POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	Special Interest Groups Contact List
Effective Date:	14 Feb 2019
Reference Number:	ISMS-03-13
Version Number:	1.5
Owner:	Information Security Manager,
Review Date:	02 Nov 2019

Table of Contents

1. Purpose

Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

This document provides a list of the groups that can provide support, information, examples of best practice and updates in regard to the changing requirements of information security. This includes information on regulatory changes, new security vulnerabilities and security threats, and forums for discussing information security issues and processes.

This document also provides details of both free-to-join and subscription groups.

2. Scope

Details of special interest groups involved in the topics of information security, and the roles responsible for maintaining interaction with one or more of these identified groups or equivalent communities.

3. Responsibilities

The TRE Operations Manager is responsible for:

- Monitoring and updating the details of the groups listed below
- Maintaining contact with at least one of the groups
- Reporting regulatory changes and suggestions of improvement to the senior management team

Process Owners are responsible for:

- Maintaining awareness of the wider community related to their ISMS Process and making recommendations to add an SIGs to this document

Any CHI personnel may join a special interest group and report suggestions for system improvement via the Q-Pulse wizard.

Note: Requests to groups requiring a membership fee will require approval from the operations manager.

4. Procedure

4.1. Purpose of Special Interest Groups

The purpose of special interest groups (SIGs) is to provide a forum for collaborative approaches to the issues of information security and best practices. These groups are mostly specialised around specific information security topics and aim to share and develop knowledge.
Annex A of the ISO 27001 standard suggests contact with such groups as a way to keep on top of changes to regulatory requirements, alerts, threats and best practices.

4.2. What can be classified as a Special Interest Group?

A Special Interest Group (SIG) is a community, usually within a larger organisation, with a shared interest in advancing a specific area of knowledge, learning or technology where members cooperate to affect or to produce solutions within their particular field, and may communicate, meet, and organise conferences. These groups may be professional organisations, or originate from manufacturers' client bases, government forums or other specialised communities.

4.3. Information from Special Interest Groups

Due to the diverse origins of SIGs, it is necessary to be cautious of the quality of information being obtained from such sources. Information obtained from these groups could potentially impact on the information security management system (ISMS) and therefore any staff member interacting with these groups should consider:

- The quality of the information – has the information come from a user forum, has it been supported by references?
- How frequently the group is updated – is the group regularly updated with current threats or alerts?
- Legitimacy of the information source - is the group provided by a reliable professional organisation, or is it recognised by security peers?

Regardless of the source of the information, any changes to ISMS process, policy or procedure must first be risk assessed before implementation is agreed by senior management.

4.4. Special Interest Group Details

Association for computing Machinery: Catalogue of SIGs http://www.acm.org/sigs/	Free List of groups	Full range of topics
Information Security Systems Association https://www.issa.org/?page=SIGs	Free SIG log in option	I.S. for Healthcare, Security awareness
27001 Academy http://advisera.com/27001academy/?icn=homepage-27001&ici=top-27001academy-txt	Free 27001 course and information	Requires users to sign up to a mailing list to access some free features
Gael Portal – Ideagen (Q-Pulse) http://customer.gaelquality.com/	Free	Q-Pulse help and support
Information Security Forum https://www.securityforum.org/	Some free tools Membership is required	Information security
Security TechCenter https://technet.microsoft.com/en-us/security/dd252948.aspx	Free to join email alerts	Microsoft Technical Security Notifications
BRENT OZAR		

https://www.brentozar.com/responder/	Free	SQL Server first Responder Kit
University of Manchester IT Tech Listserv its-tech-info@listserv.manchester.ac.uk	Free	Email alerts
UK Anonymisation Network http://ukanon.net/join-the-network/admin@ukanon.net	Free advice on anonymisation of data	Email alerts
Secure Data Working Group securedatagroup.org	UK data safe haven professionals	Meet every few months to discuss safe data access

5. Cross-referenced ISMS Documents

Number	Type	Title

6. Appendices

None