:

What:	*“A process to ensure that all collections of users of their infrastructure are aware of, and agree to abide by, infrastructure policy requirements, including the capability to collaborate in the handling of security incidents.”*
Why:	Collections of Users may operate a service that, to maintain the security of the Infrastructure, must abide by Infrastructure security policies. Additionally, those managing Collections of Users are responsible for contacting end users and providing traceability information that may be of help in an incident.
How:	Infrastructure security policies applicable to collections of users must be communicated to those responsible for the collection to ensure that they understand their responsibilities with regard to Infrastructure security. It is recommended that, as a minimum, a top level Infrastructure Security Policy is created defining all participants’ primary responsibilities, including those of collections (communities) of users. The AARC Policy Development Kit provides a template top level policy, with further guidance on its use.
Checks:	- Define a collection’s responsibilities in policy or at least in a top level policy - Have an onboarding process by which access for each collection is enabled - Copy and adapt the AARC top level policy if useful

PRC2 - User Registration & Management (Collections of Users)

Each infrastructure has:

What:	*"Policies and procedures regulating the management of the membership of individual users, including registration, periodic renewal, suspension and removal, including forced removal due to policy violation. These must address the validation of the accuracy of contact information both at initial collection and on periodic renewal."*
Why:	Membership management is crucial to allow Infrastructure Services to trust the validity and accuracy of User attributes sufficiently to be able to grant Users access.
How:	The lifecycle stages of individual users within a collection must be defined and managed from the collection of accurate registration data (with AUP acceptance, see PRU2 above) through to the user's eventual removal from the collection. The AARC Policy Development Kit provides a template Membership Management Policy and further guidance on its use, covering the stages itemised above, as well as personal data protection and record keeping for use in case of a security incident.
Checks:	- Define how collections must manage the lifecycle of their users - Include the verification and periodic testing of users' contact information - Use the AARC Top Level & Membership Management policies if required

PRC3 - Responsibility for Actions (Collections of Users)

Each infrastructure has:

What:	*"A process to inform collections of users that they will be held responsible for the actions of each individual member of the collection, which may affect the ability of all members to utilise the infrastructure."*
Why:	If the Management of a Collection of Users fails to take action against problematic users, Infrastructures must be able to exclude the entire Collection of Users. It is important that Collections of Users are aware of this risk and the associated responsibility.
How:	Policies must make it clear that collections of users will be held collectively responsible for the actions of their members i.e. the actions of one member, in violation of a policy requirement, could result in all the collection's members

	losing access to the infrastructure. The collection onboarding process (PRC1) must reference these policies.
Checks:	- Onboarding collections process addresses collective responsibility

PRC4 - User Identification & Traceability (Collections of Users)

A collection of users has:

What:	*“A process to identify the individual user responsible for an action.”*
Why:	Collections of Users provide the link between identity credentials and an individual User and are essential for managing a security incident, including the collection of evidence.
How:	Related to TR1 above, sufficient information must be logged related to a user’s interaction with the infrastructure to enable actions to be traced back to their originating user. Where users interact indirectly with the infrastructure (job submission, file movement etc.) via a portal interface, those designated as responsible for the portal by the collection must ensure that a complete audit trail is created in the logs of the portal.
Checks	- Log event timestamps and (unique) user identifiers on all systems - Securely store the logs, ideally on a separate system - Document (and test) how to trace events identifying the user across logs

PRC5 - Logs of Membership Management Actions (Collections of Users)

A collection of users has:

What:	*“Appropriate logs of membership management actions sufficient to participate in security incident response.”*
Why:	Being able to understand whether a User was authorised (by the Collection) to take the actions observed at a particular point in time, or whether an identity may have been stolen and misused, could be vital in understanding the origins of a security incident.
How:	As with PRC4 and TR1 above, membership management processes and systems must log information related to events during the lifecycle of a user’s membership of a collection (registration to removal). The information must be retained, securely, for a period of time defined by infrastructure policy.

Checks:	- Save logs of user lifecycle events, including identifiers and timestamps - Have a process to delete saved records older than policy requirements

PRC6 - Define Common Aims & Purposes (Collections of Users)

A collection of users has:

What:	*"Defined their common aims and purposes and made this available to the infrastructure and/or service providers to allow them to make decisions on resource allocation."*
Why:	Each Service Provider has funding, or has otherwise agreed, to provide resources to a particular project or research activity. Defining its 'aims and purposes' allows Service Providers to match resources to appropriate Collections and their Users. As well as allowing resource allocation decisions, whether or not a resource is being misused will depend on under what understanding a user of a service was granted access. Having a Collection make a clear statement of its 'aims and purposes' allows such decisions to be made.
How:	A simple statement such as "to further the science goals of the BIG project" is sufficient and will be asked for by the Infrastructure as part of the Collection's onboarding process.
Checks:	- Define and publish the collection's common aims and purposes.

PRS1 - Compliance Ensurement Procedures (Service Providers)

Each infrastructure has:

What:	*"Policies and procedures to ensure that service providers understand and agree to abide by all applicable requirements in this document, including the capability to collaborate in the handling of security incidents."*
Why:	Establishing trust in the behaviour of Infrastructure participants, including Service Providers, is essential to managing the risk posed to participants by their activity in the Infrastructure, and to enable the necessary exchange of information in the event of an incident. By agreeing to abide by a common set of procedures and policies, Service Providers create an environment where such trust can be fostered.
How:	Compliance with SCI results in requirements placed on service providers, such as log generation and storage. The SCI checklist can be used to make sure that all such requirements are gathered. It is recommended that, as a

	minimum, a Top Level Security Policy is created to fulfill this requirement. The AARC Policy Development Kit provides a template top level policy with further guidance on its use. Define a process by which these requirements are communicated to service providers before their service is attached to the infrastructure.
Checks:	- Define the SP's responsibilities in policy or at least in a top level policy - Have an "onboarding" process, which all service providers go through - Copy and adapt the AARC Top Level policy if useful

Data Protection [DP]

DP1 - Policies for Protection of Personal Data

Each infrastructure has:

What:	*"Defined and enforced policies or a policy framework, together with associated procedures to protect the privacy of individuals according to legal requirements. These controls relate to the processing of their personal data (personally identifiable information) collected as a result of their participation in the infrastructure. Such data includes but is not limited to that used for accounting, user registration, monitoring and logging."*
Why:	Personal data (or personally identifiable information[4]) is inevitably involved in operating the Infrastructure. The personal data referred to here is that relating to the users or operators (e.g. service managers, security officers) of the infrastructure and not personal data which might be included within the science datasets processed or stored on the infrastructure. The latter must be subject to separate contractual arrangements. Usage (processing) of personal data information may have legal ramifications which, for example, may include fines or sanctions imposed for failure to adequately protect users' personal data.
How:	To understand what policies and protection measures need to be put in place it is essential that the Infrastructure first knows what personal information is processed. After understanding what data is processed, and for which purposes, an assessment of the risk posed to the owners (the users) of the data can be made to arrive at a view as to how this information should be protected, including who has access to the data.

[4] We assume the broader definition of personal data defined by GDPR

	Reasons for processing can be multifold, and include for accounting, user registration, security requirements, logging. An example of policy regulating the processing of personal information can be found in the PDK[5].
Checks:	- A list of the personal data being processed is available - An assessment of the risks posed by the processing has been made - Controls have been put in place to adequately minimise the risks - All of the above is documented as a framework of policies and procedures

DP2 - Privacy Policy

Each infrastructure has:

What:	*"A process to make all participants aware, where applicable, that they must provide, in an easily accessible and visible way, a Privacy Policy covering the participant's processing of personal data for purposes necessary for the safe and reliable operation of their service, compliant with the infrastructure policy, or policy framework. This Privacy Policy should, where appropriate, describe the nature and scope of an individual's consent to processing, including rights for correction or erasure, and protections against unauthorised disclosure."*
Why:	All participants in the operation and usage of the Infrastructure (i.e. identity providers, proxies, service providers, users) should be aware what kind of processing of personal data occurs.
How:	All participants (apart from users) should define their own privacy policy. This policy should be clearly visible to the users, and should define which data is processed and why. An example is provided by the PDK[6].
Checks:	- A privacy policy has been defined - The privacy policy has been shown to all owners of personal data processed

REFERENCES

- https://wiki.geant.org/display/WISE/Guidance+for+SCI+version+1

[5] https://docs.google.com/document/d/1QseGQVzUQqvosqhjkF2qlHUI4Swlhgb8oDe8N6NWcqE/edit
[6] https://docs.google.com/document/d/1ZU7VjH3g7qcfWcz0Z8TTv-vQiVoRA_wOsuMyJaz28Og/edit