ICT Security Services
Service Definitions

HEAnet
Ireland's National Education & Research Network

Contents

ICT Security Services – What We Do

What we do.

HEAnet provides a range of ICT Security services. The objective is to provide a standardised set of core security services which are common to all clients. These will be provided using a dedicated HEAnet team to augment the Institutions IT Department resources, whilst using a suite of services which are common, sharable and repeatable across HEAnet clients.

Component One

Security Policy Review and Development

Overview

ICT Security Policies play a critical and strategic role in ensuring an institution's information is managed appropriately and securely. It is important that policies are reviewed and updated on a regular basis to ensure they are in line with business requirements and industry best practices.

Service Methodology

The client will select number of ICT policies for review and / **or** a number of new IT policies developed (please refer to contract to reference amounts available) The service will include:

- An initial meeting /email with HEAnet to discuss the selected policies and how they are implemented within the client's environment.
- A review and comparison of the selected policies will be conducted against the relevant best practices e.g. UCISA, SANS, ISACA
- A meeting / workshop with a HEAnet adviser to discuss gaps and findings, finalise the report and advise of recommended actions.
- Provision of new policies (where applicable) to the institution based on the HEAnet Policy bank using best practices highlighted above.
- Where deemed appropriate sample workflow diagrams to support specific process driven policies.

Service Deliverables

- An observation / point-in-time summary which includes the outcome of the policy review along with any recommendations determined from the review.
- A documented review of the policy with suggestions and recommendations in line with best practice and what is feasible.
- New policies as required (In line with contract caps set out on page X of contract)

Polices in Scope:

The ICT policies would include a range of best practice policies (not limited to)

- Information security policy
- Business continuity management and planning
- Outsourcing and third-party access
- Physical Security

- User Access Management
- Network
- Software
- Mobile computing
- Remote Working
- Cryptography

The above policies may be individual standalone policies or subsets of an overarching Information Security policy.

Service Dependencies:

- Access to relevant policy documents in electronic format
- Availability and access to appropriate staff in the institution e.g. IT Director, Network Administrators, System Administrators, Risk and Legal.

Service Exclusions

- Participation in internal Institution policy review boards or meetings to implement policy changes or related actions e.g. communication plans, training etc.
- Development of institution specific policies (Not included in the HEAnet Policy bank).

Component Two

Security and Risk Assessment of the ICT Environment

Overview

Our Security and Risk Assessment of the ICT Environment service is designed to provide a high-level assessment of the maturity of your Institution's Information Security Program. This service is distinct from an audit or compliance review. The SRA focus on assessing the overall posture of your cybersecurity strategies, identifying potential gaps, and providing insights into areas for improvement.

Key Features

Maturity Level Evaluation

The ICTSS team assesses the current state of your Institution's Information Security Programme, determining its maturity level in alignment with industry best practices. This evaluation helps you understand where your program stands regarding its ability to protect against, respond to, and recover from security threats.

Tailored Questionnaire

Our service includes a comprehensive, proprietary questionnaire designed to gather essential information about your Institution's security practices. The questionnaire covers critical areas such as governance, risk management, incident response, data protection, and more, ensuring a thorough evaluation of your security environment.

Industry Best Practices

The assessment is grounded in recognised security standards and frameworks, ensuring that your Institution is evaluated based on the highest benchmarks in the industry. This approach ensures the ITCSS team's recommendations are relevant, actionable, and aligned with current security trends.

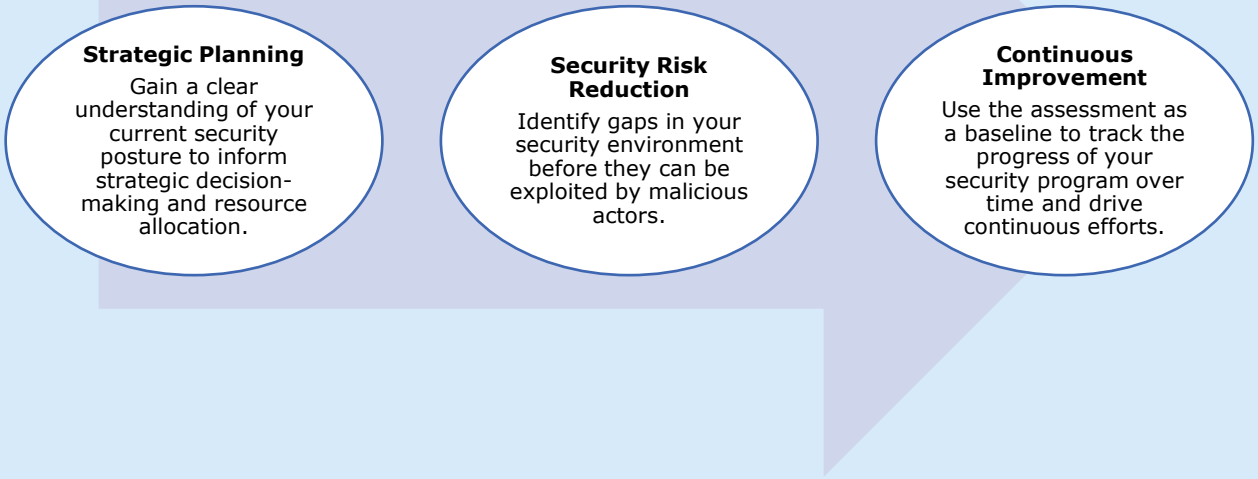
Actionable Insights

Upon completion of the assessment, you will receive a detailed report highlighting the strengths of your current Information Security Program and areas that require improvement.

Benefits

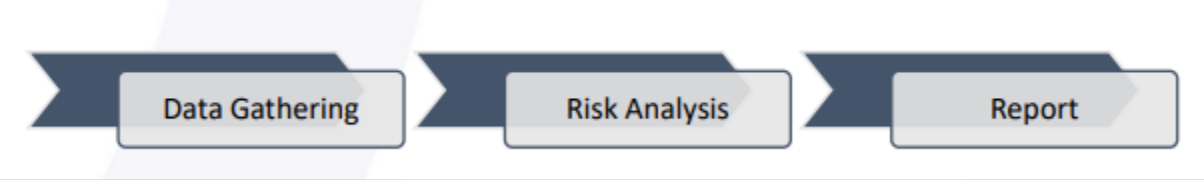
This service is ideal for Institutions seeking to benchmark their information security program, identify opportunities for enhancement, and strengthen their overall cybersecurity resilience.

Benefits of our SRA service



This assessment can also be used to measure progress on a year-to-year basis and provides clients with the opportunity to benchmark their security posture ratings against those of other client institutions should they wish to do so.

Service Methodology



➔ **Step 1 – Data Gathering:**

The high-level assessment of the Institution's ICT environment is carried out through the completion of a questionnaire, discussion and feedback using a methodology developed by HEAnet based on best practices and standards in the cybersecurity industry and aligned with core elements of the ISO/IEC 27001:2022 - Annex A (or ISO 27002), the NIST Cyber Security Framework, and the Cyber Security Baseline Standards for the Irish Public. Besides that, high-level EU GDPR and NIS2 considerations are incorporated where applicable.

➔ **Step 2 – Risk Analysis:**

ICT Security Service team will carry out a risk analysis based on the responses to the questionnaire and discussion with the client using a simple Risk Assessment Matrix. The risk analysis will identify risks and classify them for prioritisation. A workshop will also be conducted with the institution to work through any queries the ICTSS team may have.

➔ **Step 3 – Report:**

The final report will be agreed with the client and document the results of the risk analysis including recommendations and areas for improvement. The report will benchmark the institution against current Information Security best practices.

Service Deliverables

- A review meeting to discuss the report findings and recommendations; AND Report documenting the results/security posture of the risk analysis including recommendations and areas for improvement.

Service Dependencies

- Access to relevant documents in electronic format when appropriate; AND Availability and access to appropriate staff in the institution e.g. IT Director, Network Administrators, System Administrators, Risk and Legal.

Service Exclusions

- This service is not an audit or a compliance review. This service is a HEAnet assessment of an overall posture rather than a certification of a specific standard. Moreover, remediation of gaps identified is not part of this service.
- The scope of all Security and Risk Assessment service conducted by the ICT Security and Services team does not include testing of 3rd party applications and controls operated by 3rd party.

Component Three

Vulnerability Scans (Part 1)

Overview

Security best practices recommend frequent Security and Perimeter Assessments to identify potential vulnerabilities that may be exploited by malicious actors. The ICTSS Security and Perimeter Assessments are classified based on the type of asset, as follows:

- External Network and Perimeter Assessment – which aims at identifying security threats and known vulnerabilities on assets and data within a defined external (internet-facing) network perimeter. *Our service deliverables* will help you identify active hosts/ports and services, files, and metadata publicly available; that could be used to plan further attack strategies against the institution.
- Internal Network Security Assessment – aimed at evaluating the security and access controls of internal network infrastructures. *Our service deliverables* will assist you to identify known vulnerabilities associated to hosts within the defined internal network, possible rogue network assets, over-permissive access controls.
- Cloud Infrastructure Security Assessment – which aims at identifying threats and vulnerabilities associated to assets hosted with cloud providers (e.g., Microsoft Azure, Amazon AWS). *Our service deliverables* will provide you with details of known security issues on both the asset (server/host), as well as cloud-based misconfigurations.

- Each Security Assessment will address a standard scope as defined by HEAnet. This will be based on the level of complexity and effort required in consultation with the client.

A Security Assessment and corresponding report(s) are a point in time view of the vulnerabilities and risk and should be carried out on a regular basis.

Service Methodology

Planning

We will work with you to identify, priorities and schedule required security and perimeter assessments.

Assessment

ICTSS' team will perform a vulnerability assessment and/or configuration review to enumerate, map and;

- Identify and list business assets in scope including both tangible (i.e. data) and intangible (i.e. brand value) assets.
- Identify associated vulnerabilities and insecure configurations to the identified assets (e.g. cloud infrastructure, network devices), which could affect the confidentiality, integrity and availability of services and data.

Risk Analysis

ICTSS will apply a risk-based approach on the likelihood and impact of the perceived vulnerabilities and threats. This will be calculated by evaluating the likelihood of the vulnerabilities being exploited against the possible impact these could have on your infrastructure, as follows:

Likelihood	Impact				
	Informational	**Low**	**Medium**	**High**	**Critical**
Very Likely	Low	Medium	High	Critical	Critical
Likely	Informational	Low	Medium	High	Critical
Possible	Informational	Low	Medium	High	High
Unlikely	Informational	Low	Low	Medium	High
Very Unlikely	Informational	Informational	Low	Medium	Medium

Service Deliverables

On completion of the above risk analysis, ICTSS will provide a Technical report and a separate Management report detailing security issues identified during the network and perimeter assessment. ICTSS will provide a proposed set of recommendations. The final report will include the following:

- Executive Summary.

- Summary of the information that was gathered and the areas that were examined.

Service Dependencies:

ICTSS will need the following in order to provide an end-to-end support during the network and perimeter assessments:

- Permission for scanning known servers / assets within the in-scope perimeter / cloud infrastructure.
- Technical support by technical staff within the institution.
- IP addresses used by the ICTSS will need to be whitelisted.

Service Exclusions

The security assessment service does NOT include:

- Mitigation of the risks identified in the report
- Network or security architecture reviews
- Penetration testing (This service is provided by ICTSS as per service definition
- Network architecture assessments
- Security architecture assessments
- Cloud vendor assessments due diligence
- Application architecture assessments, code testing or code reviews

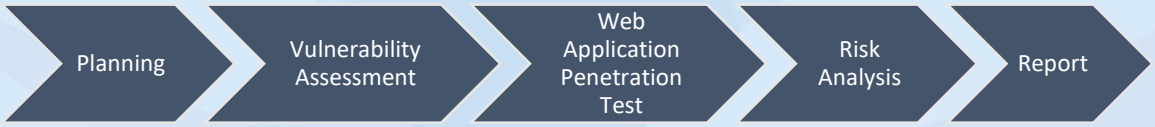
Penetration Testing (Part 2)

Overview

Penetration Testing aims to identify security vulnerabilities, the likelihood of these being exploited and the impact of these could have on the confidentiality, integrity and availability of data and services provided by the in-scope application.

Penetration tests play a critical role within every organisation, as many of the vulnerabilities and threats identified through manual testing, are normally missed by common vulnerability scanners.

Service Methodology



Planning

We will work with the institute to identify and establish a time frame to conduct assessment, review, and delivery of the technical and management reports.

Vulnerabilities Assessment

ICTSS team will perform a vulnerability assessment to enumerate, map and;

- Identify and list business assets in scope including both tangible (i.e. data) and intangible (i.e. brand value) assets.
- Identify associated vulnerabilities and insecure configurations to the identified assets, which could affect the confidentiality, integrity and availability of services and data.

Web/Cloud Application Penetration Test

ICTSS team will then perform manual testing of vulnerabilities, as well as threats associated to entry points identified during the previous phase. This process is accompanied by the web application penetration test which uses OWASP (Open Web Application Security Project) Application Security Verification Standard (ASVS).

It should be noted; the application penetration test will depend on the access levels granted to the ICTSS team, as well as the purpose and available use cases within.

Risk Analysis

ICTSS will apply a risk-based approach on the likelihood and impact of the perceived vulnerabilities and threats. This will be calculated by evaluating the likelihood of the vulnerabilities being exploited against the possible impact these could have on your infrastructure, as follows:

Likelihood	Impact				
	Informational	Low	Medium	High	Critical
Very Likely	Low	Medium	High	Critical	Critical
Likely	Informational	Low	Medium	High	Critical
Possible	Informational	Low	Medium	High	High
Unlikely	Informational	Low	Low	Medium	High
Very Unlikely	Informational	Informational	Low	Medium	Medium

Service Deliverables:

On completion of the above risk analysis, ICTSS will provide a Technical report and a separate Management report detailing security issues identified during the web application penetration test. ICTSS will also provide a proposed set of recommendations. The final report will include the following:

- Executive Summary
- Summary of the information that was gathered and the areas that were examined

Service Dependencies:

ICTSS will need the following in order to provide an end-to-end support during the web application penetration test:

- Permission for testing by the application owner.
- Technical support by the web application owner / technical staff.
- IP addresses used by the ICTSS penetration testers will need to be whitelisted.

Service Exclusions:

The Penetration Testing service does NOT include:

- Application architecture assessments, code testing or code reviews
- Network architecture assessments
- Security architecture assessments
- Cloud vendor assessments due diligence
- Implementing fixes for defects found during the test

Component Four

General Security Awareness Training (Part 1)

Includes live and on demand training

Overview

One of main sources of ICT security exposure may be the users within the institution. Users may expose the institution to risks by their behaviour whether maliciously or through bad practices or lack of understanding. Educating users is an important part of an organisation's approach to minimising and mitigating risk so that users understand potential threats that the business could be exposed to e.g.

- Password Management
- Phishing
- Ransomware
- How to stay safe online

HEAnet will provide a general security awareness training programme delivered online or face to face training The security awareness training is aimed at Faculty staff and tailored to the needs of the Irish Education and Research sector.

Service Methodology

- General Security Awareness training course (approx. 1 hour in duration)
- HEAnet will provide and update the training content as appropriate based on the latest developments in ICT Security and Risk, feedback from users and clients.
- Training will be conducted either in person or online, based on the preference of the client.

Service Deliverables:

- A training course accessible to nominated staff of the institution delivered as a group training session.
- Maximum session number of one hundred attendees (100) per session for online training and One hundred (100) for face-to-face sessions.
- Top Tips document for all attendees.

Service Dependencies:

- The client communicating course details to all relevant staff where appropriate Training is hosted by HEAnet via MS Teams Webinar. Faculty staff can register for training using a registration link prepared by HEAnet and distributed by the client.

On Demand Training (Available January 2025)

- A managed service provider for Cybersecurity eLearning which will include key elements such as
  - Report Management
  - Learner Upload
  - Distribution of eLearning (access for learners)
  - Up to 500 learners per client per year can be trained

A variety of eLearning tools to choose from including

- Videos
- Quizzes
- Simulations

Customisation of Platform for each client

- Client Logo
- Client specific access
- Client specific learning will be available in April 2025 such as custom videos and PDFs.

Phishing Simulations (Part 2)

Overview

Phishing simulations are a very important part of the security awareness training, as they allow institutions to assess how their staff handle phishing attacks by sending realistic phishing emails to the staff. The resulting statistics can then be used by the institution to establish a baseline security level, as well as to identify areas of improvement in terms of security awareness.

The phishing campaigns provided by the ICT Security Services team can be tailored to specific users or departments and can be further refined to send out the phishing emails at various phases throughout the assessment. HEAnet gives you broad control over the target, time, and appearance of phishing campaigns.

Service Methodology

Planning of Engagement

We will work with you to identify and establish a time frame to conduct phishing simulation, review, and delivery of management report.

Fieldwork

HEAnet ICTSS team will create relevant elements for running phishing campaigns as per statement of work.

Report

We will provide you with a written management report detailing statistics for the in-scope phishing campaigns, as well as recommendations to improve employee's security awareness. The final report will include the following:

- Executive Summary.
- Review and statistics of the information that was gathered and the areas that were identified, and recommendation.

Service Dependencies:

ICTSS will need the following to provide an end-to-end support:

- Target list with email addresses for each of the phishing campaigns.
- Relevant email templates (where appropriate) and / or email address you want to be used for the simulation. Point of contact prior to simulation to test elements as deemed appropriate.
- Domains and email addresses created by the ICTSS team will need to be whitelisted by the client.

Service Exclusions:

The service does NOT include:

- Vulnerability assessment or penetration test of client's infrastructure
- Denial of Service (DoS) activities
- Review or development of Information Security policies, standards, and processes

Component Five

Access to Cyber Security Competence

Overview:

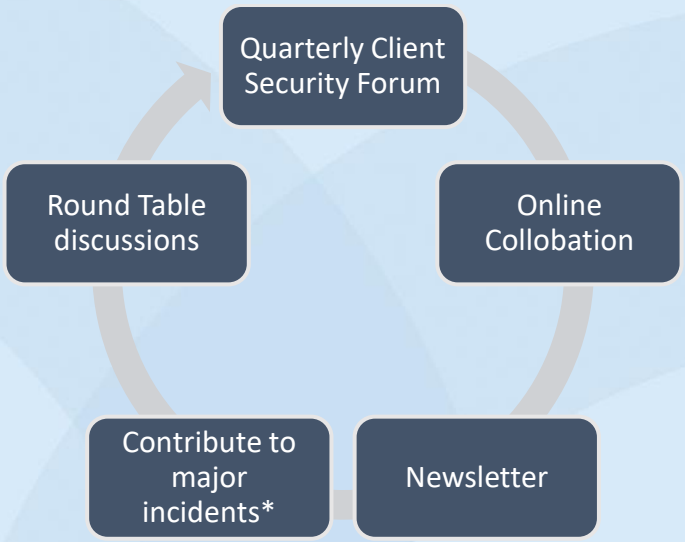
The objective of this component of the ICT Security services is for HEAnet to take a leadership role to advise and assist clients on their security and risk challenges by providing access to security and risk competencies in key areas. HEAnet has a broad range of ICT security skills which it will continue to develop and share with clients through a variety of channels.

Service Methodology:

HEAnet will provide access to Cyber Security Competencies to clients using several channels (please see Service Deliverables). HEAnet will leverage its existing expertise and develop its knowledge and competencies in Security by utilising leading security organisations guidance such as UCISA, ISACA and ISC2 as well as developing existing relationships with other NRENs and GÉANT.

Service Deliverables:

HEAnet will provide access to its expert advice using several channels appropriate to the topic and staff participating including:



- Client Security Forums hosted on a quarterly basis to facilitate collaboration across the sector.
- Client Security Forums on topics identified by the clients of the ICTSS Service.
- Online Security forum to communicate to the broader HEAnet client community (collaboration)
- Bulletins of high profile/client affecting incidents.
- Round table discussions based on client ideas and requests
- *Contribute where appropriate to a sectoral response to a major incident (on a best effort basis)

Service Dependencies:

- Availability of key staff with ICT security skills in HEAnet (or external), the HE sectors and willingness to share and collaborate openly (within an agreed confidentiality/Non-Disclosure Agreement policy).
- Identify key competency skills/focus areas for HEAnet to develop on as areas of expertise.

Service Exclusions:

- This service does NOT include 24/7 on-call support
- This service does NOT include operational support e.g. incident management.

Contact HEAnet

Telephone: +353 1 660 90 40
Email: ictsecurityservices@heanet.ie

HEAnet CLG
3rd Floor, North Dock Two,
93-94 North Wall Quay,
Dublin 1,
Ireland

Reviewed 18.12.2024
Registered in Ireland No: 275301
Charities Regulator No: 20036270