Health & Social Care Information Centre

Health and Social Care Information Centre

Information Assurance and Cyber Security Committee (IACSC)

Terms of Reference

Date: 2014-15

Contents

1 Introduction

These terms of reference have been produced based on the specimen good practice versions provided in both the Department of Health and HM Treasury Audit Committee Handbooks. They have been slightly amended to reflect the views and wishes of the Committee members.

2 Constitution

The HSCIC Board hereby resolves to establish a Committee of the Board to be known as the Information Assurance and Cyber Security Committee (IACSC).

3 Membership

The Information Assurance and Cyber Security Committee will be appointed by the HSCIC Board from amongst the independent non-executive Directors of the HSCIC and will comprise three members. A quorum will be two members along with either the HSCIC's SIRO[1] or Caldicott Guardian.

The Chair of the HSCIC Board will not be a member of Information Assurance and Cyber Security Committee. The HSCIC Board will appoint the Chair of the Committee from amongst the independent non-executive Directors and this appointment will be reviewed on an annual basis.

4 Attendance

The Information Assurance and Cyber Security Committee will normally be attended by:

- The Chief Executive Officer;
- The Director of Operations and Assurance Services, who as SIRO will cover information governance and information risks;
- The Chief Technology Officer, once appointed;
- The Director of HR;
- Caldicott Guardian; and
- Cross-Government representatives, led by Cabinet Office.

A representative from the Department of Health Sponsor Team may also be invited to attend.

The Secretary of Information Assurance and Cyber Security Committee will be the HSCIC Board Secretary.

5 Access

Representatives of sub-groups of the Information Assurance and Cyber Security Committee will have free and confidential access to the Chair of the Committee.

[1] Senior Information Risk Owner

6 Frequency

Meetings shall be held not less than four times a year, but will meet more regularly, initially as the delivery of the Cyber Security Programme (CSP) needs ongoing oversight or if other circumstances dictate.

7 Authority

The Information Assurance and Cyber Security Committee is authorised by the Board:

- To investigate any activity within the terms of reference. It is authorised to seek any information that it requires from any employee and all employees are directed to cooperate with any request made by the Information Assurance and Cyber Security Committee

- To obtain outside legal or independent professional advice, at the HSCIC's expense, and to secure the attendance of outsiders with relevant experience and expertise if it considers this necessary.

8 Duties

The duties of the Information Assurance and Cyber Security Committee can be categorised as follows:

8.1 Internal control and risk management responsibilities

The Information Assurance and Cyber Security Committee shall review and monitor the effectiveness of the system of integrated governance, risk management and internal control relating to information assurance; information governance; cyber and other security; and data quality.

Corporate Strategic and Operational risks are recorded on the Corporate Risk Registers and actively managed by the Executive team. The Information Assurance and Cyber Security Committee will provide oversight, review and challenge of the detailed Information Assurance/Information Governance/Cyber Security risks that are maintained across the organisation.

In particular, the Information Assurance and Cyber Security Committee will review the adequacy of and make recommendations to the Board or the Assurance and Risk Committee as identified below:

Assurance and Risk Committee

- Input and recommendations to risk and control related disclosure statements, (in particular the Annual Governance Statement) prior to the endorsement of the Board

- The operational effectiveness of policies and procedures

The HSCIC Board

- The underlying assurance processes that indicate the degree of the achievement of corporate Information Assurance and Cyber Security objectives, the effectiveness of the management of threats and risks to HSCIC information systems

- The structures, processes and responsibilities for identifying and managing key Information Assurance and Cyber Security risks facing the organisation

- The policies for ensuring that there is compliance with relevant regulatory, legal and code of conduct requirements as set out in the Controls Assurance Standards and other relevant guidance

In carrying out this work the Information Assurance and Cyber Security Committee will primarily utilise the work of the Information Assurance and Standards Assurance functions. It will also seek reports and assurances from directors and senior managers as appropriate.

8.2 Information Assurance

The Information Assurance and Cyber Security Committee will ensure that there is an effective Information Assurance function established by management that meets recognised industry and Government standards and provides appropriate independent assurance to the Chief Executive and Board. This will be achieved by:

- Reviewing and making recommendations to the Board on the structure, function and remit of the Information Assurance function.

- Reviewing the operation of Information Assurance functions, considering the major findings of investigations (and management’s response), and ensuring co-ordination between relevant expertise areas.

- Ensuring that the Information Assurance function is adequately resourced and has appropriate standing within the organisation

- Annual review of the effectiveness of the Information Assurance function.

8.3 Cyber Security

The Information Assurance and Cyber Security Committee will review the work and findings of the Cyber Security Programme and take account of the implications and management responses to their work. This will include:

- Acting as an effective Programme Board providing the strategic direction for the Cyber Security Programme.

- Reviewing and making any recommendations to the Board as necessary on reports relating to Information Assurance and Cyber Security.

8.4 Other Assurance Functions

The Information Assurance and Cyber Security Committee will review the findings of other significant assurance functions, both internal and external to the organisation, and consider the implications to the governance of the organisation.

The Information Assurance and Cyber Security Committee will ensure that the appropriate sub-groups are put in place for following Information Assurance functions:

- Data Access
- Corporate Information Security
- Programme Information Assurance
- Management Systems and Standards
- Other required bodies and legal boards

In addition, the Information Assurance and Cyber Security Committee will review the work of other committees within the organisation, whose work can provide relevant assurance to the Information Assurance and Cyber Security Committee's own scope of work.

8.5 Management

The Information Assurance and Cyber Security Committee will request and review reports and positive assurances from directors and senior managers on the overall arrangements for governance, security and internal control.

The Information Assurance and Cyber Security Committee may also request specific reports from individual functions within the organisation as they may be appropriate to the overall arrangements.

9 Reporting

The minutes of the Information Assurance and Cyber Security Committee meetings will be recorded and maintained. The Chair of the Information Assurance and Cyber Security Committee will report verbally to each HSCIC Board meeting with any required discussion points being raised to the private session of the Board.

The Information Assurance and Cyber Security Committee will report to the Board annually on its work in support of the Annual Governance Statement.

The Information Assurance and Cyber Security Committee will annually review its terms of reference and its own effectiveness and recommend any necessary changes to the Board.