CPNI
Centre for the Protection of National Infrastructure

Insider Threat Stakeholder Group – Terms of Reference Template

PUBLISH DATE: August 2020

CLASSIFICATION: Official

CPNI's Insider Risk Mitigation Framework highlights the recommended approach an organisation should adopt to develop their Insider Threat Programme to reduce insider risk. A key component of this framework includes standing up an Insider Threat Stakeholder Group (ITSG).

CPNI's Insider Risk Mitigation Framework can be found here

The ITSG provides your Insider Threat Programme with the appropriate level of ownership and compliance to develop policies, procedures and guidance and to make appropriate insider risk decisions with confidence.

Below is a template outlining an ITSG's Terms of Reference to support your organisation when setting up this group.

Introduction Insider Threat Stakeholder Group (ITSG) – Terms of Reference

1. Definition of Insider

1.1 An insider is an individual who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes.

2. Purpose of Group

2.1 The ITSG will have responsibility for managing the Insider Threat Programme which aims to reduce Insider Risk in [Organisation name]. The activities of the ITSG will support organisational security development and security risk reduction through the best use of insider risk mitigation strategies. Through the application of security risk management best practice, the ITSG will ensure organisational security measures are demonstrably pragmatic, proportionate and effective.

3 Membership

3.1 Nominated individual [Senior Executive of Organisation Name] will be responsible for overseeing and supporting the objectives of the Insider Threat Stakeholder Group.

3.2 Group Chair (duration of Chairperson to be confirmed) will be responsible for meeting scheduling, setting agenda, chairing meeting and reporting to Organisation

Senior Executive / Organisation Governance arrangements in place on ITSG's progress on agreed objectives.

3.3 ITSG representatives will include those who have deep knowledge of particular employee roles for their business area and the authority to understand the entirety of the business needs and existing working practices to support the implementation of any insider risk mitigation measures.

Organisational structures will vary however consideration of ITSG representatives from the following business areas may be considered – Physical Security, Information Technology, Operational Technology, Technical Specialists, Information Specialist, Senior HR, Senior Vetting, Facilities Manager, Contract Management, Procurement, Finance, Counter Fraud, Legal, Training, Communications and Staff/Trade Union Rep.

Stakeholders who may not be employed by your Organisation, but play a vital role in contributing to the group's discussions should also be considered for membership. This may include those providing threat or protective security advice (CTSA, Local Police Force, CPNI, neighbouring security managers or business partners).

If the organisation has multiple stakeholders (for example an Airport Operator) that are critical to supporting an Insider Threat Management Programme extending membership of group is strongly recommended.

4. ITSG Aims & Objectives

4.1 The ITSG will own and manage the Insider risk assessment process on behalf of the Board, Senior Executive or SRO for [Organisation Name] Insider Threat Programme.

4.2 To achieve the above the ITSG will develop a clear understanding of [Organisation name] insider risks (documented) posed by workers based on their level of access to critical assets/systems as follows;

- Identify, categorise and/or classify assets/systems based on importance;
- Identify threats to these assets;
- Calculate risks based on likelihood and impact of threats transpiring;
- Prioritise assessed Insider risks;
- Starting with highest priority risks, the ITSG will identify what countermeasures are in place to mitigate the identified risks and evaluate whether these are sufficient.

Where existing mitigations are identified as inadequate, additional cost effective and proportionate security mitigations which seek to reduce the likelihood and impact of the threat to an acceptable level (based on Organisation X's risk appetite) should be documented and submitted to [Organisation Senior Level] for sign off and implementation;

- [Organisation Name] will record the data gathered in a risk register to support senior decision makers to make informed judgements on risk appetite and resource allocation and ensure effective audit of decision making;
- Subject to senior owner sign off, ITSG to work with relevant business areas to implement (following prioritisation process) identified security mitigations with ITSG action owners assigned;
- ITSG to adopt a continuous review of insider risks and mitigations to measure the effectiveness of any resources used and that it correctly reflects the threats and vulnerabilities in [Organisation Name].

5. Meetings

5.1 Supporting the ITSG's aims;

- Identify [Organisation Name's] assets/systems;
- ITSG to seek current threat related information on Insider Activity from 3rd Parties (Police Partners/ CPNI/Lead Government Department) to inform the assessment process at each meeting;
- ITSG to review Insider Risk Register and RAG rating of each risk;
- ITSG Action Owners to discuss work streams and provide an update on status at each meeting;
- ITSG to provide report [frequency TBC] to Organisation Senior's on progress of group – highlighting progress made, blockers, decisions that need Senior sign off.
- ITSG to identify trends in insider threat within the organisation and recommend actions to mitigate these.

6. Administration

6.1 The ITSG should meet no less than every quarter. However, this frequency should be increased whilst the group is first being stood up and objectives commence.

6.2 In the event of change in threat level and or operating environment, an incident, near miss or 3rd party report of insider activity the ITSG should consider how to urgently convene out of meeting to discuss and review risk [Organisation name] and update the risk register accordingly. Information flows should also be considered to keep Seniors informed of any change in risk via the ITSG's reporting mechanisms.

6.3 The ITSG may convene sub sets of the ITSG membership based on a review of requirements and the need for confidentiality. All stakeholders are therefore required to sign a code of conduct confirming they have read and agree to follow [Organisations Name] ITSG's security protocol and information handling caveats, and may require additional levels of background checks.

6.4 Minute taking of the ITSG will be rotated across ITSG members.

CPNI
Centre for the Protection of National Infrastructure

ITSG Training

For the initial meeting it is recommended that an Insider Threat Awareness Briefing is delivered to ITSG representatives. Whilst the terminology 'Insider' may have been used previously by individual stakeholders it is vital that there is a common level understanding of what constitutes insider activity from the outset for the ITSG.

Organisations should give careful consideration as to who delivers this briefing to the ITSG. *[CPNI Advisors can support organisations in briefing material and signposting to relevant resources].*

The awareness briefing should cover;

- Insider Threat Terminology;
- Types of Insider Activity;
- Types of Insider Behaviour (Deliberate / Opportunistic / Exploited or Recruited / Unwitting / Leaver);
- Motivations insider Activity;
- Case Studies of Insider Activity (make it relevant to your organisation's business e.g. for a Bank use a previous example of financial corruption within the banking sector);
- Overview of what needs to be in place as part of an effective Insider Threat programme;
- Explain clearly the role of the ITSG and how they will play their part in contributing to the group.

The diagram below will help explain what an effective Insider Threat Mitigation Programme should include;