www.pwc.co.uk

Internal Audit Risk Assessment and Plan 2016/17

FINAL

NHS Grampian

March 2016

pwc

Contents

Distribution List	
For action	Assistant Director of Finance
For information	Audit Committee

This document has been prepared only for NHS Grampian and solely for the purpose and on the terms agreed with NHS Grampian.

1. Introduction and approach

Introduction

The following paper sets out our indicative Internal Audit Plan for 2015/16, along with indicative timings for review and a brief description of the expected scope of the review. As such, this Plan is a draft document for consideration and comment.

Approach

The internal audit service will be delivered in accordance with the Internal Audit Charter. A summary of our approach to undertaking the risk assessment and preparing the internal audit plan is set out below. The internal audit plan is driven by NHS Grampian's organisational objectives and priorities, and the risks that may prevent NHS Grampian from meeting those objectives. A more detailed description of our approach can be found in Appendix 1 and 2.

Step 1 Understand corporate objectives and risks	• Obtain information and utilise sector knowledge to identify corporate level objectives and risks.
Step 2 Define the audit universe	• Identify all of the auditable units within the organisation. Auditable units can be functions, processes or locations.
Step 3 Assess the inherent risk	• Assess the inherent risk of each auditable unit based on impact and likelihood criteria.
Step 4 Assess the strength of the control environment	• Assess the strength of the control environment within each auditable unit to identify auditable units with a high reliance on controls.
Step 5 Calculate the audit requirement rating	• Calculate the audit requirement rating taking into account the inherent risk assessment and the strength of the control environment for each auditable unit.
Step 6 Determine the audit plan	• Determine the timing and scope of audit work based on the organisation's risk appetite.
Step 7 Other considerations	• Consider additional audit requirements to those identified from the risk assessment process.

Basis of our plan

The level of agreed resources for the internal audit service for April 2016 to March 2017 is £135,000. Within our proposal for Internal Audit services for the period 2014-2017, we set out our three year strategic plan for NHS Grampian based on our assessment of your risks at that date. We recognise that risks change over time, which is why it is important that we review and update our risk assessment at least annually to take account of these changes and adjust our Internal Audit Plan accordingly.

Basis of our annual internal audit conclusion

Internal audit work will be performed in accordance with PwC's Internal Audit methodology which is aligned to the Public Sector Internal Audit Standards. As a result, our work and deliverables are not designed or intended to comply with the International Auditing and Assurance Standards Board (IAASB), International Framework for Assurance Engagements (IFAE) and International Standard on Assurance Engagements (ISAE) 3000.

Our annual internal audit opinion will be based on and limited to the internal audits we have completed over the year and the control objectives agreed for each individual internal audit. The agreed control objectives will be reported within our final individual internal audit reports.

In developing our internal audit risk assessment and plan we have taken into account the requirement to produce an annual internal audit opinion by determining the level of internal audit coverage over the audit universe and key risks.

Other sources of assurance

In developing our internal audit risk assessment and plan we have taken into account other sources of assurance that are available, such as external inspections, external audit work, and ISO accreditations. We do not intend to place reliance upon these other sources of assurance.

2. Audit universe and strategic risks, themes and objectives

Audit universe

The diagram below represents the high level auditable units within the audit universe of NHS Grampian. These units form the basis of the internal audit plan.
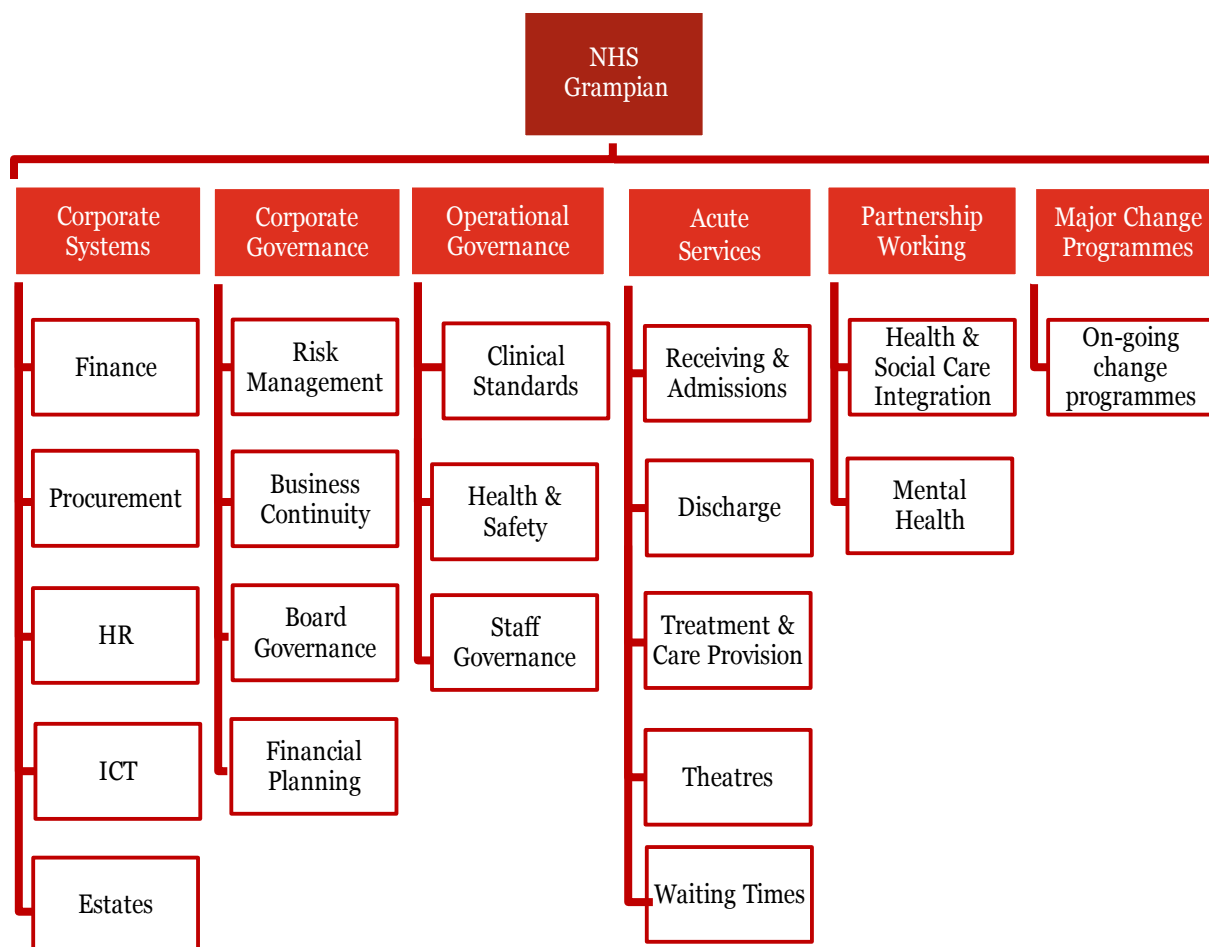
Strategic risks, themes and objectives

Strategic level risks, themes and objectives have been determined by NHS Grampian. These are recorded within Appendix 1 and have been considered when preparing the internal audit plan

3. Risk assessment

Risk assessment results

Each auditable unit has been assessed for inherent risk and the strength of the control environment, in accordance with the methodology set out in Appendix 2 and 3. The results are summarised in the table below.

Ref	Auditable Unit	Inherent Risk Rating	Control Environment Indicator	Audit Requirement Rating	Colour code	Frequency
A	**Corporate systems**					
A.1	Finance	6	5	4	🔴	Annual
A.2	Procurement	5	5	3	🟠	Every two years
A.3	HR	5	5	3	🟠	Every two years
A.4	ICT	6	5	4	🔴	Annual
A.5	Estates	5	3	4	🔴	Annual
B	**Corporate Governance**					
B.1	Risk Management	3	3	2	🟡	Every three years
B.2	Business Continuity Planning	5	4	3	🟠	Every two years
B.3	Board Governance	3	3	2	🟡	Every three years
B.4	Financial Planning	5	4	3	🟠	Every two years
C	**Operational Governance**					
C.1	Clinical Standards	5	4	3	🟠	Every two years
C.2	Health and Safety	3	3	2	🟡	Every three years
C.3	Staff Governance	3	3	2	🟡	Every three years
D	**Acute services**					
D.1	Receiving and Admissions	4	3	2	🟡	Every three years
D.2	Discharge Process	6	3	5	🔴	Annual
D.3	Treatment and Care Provision	5	5	3	🟠	Every two years
D.4	Theatres	4	4	2	🟡	Every three years
D.5	Waiting Times	4	4	2	🟡	Every three years
E	**Partnership Working**					

Ref	Auditable Unit	Inherent Risk Rating	Control Environment Indicator	Audit Requirement Rating	Colour code	Frequency
E.1	Health and Social Care Integration	6	5	4	🔴	Annual
E.2	Mental Health	4	3	3	🟠	Every two years
F	**Major Change Programmes**					
F.1	On-going Change Programmes	6	4	4	🔴	Annual

Key to frequency of audit work

Audit Requirement Rating	Frequency	Colour Code
6	Annual	🔴
5	Annual	🔴
4	Annual	🟠
3	Every two years	🟡
2	Every three years	🟡
1	No further work	🟢
	Key areas of focus	🟡🔴

4. Annual plan

Annual plan and indicative timeline

The following table sets out the internal audit work planned for April 2016 to March 2017, together with indicative dates for each audit.

Ref	Auditable Unit	Proposed review	Q1	Q2	Q3	Q4	Proposed scope of review (high level)
A							
A.1	Finance	Key Financial Controls				Q4	Review of key financial controls: purchase & payables, income & debtors, payroll, bank & cash and asset management
A.1	Finance	Property Transaction Monitoring		Q2			Review of disposal and acquisition of property by during 2015/16 in accordance with the Scottish Government Health Directorate's Property Transaction Manual.
A.2	Procurement	Family Health Service Contractors			Q3		A review of the management arrangements for Family Health Service contractors, specifically reviewing how they are held accountable against the requirements of their contracts with NHS Grampian.
A.4	ICT	Data Quality in Management Information		Q2			A review of the processes in place around management information to ensure quality of data used in developing the Board's strategic plans. Areas to consider could include: processes and controls around data collection and input, and robustness of management information systems. Scope also to include consideration of the process and controls for the review and sign off of external information returns and communication by Senior Management.
A.4	ICT	Cyber Security			Q3		A review of cyber security maturity, assessing how the Board identifies cyber threats and risks, and how it develops responses to those threats and risks.
A.5	Estates	Project Management of Non-Capital Change Projects				Q4	A review of management arrangements for non-capital change projects. Full scope to be agreed with management but to include consideration of the strategy for the allocation of accommodation and processes for decision making for non-clinical support functions.

Ref	Auditable Unit	Proposed review	Q1	Q2	Q3	Q4	Proposed scope of review (high level)
B							
B.3	Board Governance	Governance Statement				Q4	Assess the evidence provided by NHS Grampian to support the Accountable Officer's completion of the Governance Statement.
C							
C.3	Staff Governance	Staff Continuity and Planning	Q1				A review of staff continuity and succession planning, including; identification of critical roles, process for identifying capacity and where staff are stretched, assessment and identification of staff requirements for personal development and support.
D							
D.3	Treatment and Care Provision	Homecare Prescribing Services		Q2			We will examine the controls in place around the operation of the Homecare Service , including reviewing the following key areas; • Appropriate processes are in place for the registration of patients with medicines homecare services; • Notification of intention to supply medicines though a homecare service provider is sent to the patient's General Practitioner; • Appropriate processes are in place to ensure patients from the rheumatology, dermatology and MS service prescribed medicines under a homecare arrangement are reviewed to establish whether the treatment is effective; and • Appropriate processes are in place for notification of any problems or errors within medicines homecare services.

Ref	Auditable Unit	Proposed review	Q1	Q2	Q3	Q4	Proposed scope of review (high level)
D.4	Theatres	Theatre Utilisation	Q1				The sub-processes and related control objectives included in this review are: • Policies and Procedures are in place to help staff maximise theatre utilisation; • Governance arrangements are in place to monitor and report on theatre utilisation, including actions taken to ensure theatre utilisation is maximised, the sharing of lessons learnt across theatres, and across sites; • Processes are in place to review the use of locum doctors to support and sustain services; • Arrangements are in place to monitor and report theatre utilisation performance by specialty, theatre, and site; • Processes are in place to proactively manage potential DNAs (did not attends), operation overruns and appointments cancelled as not fit for surgery; and • NHS Grampian has processes in place to participate in the national benchmarking reporting managed by the National Theatre Implementation Group.
E							
E.1	Health and Social Care Integration	Health and Social Care Integration – Resource Allocation and Staff Governance			Q3		Review to include consideration of the processes for allocating resources to the Integrated Joint Boards (IJBs) and the arrangements for staff governance for NHS Grampian staff working as part of the IJBs.
E.2	Mental Health	Patient Management in Mental Health Acute Services			Q3		The overall objective of this internal audit review would be to consider the arrangements in place for patient management within mental health acute services. The review would consider the following areas: • Performance targets; • Information management; and • Reporting and monitoring of performance and actions. Our approach would include interviews with mental health services operational and performance management staff as well as the review of reports and documentation associated with managing performance in patient management.

Ref	Auditable Unit	Proposed review	Q1	Q2	Q3	Q4	Proposed scope of review (high level)
F							
F.1	On-going Change Programmes	Digital Strategy	Q1				A review of the Board's IT and digital strategy. Areas to consider could include; how the Board is utilising technology to enhance services, how the IT and digital strategy links to the Board's overall strategy and vision, and how the Board manages technology risks.
	Follow Up		Q1	Q2	Q3	Q4	Follow-up of actions taken to address high priority internal audit recommendations.
	Contract Management						
	Total						

Appendix 1. NHS Grampian Strategic level risks, themes and objectives

Strategic level risks, themes and objectives aims have been determined by NHS Grampian and are set out in the "The Vision and Values of NHS Grampian" and the Strategic Risk Register. These have been considered when preparing the internal audit plan.

Strategic Risk Register

The linkage of NHS Grampians Strategic Risk Register and the Internal Audit Plan for 2016/17 are set out in the table below:

Corporate Level Risk	*Cross reference to Internal Audit Plan for 2016/17*
Partnership working with local authorities, third sector, independent contractors, and community (586)	• Governance Statement • Homecare Prescribing Services • Patient Management in Mental Health Acute Services • Family Health Service Contractors
Involvement and engagement (610)	• Governance Statement
Staff Governance Standards Compliance (752)	• Governance Statement • Staff Continuity and Planning
Delivery strategies to meet the future health needs of the population (851)	• Governance Statement • Theatre Utilisation
Patient safety (853)	• Governance Statement • Staff Continuity and Planning • Theatre Utilisation • Homecare Prescribing Services • Patient Management in Mental Health Acute Services • Family Health Service Contractors
Infrastructure (855)	• Governance Statement • Property Transaction Monitoring • Cyber Security • Project Management of Non-Capital Change Projects
Sustaining access to professional clinical staff in Grampian (859)	• Governance Statement • Staff Continuity and Planning
Sustainable Workforce (1134)	• Governance Statement • Staff Continuity and Planning
Evidence and Intelligence Informed Strategy (1262)	• Governance Statement • Key Financial Controls • Property Transaction Monitoring • Data Quality in Management Information • Digital Strategy • Family Health Service Contractors • Project Management of Non-Capital Change Projects

Health & Safety (1448)	• Governance Statement
Integration of Health and Social Care (1784)	• Governance Statement • Health and Social Care Integration – Resource Allocation and Staff Governance

Strategic Themes and Objectives

The linkage of the NHS Grampian Strategic Themes and Objectives and the Internal Audit Plan for 2016/17 are set out in the table below:

Strategic Aim	*Cross reference to Internal Audit Plan for 2016/17*
(1) Improving Health & Reducing Inequalities • Reduce inequalities in health outcomes and access to & use of healthcare • Sustain & improve the population's health • Work in partnership to support healthier & fairer communities	• Home Prescribing Services • Patient Management in Mental Health Acute Services • Family Health Service Contractors • Health and Social Care Integration – Resource Allocation and Staff Governance
(2) Delivering High Quality Care in the Right Place • Provide safer, effective, sustainable services built around people • Exploit the opportunities arising from integrated working • Modernise health care services to improve outcomes	• Key Financial Controls • Property Transaction Monitoring • Staff Continuity and Planning • Data Quality in Management Information • Theatre Utilisation • Home Care Prescribing Services • Patient Management in Mental Health Acute Services • Family Health Service Contractors • Project Management of Non-Capital Change Projects • Digital Strategy
(3) Involving our Patients, Public, Staff & Partners • Ensure public and patients are fully informed in a way relevant to their needs • Ensure all plans, programmes and services demonstrate active and meaningful involvement • Embed a culture of genuine partnership in all NHSG services	• Theatre Utilisation • Homecare Prescribing Services • Patient Management in Mental Health Acute Services • Health and Social Care Integration – Resource Allocation and Staff Governance
(4) Developing and Empowering our Staff • Alignment of staff across partnerships to deliver outcomes • Creation of a supportive and empowering organisation climate and culture • Be the NHS employer of choice	• Staff Continuity and Planning • Patient Management in Mental Health Acute Services • Health and Social Care Integration – Resource Allocation and Staff Governance

Appendix 2. Detailed methodology

Step 1 - Understand corporate objectives and risks

In developing our understanding of your corporate objectives and risks, we have:

- Reviewed your strategic level risks, themes and objectives;
- Drawn on our knowledge of the NHS ; and
- Met with a number senior management and non-executive members.

Step 2 - Define the Audit Universe

In order that the internal audit plan reflects your management and operating structure we have identified the audit universe for NHS Grampian made up of a number of auditable units. Auditable units include functions, processes, systems, products or locations. Any processes or systems which cover multiple locations are separated into their own distinct cross cutting auditable unit.

Step 3 - Assess the inherent risk

The internal audit plan should focus on the most risky areas of the business. As a result each auditable unit is allocated an inherent risk rating i.e. how risky the auditable unit is to the overall organisation and how likely the risks are to arise. The criteria used to rate impact and likelihood are recorded in Appendix 2.

The inherent risk assessment is determined by:

- Mapping the corporate risks to the auditable units;
- Our knowledge of your business and the NHS; and
- Discussions with management.

Impact Rating	Likelihood Rating					
	6	**5**	**4**	**3**	**2**	**1**
6	6	6	5	5	4	4
5	6	5	5	4	4	3
4	5	5	4	4	3	3
3	5	4	4	3	3	2
2	4	4	3	3	2	2
1	4	3	3	2	2	1

Step 4 - Assess the strength of the control environment

In order to effectively allocate internal audit resources we also need to understand the strength of the control environment within each auditable unit. This is assessed based on:

- Our knowledge of your internal control environment;
- Information obtained from other assurance providers; and
- The outcomes of previous internal audits.

Step 5 - Calculate the audit requirement rating

The inherent risk and the control environment indicator are used to calculate the audit requirement rating. The formula ensures that our audit work is focused on areas with high reliance on controls or a high residual risk.

Inherent Risk Rating	Control design indicator					
	1	2	3	4	5	6
6	6	5	5	4	4	3
5	5	4	4	3	3	n/a
4	4	3	3	2	n/a	n/a
3	3	2	2	n/a	n/a	n/a
2	2	1	n/a	n/a	n/a	n/a
1	1	n/a	n/a	n/a	n/a	n/a

Step 6 - Determine the audit plan

Your risk appetite determines the frequency of internal audit work at each level of audit requirement. Auditable units may be reviewed annually, every two years or every three years.

In some cases it may be possible to isolate the sub-process (es) within an auditable unit which are driving the audit requirement. For example, an auditable unit has been given an audit requirement rating of 5 because of inherent risks with one particular sub-process, but the rest of the sub-processes are lower risk. In these cases it may be appropriate for the less risky sub-processes to have a lower audit requirement rating be subject to reduced frequency of audit work. These sub-processes driving the audit requirement areas are highlighted in the plan as key sub-process audits.

Step 7 - Other considerations

In addition to the audit work defined through the risk assessment process described above, we may be requested to undertake a number of other internal audit reviews such as regulatory driven audits, value enhancement or consulting reviews. These have been identified separately in the annual plan.

Appendix 3. Risk assessment criteria

Determination of Inherent Risk

We determine inherent risk as a function of the estimated **impact** and **likelihood** for each auditable unit within the audit universe as set out in the tables below.

Impact rating	Assessment rationale
6	Critical impact on operational performance; or Critical monetary or financial statement impact; or Critical breach in laws and regulations that could result in material fines or consequences; or Critical impact on the reputation or brand of the organisation which could threaten its future viability.
5	Significant impact on operational performance; or Significant monetary or financial statement impact; or Significant breach in laws and regulations resulting in large fines and consequences; or Significant impact on the reputation or brand of the organisation.
4	Major impact on operational performance; or Major monetary or financial statement impact; or Major breach in laws and regulations resulting in significant fines and consequences; or Major impact on the reputation or brand of the organisation.
3	Moderate impact on the organisation's operational performance; or Moderate monetary or financial statement impact; or Moderate breach in laws and regulations with moderate consequences; or Moderate impact on the reputation of the organisation.
2	Minor impact on the organisation's operational performance; or Minor monetary or financial statement impact; or Minor breach in laws and regulations with limited consequences; or Minor impact on the reputation of the organisation.
1	Insignificant impact on the organisation's operational performance; or Insignificant monetary or financial statement impact; or Insignificant breach in laws and regulations with little consequence; or Insignificant impact on the reputation of the organisation.

Likelihood rating	Assessment rationale
6	Has occurred or probable in the near future
5	Possible in the next 12 months
4	Possible in the next 1-2 years
3	Possible in the medium term (2-5 years)
2	Possible in the long term (5-10 years)
1	Unlikely in the foreseeable future