

## SERVIÇO DE AUDITORIA INTERNA

**CRITÉRIOS DE REFERÊNCIA:** 1.28; 2.7; 3.16 a 3.19; 35.14; 35.16

**ÂMBITO:** Aplicável ao Serviço de Auditoria Interna do Hospital de Magalhães Lemos, EPE

## ÍNDICE

OBJECTIVO .....	2
RESPONSABILIDADE .....	2
DESCRIÇÃO .....	2
1. Conteúdo e finalidades do serviço de auditoria interna .....	2
2. Enquadramento legal e normativo .....	2
3. Nexo hierárquico e funcional .....	2
4. Funções .....	3
5. Remessa de planos anuais de auditoria e de relatórios anuais à ACSS/DGTF/IGAS/IGF .....	3
6. Confidencialidade .....	3
7. Auditor interno: modo de nomeação e período de exercício de funções .....	4
8. Âmbito de acesso à informação .....	4
9. Reserva de competência .....	5
9.1. Contratação de serviços externos .....	5
10. Articulação do serviço de auditoria interna com o fiscal único do HML, EPE .....	5
11. Articulação com o núcleo de auditoria da qualidade .....	5
12. Disposições normativas complementares .....	5
DOCUMENTOS RELACIONADOS .....	6
ANEXOS .....	6
<i>Anexo I - Decreto-Lei n.º 233/2005, de 29-12, (c/a nova redação introduzida pelo Decreto-Lei n.º 244/2012, de 9-11)</i>	
<i>Anexo II - International Standards for the Professional Practice of Internal Auditing</i>	
<i>Anexo III - Organograma do Serviço de Auditoria Interna</i>	

---

## SERVIÇO DE AUDITORIA INTERNA

---

**CRITÉRIOS DE REFERÊNCIA:** 1.28; 2.7; 3.16 a 3.19; 35.14; 35.16

---

**ÂMBITO:** Aplicável ao Serviço de Auditoria Interna do Hospital de Magalhães Lemos, EPE

---

### OBJETIVO

Dar conhecimento das finalidades, nexos orgânico-funcional, estrutura e funcionamento do Serviço de Auditoria Interna do Hospital de Magalhães Lemos, EPE (HML, EPE).

### RESPONSABILIDADE

É da responsabilidade do Conselho de Administração a homologação e do Serviço de Auditoria Interna a implementação do presente normativo.

### DESCRIÇÃO

#### 1. Conteúdo e finalidades do serviço de auditoria interna

O Serviço de Auditoria Interna, suportado no modelo de gestão do risco e no sistema de controlo interno institucionalmente implementados, nos termos do art.º 17.º-A Decreto-Lei n.º 233/2005, de 29 de dezembro (com a nova redação introduzida pelo Decreto-Lei n.º 244/2012, de 9 de novembro) desenvolve uma atividade independente, de avaliação objetiva e de consultadoria, destinada a acrescentar valor e melhorar as operações do HML, EPE. Assiste a instituição na consecução dos seus objectivos, através de uma abordagem sistemática e disciplinada na avaliação e melhoria da eficácia dos processos de gestão do risco, controlo e governação, nos domínios contabilístico, financeiro, operacional, informático e de recursos humanos.

#### 2. Enquadramento legal e normativo

O Serviço de Auditoria Interna enquadra-se no âmbito do estabelecido no n.º 3 do art.º 9.º do Capítulo II e no art.º 17.º do Anexo II do Decreto-Lei n.º 233/2005, de 29 de dezembro (com a nova redação introduzida pelo Decreto-Lei n.º 244/2012, de 9 de novembro) – cfr. transcrição dos preceitos referidos no *Anexo I* ao presente regulamento.

O desenvolvimento da atividade de auditoria interna subordina-se também aos *International Standards for the Professional Practice of Internal Auditing*, tal como definidos pelo *The Institute of Internal Auditors (IIA)* – reproduzidos no *Anexo II* ao presente normativo.

#### 3. Nexos hierárquico e funcional

O Serviço de Auditoria Interna depende, em termos orgânicos, do Presidente do Conselho de Administração.

---

## SERVIÇO DE AUDITORIA INTERNA

---

**CRITÉRIOS DE REFERÊNCIA:** 1.28; 2.7; 3.16 a 3.19; 35.14; 35.16

---

**ÂMBITO:** Aplicável ao Serviço de Auditoria Interna do Hospital de Magalhães Lemos, EPE

---

No âmbito da sua atividade, o Serviço de Auditoria Interna colabora com a Administração Central dos Serviços de Saúde, I.P. (ACSS) e a Inspeção Geral das Atividades em Saúde (IGAS).

### 4. Funções

Ao Serviço de Auditoria Interna compete em especial:

- a) Fornecer ao Conselho de Administração análises e recomendações sobre as atividades revistas para melhoria do funcionamento dos serviços;
- b) Receber as comunicações de irregularidades sobre a organização e funcionamento do HML, EPE apresentadas pelos demais órgãos estatutários, trabalhadores, colaboradores, utentes e cidadãos em geral;
- c) Elaborar o plano anual de auditoria interna;
- d) Elaborar anualmente um relatório sobre a atividade desenvolvida, em que se refiram os controlos efetuados, as anomalias detetadas e as medidas corretivas a adotar.

Adicionalmente, o Serviço de Auditoria Interna submete ao critério de apreciação/deliberação do Conselho de Administração:

- Propostas visando a melhoria da eficiência e eficácia da instituição na realização dos objetivos definidos (incluindo, designadamente, a eventual subcontratação de auditores externos, quando as matérias a auditar tornem necessário o contributo de valências profissionais específicas);
- Plano de formação do Serviço de Auditoria Interna;
- Resolução de eventuais diferendos com os auditados.

### 5. Remessa de planos anuais de auditoria e de relatórios anuais à ACSS/DGTF/IGAS/IGF

O plano anual de auditoria e o relatório anual de auditoria são aprovados e submetidos pelo Conselho de Administração à ACSS, à Direção-Geral do Tesouro e Finanças (DGTF), à IGAS e à Inspeção-Geral de Finanças (IGF), respetivamente, até 15 de dezembro e 15 de março de cada ano.

### 6. Confidencialidade

O Serviço de Auditoria Interna está obrigado ao dever de confidencialidade em matéria de toda a informação a que tem acesso. Tal implica a não utilização da informação de modo contrário à lei ou em detrimento dos objectivos legítimos e éticos do HML, EPE.

## SERVIÇO DE AUDITORIA INTERNA

**CRITÉRIOS DE REFERÊNCIA:** 1.28; 2.7; 3.16 a 3.19; 35.14; 35.16

**ÂMBITO:** Aplicável ao Serviço de Auditoria Interna do Hospital de Magalhães Lemos, EPE

### 7. Auditor interno: modo de nomeação e período de exercício de funções

Nos termos do n.º 4 do art.º 17.º do Anexo II do Decreto-Lei n.º 233/2005, de 29 de dezembro (com a nova redação introduzida pelo Decreto-Lei n.º 244/2012, de 9 de novembro), e observado o condicionalismo consignado no n.º 6 do mesmo artigo e diploma, o auditor interno é designado pelo Conselho de Administração, de entre individualidades que reúnam os seguintes requisitos:

- a) Qualificação técnica, competências e experiência em auditoria;
- b) Inscrição no organismo nacional que regule a atividade de auditoria interna<sup>1</sup>.

O Conselho de Administração comunica à ACSS, à Direção-Geral do Tesouro e Finanças, à IGAS e à Inspeção-Geral de Finanças a identidade do auditor interno e as datas de início e termo de funções (cfr. n.º 8 do art.º 17.º do Anexo II do Decreto-Lei n.º 233/2005, de 29 de dezembro, com a nova redação introduzida pelo Decreto-Lei n.º 244/2012, de 9 de novembro).

Em conformidade com os números 3 e 7 do art.º 17.º do Anexo II do Decreto-Lei n.º 233/2005, de 29 de dezembro (com a nova redação introduzida pelo Decreto-Lei n.º 244/2012, de 9 de novembro), o auditor interno exerce as respetivas funções a tempo inteiro, de acordo com as normas internacionais para a prática profissional de auditoria interna e gestão de riscos, pelo período de cinco anos, renovável por iguais períodos, até ao limite máximo de três renovações consecutivas ou interpoladas.

### 8. Âmbito de acesso à informação

De acordo com o n.º 14 do art.º 17.º do Anexo II do Decreto-Lei n.º 233/2005, de 29 de dezembro (com a nova redação introduzida pelo Decreto-Lei n.º 244/2012, de 9 de novembro), e no sentido de obter informação adequada para o desenvolvimento das suas competências, o Serviço de Auditoria Interna tem acesso livre a registos, documentação, computadores, instalações e pessoal do hospital, com exceção dos registos clínicos individuais dos utentes.

<sup>1</sup> Instituto Português de Auditoria Interna (IPAI).

---

## SERVIÇO DE AUDITORIA INTERNA

---

**CRITÉRIOS DE REFERÊNCIA:** 1.28; 2.7; 3.16 a 3.19; 35.14; 35.16

---

**ÂMBITO:** Aplicável ao Serviço de Auditoria Interna do Hospital de Magalhães Lemos, EPE

---

### 9. Reserva de competência

Em conformidade com as normas internacionais para a prática profissional de auditoria interna, o Serviço de Auditoria Interna apenas desenvolve ações de *audit* para as quais disponha do necessário conhecimento, capacidades e experiência.

#### 9.1. Contratação de serviços externos

O Serviço de Auditoria Interna deverá propor superiormente o recurso à contratação de serviços externos quando:

- Não haja no Serviço de Auditoria Interna e neste não se justifique a existência de recursos especializados para efetuar auditorias a determinadas atividades;
- Os custos internos para efetuar auditorias a determinadas atividades forem superiores aos custos incorridos com a contratação de serviços externos;
- O trabalho a efetuar necessite de reforço temporário de recursos.

### 10. Articulação do serviço de auditoria interna com o fiscal único do HML, EPE

Com vista ao incremento do valor resultante do desempenho das atribuições sobre ele independentes, o Serviço de Auditoria Interna deverá assegurar uma adequada articulação funcional com o Fiscal Único do HML, EPE.

### 11. Articulação com o núcleo de auditoria da qualidade

O Serviço de Auditoria Interna articula-se funcionalmente com o Núcleo de Auditoria da Qualidade e com o Gabinete de Gestão do Risco.

### 12. Disposições normativas complementares

Em tudo o não referido no presente regulamento, rege o disposto no Decreto-Lei n.º 233/2005, de 29 de dezembro, com a nova redação introduzida pelo Decreto-Lei n.º 244/2012, de 9 de novembro (*Anexo I*), bem como as normas internacionais para a prática profissional de auditoria interna (*Anexo II*).

---

**SERVIÇO DE AUDITORIA INTERNA**

---

**CRITÉRIOS DE REFERÊNCIA:** 1.28; 2.7; 3.16 a 3.19; 35.14; 35.16

---

**ÂMBITO:** Aplicável ao Serviço de Auditoria Interna do Hospital de Magalhães Lemos, EPE

---

**DOCUMENTOS RELACIONADOS**

- Decreto-Lei n.º 233/2005, de 29 de dezembro
- Decreto-Lei n.º 244/2012, de 9 de novembro
- *International Standards for the Professional Practice of Internal Auditing*
- Manuais de Procedimentos da Administração Central de Serviços de Saúde, I.P.
- *Standards for International Hospitals Accreditation Programme (CHKS):*
  - *Leadership and Corporate Management Module (1st edition - June 2012)*
  - *Risk and Safety Accreditation Programme (1st edition - November 2011)*
- Código das Sociedades Comerciais
- PRO.006.HML – Âmbito, Frequência e Metodologia Genérica de Realização de Auditorias
- PRO.009.HML – Estratégia de Gestão do Risco
- POL.001.GGR - Sistema de Notificação de Acontecimentos Adversos
- PRO.001.GGR – Programa de Avaliação dos Riscos nos Serviços/Unidades
- PRO.105.HML - Procedimento de Notificação e Gestão de Incidentes Sentinela
- REG.002.HML – Regulamento do Núcleo de Auditoria da Qualidade

**ANEXOS**

*Anexo I - Decreto-Lei n.º 233/2005, de 29-12, (c/a nova redação introduzida pelo Decreto-Lei n.º 244/2012, de 9-11)*

*Anexo II - International Standards for the Professional Practice of Internal Auditing*

*Anexo III - Organograma do Serviço de Auditoria Interna*

## REGULAMENTO

CÓDIGO: **REG.021.HML**  
EDIÇÃO Nº: **001**  
REVISÃO Nº: **001**  
DATA DE HOMOLOGAÇÃO: **17/01/2013**

Documento Aprovado (Assinatura Digital)

---

### SERVIÇO DE AUDITORIA INTERNA

---

**CRITÉRIOS DE REFERÊNCIA:** 1.28; 2.7; 3.16 a 3.19; 35.14; 35.16

---

**ÂMBITO:** Aplicável ao Serviço de Auditoria Interna do Hospital de Magalhães Lemos, EPE

---

## ANEXOS

## REGULAMENTO

CÓDIGO: **REG.021.HML**  
EDIÇÃO Nº: **001**  
REVISÃO Nº: **001**  
DATA DE HOMOLOGAÇÃO: **17/01/2013**

Documento Aprovado (Assinatura Digital)

---

### SERVIÇO DE AUDITORIA INTERNA

---

**CRITÉRIOS DE REFERÊNCIA:** 1.28; 2.7; 3.16 a 3.19; 35.14; 35.16

---

**ÂMBITO:** Aplicável ao Serviço de Auditoria Interna do Hospital de Magalhães Lemos, EPE

---

### ANEXO I

*Decreto-Lei n.º 233/2005, de 29-12*

*(c/a nova redação introduzida pelo Decreto-Lei n.º 244/2012, de 9-11)*

**CAPÍTULO II**  
**Regime jurídico**  
**Artigo 9.º**  
**Organização**

3- No hospital E. P. E. existe um serviço de auditoria interna, que é dirigido por um auditor, nos termos dos Estatutos anexos ao presente decreto-lei.<sup>1</sup>

**ANEXO II**  
**ESTATUTOS**  
**CAPÍTULO II**  
**Órgãos<sup>2</sup>**  
**Artigo 5.º**  
**Órgãos**

São órgãos do hospital E. P. E.:

- a) O conselho de administração;
- b) O fiscal único;
- c) O conselho consultivo.

**SECÇÃO III**  
**Serviço de auditoria interna<sup>3</sup>**  
**Artigo 17.º**  
**Serviço de auditoria interna**

1 — Ao serviço de auditoria interna compete a avaliação dos processos de controlo interno e de gestão de riscos, nos domínios contabilístico, financeiro, operacional, informático e de recursos humanos, contribuindo para o seu aperfeiçoamento contínuo.<sup>4</sup>

2 — Ao serviço de auditoria interna compete em especial:

- a) Fornecer ao conselho de administração análises e recomendações sobre as atividades revistas para melhoria do funcionamento dos serviços;
- b) Receber as comunicações de irregularidades sobre a organização e funcionamento do hospital E. P. E. apresentadas pelos demais órgãos estatutários, trabalhadores, colaboradores, utentes e cidadãos em geral;
- c) Elaborar o plano anual de auditoria interna;
- d) Elaborar anualmente um relatório sobre a atividade desenvolvida, em que se refiram os controlos efetuados, as anomalias detetadas e as medidas corretivas a adotar.<sup>5</sup>

3 — A direção do serviço de auditoria interna compete a um auditor interno, que exerce as respetivas funções pelo período de cinco anos, renovável por iguais períodos, até ao limite máximo de três renovações consecutivas ou interpoladas, e que é apoiado tecnicamente nas suas funções por um máximo de três técnicos auditores.<sup>6</sup>

4 — O auditor interno é recrutado pelo conselho de administração, de entre individualidades que reúnam os seguintes requisitos:

- a) Qualificação técnica, competências e experiência em auditoria;
- b) Inscrição no organismo nacional que regule a atividade de auditoria interna.<sup>7</sup>

---

<sup>1</sup> Aditado pelo DL 244/2012, de 9 de novembro.

<sup>2</sup> Epígrafe alterada pelo DL 244/2012, de 9 de novembro.

<sup>3</sup> Epígrafe alterada pelo DL 244/2012, de 9 de novembro.

<sup>4</sup> Nova redação do DL 244/2012, de 9 de novembro.

<sup>5</sup> Nova redação do DL 244/2012, de 9 de novembro.

<sup>6</sup> Nova redação do DL 244/2012, de 9 de novembro.

<sup>7</sup> Nova redação do DL 244/2012, de 9 de novembro.

5 — Os técnicos que integrem o serviço de auditoria interna devem possuir curso superior adequado ao exercício das suas funções.<sup>8</sup>

6 — Não pode ser recrutado como auditor interno ou técnico do serviço de auditoria interna quem tenha exercido funções de administração no próprio hospital E. P. E., nos últimos três anos, ou em relação ao qual se verifiquem outras incompatibilidades e impedimentos previstos na lei, sendo aplicável, com as necessárias adaptações, o disposto no artigo 414.º -A do Código das Sociedades Comerciais.<sup>9</sup>

7 — O auditor interno exerce as respetivas funções a tempo inteiro, de acordo com as normas internacionais para a prática profissional de auditoria interna e gestão de riscos.<sup>10</sup>

8 — O conselho de administração comunica à Administração Central do Sistema de Saúde, I. P. (ACSS, I. P.), à Direção-Geral do Tesouro e Finanças (DGTF), à Inspeção -Geral das Atividades em Saúde (IGAS) e à Inspeção-Geral de Finanças (IGF) a identidade do auditor interno e as datas de início e termo de funções.<sup>11</sup>

9 — A não renovação ou cessação antecipada de funções do auditor interno ocorre por deliberação fundamentada do conselho de administração, precedida de comunicação ao membro do Governo responsável pela área da saúde, ou de quem, para o efeito, detenha poderes delegados.<sup>12</sup>

10 — A retribuição mensal ilíquida do auditor interno, incluindo suplementos remuneratórios, não pode ser superior a 85 % do vencimento mensal ilíquido estabelecido para o vogal do conselho de administração.<sup>13</sup>

11 — No âmbito da sua atividade, o serviço de auditoria interna colabora com a ACSS, I. P., e a IGAS.<sup>14</sup>

12 — O plano anual de auditoria e o relatório anual de auditoria são aprovados e submetidos pelo conselho de administração às entidades referidas no n.º 8, respetivamente, até 15 de dezembro e 15 de março de cada ano.<sup>15</sup>

13 — O serviço de auditoria interna depende, em termos orgânicos, do presidente do conselho de administração.<sup>16</sup>

14 — No sentido de obter informação adequada para o desenvolvimento das suas competências, o serviço de auditoria interna tem acesso livre a registos, documentação, computadores, instalações e pessoal do hospital, com exceção dos registos clínicos individuais dos utentes.<sup>17</sup>

#### **Artigo 17.º -A<sup>18</sup>**

##### **Sistema de controlo interno e de comunicação de irregularidades**

1 — O hospital E. P. E. dispõe de um sistema de controlo interno e de comunicação de irregularidades, competindo ao conselho de administração assegurar a sua implementação e manutenção e ao auditor interno a responsabilidade pela sua avaliação.

2 — O sistema de controlo interno compreende o conjunto de estratégias, políticas, processos, regras e procedimentos estabelecidos no hospital E. P. E. com vista a garantir:

a) Um desempenho eficiente da atividade que assegure a utilização eficaz dos ativos e recursos, a continuidade, segurança e qualidade da prestação de cuidados de saúde, através de uma adequada gestão e controlo dos riscos da atividade, da prudente e correta avaliação dos ativos e responsabilidades, bem como da definição de mecanismos de prevenção e de proteção do serviço público contra atuações danosas;

b) A existência de informação financeira e de gestão que suporte as tomadas de decisão e os processos de controlo, tanto no nível interno como no externo;

---

<sup>8</sup> Nova redação do DL 244/2012, de 9 de novembro.

<sup>9</sup> Nova redação do DL 244/2012, de 9 de novembro.

<sup>10</sup> Nova redação do DL 244/2012, de 9 de novembro.

<sup>11</sup> Nova redação do DL 244/2012, de 9 de novembro.

<sup>12</sup> Aditado pelo do DL 244/2012, de 9 de novembro.

<sup>13</sup> Aditado pelo do DL 244/2012, de 9 de novembro.

<sup>14</sup> Aditado pelo do DL 244/2012, de 9 de novembro.

<sup>15</sup> Aditado pelo do DL 244/2012, de 9 de novembro.

<sup>16</sup> Aditado pelo do DL 244/2012, de 9 de novembro.

<sup>17</sup> Aditado pelo do DL 244/2012, de 9 de novembro.

<sup>18</sup> Aditado pelo do DL 244/2012, de 9 de novembro.

c) O respeito pelas disposições legais e regulamentares aplicáveis, bem como pelas normas profissionais e deontológicas aplicáveis, pelas regras internas e estatutárias, regras de conduta e de relacionamento, orientações tutelares e recomendações aplicáveis de entidades externas como o Tribunal de Contas.

3 — O sistema de controlo interno tem por base um adequado sistema de gestão de risco, um sistema de informação e de comunicação e um processo de monitorização que assegure a respetiva adequação e eficácia em todas as áreas de intervenção.

4 — Mediante proposta do serviço de auditoria interna, deve ser aprovado, pelo conselho de administração do hospital E. P. E., um regulamento que defina as regras e procedimentos de comunicação interna de irregularidades, através do qual possam ser descritos factos que indiciem:

a) Violação de princípios e disposições legais, regulamentares e deontológicas por parte dos membros dos órgãos estatutários, trabalhadores, fornecedores de bens e prestadores de serviços no exercício dos seus cargos profissionais;

b) Dano, abuso ou desvio relativo ao património do hospital E. P. E. ou dos utentes;

c) Prejuízo à imagem ou reputação do hospital E. P. E.

## REGULAMENTO

CÓDIGO: **REG.021.HML**  
EDIÇÃO Nº: **001**  
REVISÃO Nº: **001**  
DATA DE HOMOLOGAÇÃO: **17/01/2013**

Documento Aprovado (Assinatura Digital)

---

### SERVIÇO DE AUDITORIA INTERNA

---

**CRITÉRIOS DE REFERÊNCIA:** 1.28; 2.7; 3.16 a 3.19; 35.14; 35.16

---

**ÂMBITO:** Aplicável ao Serviço de Auditoria Interna do Hospital de Magalhães Lemos, EPE

---

### ANEXO II

*International Standards for the Professional Practice of Internal Auditing*

***INTERNATIONAL STANDARDS FOR THE PROFESSIONAL PRACTICE  
OF INTERNAL AUDITING (STANDARDS)***

Issued: October 2008  
Revised: October 2012

© 2012 The Institute of Internal Auditors

*i*

## Table of contents

<b>Attribute Standards .....</b>	<b>3</b>
<b>1000 – Purpose, Authority, and Responsibility .....</b>	<b>3</b>
1010 – Recognition of the Definition of Internal Auditing, the Code of Ethics, and the Standards in the Internal Audit Charter .....	3
<b>1100 – Independence and Objectivity .....</b>	<b>3</b>
1110 – Organizational Independence .....	4
1111 – Direct Interaction with the Board .....	4
1120 – Individual Objectivity .....	4
<b>1130 – Impairment to Independence or Objectivity .....</b>	<b>5</b>
<b>1200 – Proficiency and Due Professional Care .....</b>	<b>5</b>
1210 – Proficiency .....	5
1220 – Due Professional Care .....	6
1230 – Continuing Professional Development .....	7
<b>1300 – Quality Assurance and Improvement Program .....</b>	<b>7</b>
1310 – Requirements of the Quality Assurance and Improvement Program .....	7
1311 – Internal Assessments .....	7
1312 – External Assessments .....	7
1320 – Reporting on the Quality Assurance and Improvement Program .....	8
1321 – Use of “Conforms with the International Standards for the Professional Practice of Internal Auditing” .....	8
1322 – Disclosure of Nonconformance .....	8
<b>Performance Standards .....</b>	<b>9</b>
<b>2000 – Managing the Internal Audit Activity .....</b>	<b>9</b>
2010 – Planning .....	9
2020 – Communication and Approval .....	10
2030 – Resource Management .....	10
2040 – Policies and Procedures .....	10
2050 – Coordination .....	10
2060 – Reporting to Senior Management and the Board .....	10
2070 – External Service Provider and Organizational Responsibility for Internal Auditing .....	10
<b>2100 – Nature of Work .....</b>	<b>11</b>
2110 – Governance .....	11
2120 – Risk Management .....	11
2130 – Control .....	12
<b>2200 – Engagement Planning .....</b>	<b>13</b>
2201 – Planning Considerations .....	13
2210 – Engagement Objectives .....	13
2220 – Engagement Scope .....	14
2230 – Engagement Resource Allocation .....	14

## International Standards for the Professional Practice of Internal Auditing (*Standards*)

2240 – Engagement Work Program.....	14
<b>2300 – Performing the Engagement.....</b>	<b>14</b>
2310 – Identifying Information.....	14
2320 – Analysis and Evaluation.....	15
2330 – Documenting Information.....	15
2340 – Engagement Supervision.....	15
<b>2400 – Communicating Results.....</b>	<b>15</b>
2410 – Criteria for Communicating.....	15
2420 – Quality of Communications.....	16
2421 – Errors and Omissions.....	16
2430 – Use of “Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing”.....	16
2431 – Engagement Disclosure of Nonconformance.....	17
2440 – Disseminating Results.....	17
2450 – Overall Opinions.....	17
<b>2500 – Monitoring Progress.....</b>	<b>18</b>
<b>2600 – Communicating the Acceptance of Risks.....</b>	<b>18</b>

**INTERNATIONAL STANDARDS FOR THE PROFESSIONAL PRACTICE OF  
INTERNAL AUDITING (STANDARDS)**

***Introduction to the International Standards***

Internal auditing is conducted in diverse legal and cultural environments; within organizations that vary in purpose, size, complexity, and structure; and by persons within or outside the organization. While differences may affect the practice of internal auditing in each environment, conformance with The IIA's International Standards for the Professional Practice of Internal Auditing (Standards) is essential in meeting the responsibilities of internal auditors and the internal audit activity. If internal auditors or the internal audit activity is prohibited by law or regulation from conformance with certain parts of the Standards, conformance with all other parts of the Standards and appropriate disclosures are needed.

If the *Standards* are used in conjunction with standards issued by other authoritative bodies, internal audit communications may also cite the use of other standards, as appropriate. In such a case, if inconsistencies exist between the *Standards* and other standards, internal auditors and the internal audit activity must conform with the *Standards*, and may conform with the other standards if they are more restrictive.

The purpose of the *Standards* is to:

1. Delineate basic principles that represent the practice of internal auditing.
2. Provide a framework for performing and promoting a broad range of value-added internal auditing.
3. Establish the basis for the evaluation of internal audit performance.
4. Foster improved organizational processes and operations.

The *Standards* are principles-focused, mandatory requirements consisting of:

- Statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of performance, which are internationally applicable at organizational and individual levels.
- Interpretations, which clarify terms or concepts within the Statements.

The *Standards* employ terms that have been given specific meanings that are included in the Glossary. Specifically, the *Standards* use the word "must" to specify an unconditional requirement and the word "should" where conformance is expected unless, when applying professional judgment, circumstances justify deviation.

It is necessary to consider the Statements and their Interpretations as well as the specific meanings from the Glossary to understand and apply the *Standards* correctly.

The structure of the *Standards* is divided between Attribute and Performance Standards. Attribute Standards address the attributes of organizations and individuals performing internal auditing. The Performance Standards describe the nature of internal auditing and provide quality criteria against which the performance of these services can be measured. The Attribute and Performance Standards are also provided to apply to all internal audit services.

Implementation Standards are also provided to expand upon the Attribute and Performance standards, by providing the requirements applicable to assurance (A) or consulting (C) activities.

Assurance services involve the internal auditor's objective assessment of evidence to provide an independent opinion or conclusions regarding an entity, operation, function, process, system, or other subject matter. The nature and scope of the assurance engagement are determined by

## **International Standards for the Professional Practice of Internal Auditing (*Standards*)**

the internal auditor. There are generally three parties involved in assurance services: (1) the person or group directly involved with the entity, operation, function, process, system, or other subject matter — the process owner, (2) the person or group making the assessment — the internal auditor, and (3) the person or group using the assessment — the user.

Consulting services are advisory in nature, and are generally performed at the specific request of an engagement client. The nature and scope of the consulting engagement are subject to agreement with the engagement client. Consulting services generally involve two parties: (1) the person or group offering the advice — the internal auditor, and (2) the person or group seeking and receiving the advice — the engagement client. When performing consulting services the internal auditor should maintain objectivity and not assume management responsibility.

The Standards apply to individual internal auditors and internal audit activities. All internal auditors are accountable for conforming with the Standards related to individual objectivity, proficiency, and due professional care. In addition, internal auditors are accountable for conforming with the Standards, which are relevant to the performance of their job responsibilities. Chief audit executives are accountable for overall conformance with the Standards.

The review and development of the *Standards* is an ongoing process. The International Internal Audit Standards Board engages in extensive consultation and discussion prior to issuing the *Standards*. This includes worldwide solicitation for public comment through the exposure draft process. All exposure drafts are posted on The IIA's Web site as well as being distributed to all IIA institutes.

Suggestions and comments regarding the *Standards* can be sent to:

The Institute of Internal Auditors  
Standards and Guidance  
247 Maitland Avenue  
Altamonte Springs, FL 32701-4201, USA

E-mail: [guidance@theiia.org](mailto:guidance@theiia.org)

Web: [www.globaliia.org](http://www.globaliia.org)

\*\*\*

## **INTERNATIONAL STANDARDS FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING (STANDARDS)**

### **Attribute Standards**

#### **1000 – Purpose, Authority, and Responsibility**

The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the *Standards*. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

##### **Interpretation:**

*The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization, including the nature of the chief audit executive's functional reporting relationship with the board; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities. Final approval of the internal audit charter resides with the board.*

**1000.A1** – The nature of assurance services provided to the organization must be defined in the internal audit charter. If assurances are to be provided to parties outside the organization, the nature of these assurances must also be defined in the internal audit charter.

**1000.C1** – The nature of consulting services must be defined in the internal audit charter.

#### **1010 – Recognition of the Definition of Internal Auditing, the Code of Ethics, and the Standards in the Internal Audit Charter**

The mandatory nature of the Definition of Internal Auditing, the Code of Ethics, and the *Standards* must be recognized in the internal audit charter. The chief audit executive should discuss the Definition of Internal Auditing, the Code of Ethics, and the *Standards* with senior management and the board.

#### **1100 – Independence and Objectivity**

The internal audit activity must be independent, and internal auditors must be objective in performing their work.

##### **Interpretation:**

*Independence is the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board. This can be achieved through a dual-reporting relationship. Threats to independence must be managed at the individual auditor, engagement, functional, and organizational levels.*

## **International Standards for the Professional Practice of Internal Auditing (Standards)**

*Objectivity is an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others. Threats to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels.*

### **1110 – Organizational Independence**

The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

#### **Interpretation:**

*Organizational independence is effectively achieved when the chief audit executive reports functionally to the board. Examples of functional reporting to the board involve the board:*

- *Approving the internal audit charter;*
- *Approving the risk based internal audit plan;*
- *Approving the internal audit budget and resource plan;*
- *Receiving communications from the chief audit executive on the internal audit activity's performance relative to its plan and other matters;*
- *Approving decisions regarding the appointment and removal of the chief audit executive;*
- *Approving the remuneration of the chief audit executive; and*
- *Making appropriate inquiries of management and the chief audit executive to determine whether there are inappropriate scope or resource limitations.*

**1110.A1** – The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results.

### **1111 – Direct Interaction with the Board**

The chief audit executive must communicate and interact directly with the board.

### **1120 – Individual Objectivity**

Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

#### **Interpretation:**

*Conflict of interest is a situation in which an internal auditor, who is in a position of trust, has a competing professional or personal interest. Such competing interests can make it difficult to fulfill his or her duties impartially. A conflict of interest exists even if no unethical or improper act results. A conflict of interest can create an appearance of impropriety that can undermine confidence in the internal auditor, the internal audit activity, and the profession. A conflict of interest could impair an individual's ability to perform his or her duties and responsibilities objectively.*

## International Standards for the Professional Practice of Internal Auditing (*Standards*)

### 1130 – Impairment to Independence or Objectivity

If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

**Interpretation:**

*Impairment to organizational independence and individual objectivity may include, but is not limited to, personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations, such as funding.*

*The determination of appropriate parties to which the details of an impairment to independence or objectivity must be disclosed is dependent upon the expectations of the internal audit activity's and the chief audit executive's responsibilities to senior management and the board as described in the internal audit charter, as well as the nature of the impairment.*

**1130.A1** – Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous year.

**1130.A2** – Assurance engagements for functions over which the chief audit executive has responsibility must be overseen by a party outside the internal audit activity.

**1130.C1** – Internal auditors may provide consulting services relating to operations for which they had previous responsibilities.

**1130.C2** – If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the engagement client prior to accepting the engagement.

### 1200 – Proficiency and Due Professional Care

Engagements must be performed with proficiency and due professional care.

#### 1210 – Proficiency

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

**Interpretation:**

*Knowledge, skills, and other competencies is a collective term that refers to the professional proficiency required of internal auditors to effectively carry out their professional responsibilities. Internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certifications and qualifications, such as the Certified Internal Auditor designation and other designations offered by The Institute of Internal Auditors and other appropriate professional organizations.*

**1210.A1** – The chief audit executive must obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

## **International Standards for the Professional Practice of Internal Auditing (*Standards*)**

**1210.A2** – Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

**1210.A3** – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

**1210.C1** – The chief audit executive must decline the consulting engagement or obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

### **1220 – Due Professional Care**

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

**1220.A1** – Internal auditors must exercise due professional care by considering the:

- Extent of work needed to achieve the engagement's objectives;
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied;
- Adequacy and effectiveness of governance, risk management, and control processes;
- Probability of significant errors, fraud, or noncompliance; and
- Cost of assurance in relation to potential benefits.

**1220.A2** – In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques.

**1220.A3** – Internal auditors must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified.

**1220.C1** – Internal auditors must exercise due professional care during a consulting engagement by considering the:

- Needs and expectations of clients, including the nature, timing, and communication of engagement results;
- Relative complexity and extent of work needed to achieve the engagement's objectives; and
- Cost of the consulting engagement in relation to potential benefits.

## **International Standards for the Professional Practice of Internal Auditing (Standards)**

### **1230 – Continuing Professional Development**

Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

### **1300 – Quality Assurance and Improvement Program**

The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

#### **Interpretation:**

*A quality assurance and improvement program is designed to enable an evaluation of the internal audit activity's conformance with the Definition of Internal Auditing and the Standards and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement.*

### **1310 – Requirements of the Quality Assurance and Improvement Program**

The quality assurance and improvement program must include both internal and external assessments.

### **1311 – Internal Assessments**

Internal assessments must include:

- Ongoing monitoring of the performance of the internal audit activity; and
- Periodic self-assessments or assessments by other persons within the organization with sufficient knowledge of internal audit practices.

#### **Interpretation:**

*Ongoing monitoring is an integral part of the day-to-day supervision, review, and measurement of the internal audit activity. Ongoing monitoring is incorporated into the routine policies and practices used to manage the internal audit activity and uses processes, tools, and information considered necessary to evaluate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards.*

*Periodic assessments are conducted to evaluate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards.*

*Sufficient knowledge of internal audit practices requires at least an understanding of all elements of the International Professional Practices Framework.*

### **1312 - External Assessments**

External assessments must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organization. The chief audit executive must discuss with the board:

- The form and frequency of external assessment; and
- The qualifications and independence of the external assessor or assessment team, including any potential conflict of interest.

## **International Standards for the Professional Practice of Internal Auditing (Standards)**

### **Interpretation:**

*External assessments can be in the form of a full external assessment, or a self-assessment with independent external validation.*

*A qualified assessor or assessment team demonstrates competence in two areas: the professional practice of internal auditing and the external assessment process. Competence can be demonstrated through a mixture of experience and theoretical learning. Experience gained in organizations of similar size, complexity, sector or industry, and technical issues is more valuable than less relevant experience. In the case of an assessment team, not all members of the team need to have all the competencies; it is the team as a whole that is qualified. The chief audit executive uses professional judgment when assessing whether an assessor or assessment team demonstrates sufficient competence to be qualified.*

*An independent assessor or assessment team means not having either a real or an apparent conflict of interest and not being a part of, or under the control of, the organization to which the internal audit activity belongs.*

### **1320 – Reporting on the Quality Assurance and Improvement Program**

The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board.

#### **Interpretation:**

*The form, content, and frequency of communicating the results of the quality assurance and improvement program is established through discussions with senior management and the board and considers the responsibilities of the internal audit activity and chief audit executive as contained in the internal audit charter. To demonstrate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards, the results of external and periodic internal assessments are communicated upon completion of such assessments and the results of ongoing monitoring are communicated at least annually. The results include the assessor's or assessment team's evaluation with respect to the degree of conformance.*

### **1321 – Use of “Conforms with the International Standards for the Professional Practice of Internal Auditing”**

The chief audit executive may state that the internal audit activity conforms with the *International Standards for the Professional Practice of Internal Auditing* only if the results of the quality assurance and improvement program support this statement.

#### **Interpretation:**

*The internal audit activity conforms with the Standards when it achieves the outcomes described in the Definition of Internal Auditing, Code of Ethics, and Standards. The results of the quality assurance and improvement program include the results of both internal and external assessments. All internal audit activities will have the results of internal assessments. Internal audit activities in existence for at least five years will also have the results of external assessments.*

### **1322 – Disclosure of Nonconformance**

When nonconformance with the Definition of Internal Auditing, the Code of Ethics, or the *Standards* impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.

## Performance Standards

### 2000 – Managing the Internal Audit Activity

The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.

**Interpretation:**

*The internal audit activity is effectively managed when:*

- *The results of the internal audit activity's work achieve the purpose and responsibility included in the internal audit charter;*
- *The internal audit activity conforms with the Definition of Internal Auditing and the Standards; and*
- *The individuals who are part of the internal audit activity demonstrate conformance with the Code of Ethics and the Standards.*

*The internal audit activity adds value to the organization (and its stakeholders) when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management, and control processes.*

### 2010 – Planning

The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

**Interpretation:**

*The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consideration of input from senior management and the board. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.*

**2010.A1** – The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

**2010.A2** – The chief audit executive must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.

**2010.C1** – The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

## **International Standards for the Professional Practice of Internal Auditing (Standards)**

### **2020 – Communication and Approval**

The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.

### **2030 – Resource Management**

The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

#### **Interpretation:**

*Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the plan. Sufficient refers to the quantity of resources needed to accomplish the plan. Resources are effectively deployed when they are used in a way that optimizes the achievement of the approved plan.*

### **2040 – Policies and Procedures**

The chief audit executive must establish policies and procedures to guide the internal audit activity.

#### **Interpretation:**

*The form and content of policies and procedures are dependent upon the size and structure of the internal audit activity and the complexity of its work.*

### **2050 – Coordination**

The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

### **2060 – Reporting to Senior Management and the Board**

The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

#### **Interpretation:**

*The frequency and content of reporting are determined in discussion with senior management and the board and depend on the importance of the information to be communicated and the urgency of the related actions to be taken by senior management or the board.*

### **2070 – External Service Provider and Organizational Responsibility for Internal Auditing**

When an external service provider serves as the internal audit activity, the provider must make the organization aware that the organization has the responsibility for maintaining an effective internal audit activity.

## **International Standards for the Professional Practice of Internal Auditing (Standards)**

### **Interpretation**

*This responsibility is demonstrated through the quality assurance and improvement program which assesses conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards.*

### **2100 – Nature of Work**

The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

### **2110 – Governance**

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization;
- Ensuring effective organizational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organization; and
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

**2110.A1** – The internal audit activity must evaluate the design, implementation, and effectiveness of the organization’s ethics-related objectives, programs, and activities.

**2110.A2** – The internal audit activity must assess whether the information technology governance of the organization supports the organization’s strategies and objectives.

### **2120 – Risk Management**

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

#### ***Interpretation:***

*Determining whether risk management processes are effective is a judgment resulting from the internal auditor’s assessment that:*

- *Organizational objectives support and align with the organization’s mission;*
- *Significant risks are identified and assessed;*
- *Appropriate risk responses are selected that align risks with the organization’s risk appetite; and*
- *Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.*

*The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization’s risk management processes and their effectiveness.*

## **International Standards for the Professional Practice of Internal Auditing (Standards)**

*Risk management processes are monitored through ongoing management activities, separate evaluations, or both.*

**2120.A1** – The internal audit activity must evaluate risk exposures relating to the organization’s governance, operations, and information systems regarding the:

- Achievement of the organization’s strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts.

**2120.A2** – The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

**2120.C1** – During consulting engagements, internal auditors must address risk consistent with the engagement’s objectives and be alert to the existence of other significant risks.

**2120.C2** – Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization’s risk management processes.

**2120.C3** – When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

### **2130 – Control**

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

**2130.A1** – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization’s governance, operations, and information systems regarding the:

- Achievement of the organization’s strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts.

**2130.C1** – Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization’s control processes.

## **International Standards for the Professional Practice of Internal Auditing (*Standards*)**

### **2200 – Engagement Planning**

Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations.

### **2201 – Planning Considerations**

In planning the engagement, internal auditors must consider:

- The objectives of the activity being reviewed and the means by which the activity controls its performance;
- The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level;
- The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model; and
- The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

**2201.A1** – When planning an engagement for parties outside the organization, internal auditors must establish a written understanding with them about objectives, scope, respective responsibilities, and other expectations, including restrictions on distribution of the results of the engagement and access to engagement records.

**2201.C1** – Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding must be documented.

### **2210 – Engagement Objectives**

Objectives must be established for each engagement.

**2210.A1** – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

**2210.A2** – Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

**2210.A3** – Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management and/or the board to develop appropriate evaluation criteria.

**2210.C1** – Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed upon with the client.

**2210.C2** – Consulting engagement objectives must be consistent with the organization's values, strategies, and objectives.

## **International Standards for the Professional Practice of Internal Auditing (*Standards*)**

### **2220 – Engagement Scope**

The established scope must be sufficient to achieve the objectives of the engagement.

**2220.A1** – The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

**2220.A2** – If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.

**2220.C1** – In performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the client to determine whether to continue with the engagement.

**2220.C2** – During consulting engagements, internal auditors must address controls consistent with the engagement's objectives and be alert to significant control issues.

### **2230 – Engagement Resource Allocation**

Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

### **2240 – Engagement Work Program**

Internal auditors must develop and document work programs that achieve the engagement objectives.

**2240.A1** – Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.

**2240.C1** – Work programs for consulting engagements may vary in form and content depending upon the nature of the engagement.

### **2300 – Performing the Engagement**

Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

### **2310 – Identifying Information**

Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

## **International Standards for the Professional Practice of Internal Auditing (Standards)**

### **Interpretation:**

*Sufficient information is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor. Reliable information is the best attainable information through the use of appropriate engagement techniques. Relevant information supports engagement observations and recommendations and is consistent with the objectives for the engagement. Useful information helps the organization meet its goals.*

### **2320 – Analysis and Evaluation**

Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

### **2330 – Documenting Information**

Internal auditors must document relevant information to support the conclusions and engagement results.

**2330.A1** – The chief audit executive must control access to engagement records. The chief audit executive must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.

**2330.A2** – The chief audit executive must develop retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

**2330.C1** – The chief audit executive must develop policies governing the custody and retention of consulting engagement records, as well as their release to internal and external parties. These policies must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

### **2340 – Engagement Supervision**

Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

### **Interpretation:**

*The extent of supervision required will depend on the proficiency and experience of internal auditors and the complexity of the engagement. The chief audit executive has overall responsibility for supervising the engagement, whether performed by or for the internal audit activity, but may designate appropriately experienced members of the internal audit activity to perform the review. Appropriate evidence of supervision is documented and retained.*

### **2400 – Communicating Results**

Internal auditors must communicate the results of engagements.

### **2410 – Criteria for Communicating**

Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

## **International Standards for the Professional Practice of Internal Auditing (Standards)**

**2410.A1** - Final communication of engagement results must, where appropriate, contain the internal auditors' opinion and/or conclusions. When issued, an opinion or conclusion must take account of the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.

### **Interpretation:**

*Opinions at the engagement level may be ratings, conclusions, or other descriptions of the results. Such an engagement may be in relation to controls around a specific process, risk, or business unit. The formulation of such opinions requires consideration of the engagement results and their significance.*

**2410.A2** – Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.

**2410.A3** – When releasing engagement results to parties outside the organization, the communication must include limitations on distribution and use of the results.

**2410.C1** – Communication of the progress and results of consulting engagements will vary in form and content depending upon the nature of the engagement and the needs of the client.

## **2420 – Quality of Communications**

Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

### **Interpretation:**

*Accurate communications are free from errors and distortions and are faithful to the underlying facts. Objective communications are fair, impartial, and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances. Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information. Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness. Constructive communications are helpful to the engagement client and the organization and lead to improvements where needed. Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions. Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.*

## **2421 – Errors and Omissions**

If a final communication contains a significant error or omission, the chief audit executive must communicate corrected information to all parties who received the original communication.

## **2430 – Use of “Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing”**

Internal auditors may report that their engagements are “conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*”, only if the results of the quality assurance and improvement program support the statement.

## International Standards for the Professional Practice of Internal Auditing (*Standards*)

### 2431 – Engagement Disclosure of Nonconformance

When nonconformance with the Definition of Internal Auditing, the Code of Ethics or the *Standards* impacts a specific engagement, communication of the results must disclose the:

- Principle or rule of conduct of the Code of Ethics or *Standard(s)* with which full conformance was not achieved;
- Reason(s) for nonconformance; and
- Impact of nonconformance on the engagement and the communicated engagement results.

### 2440 – Disseminating Results

The chief audit executive must communicate results to the appropriate parties.

#### Interpretation:

*The chief audit executive is responsible for reviewing and approving the final engagement communication before issuance and for deciding to whom and how it will be disseminated. When the chief audit executive delegates these duties, he or she retains overall responsibility.*

**2440.A1** – The chief audit executive is responsible for communicating the final results to parties who can ensure that the results are given due consideration.

**2440.A2** – If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization the chief audit executive must:

- Assess the potential risk to the organization;
- Consult with senior management and/or legal counsel as appropriate; and
- Control dissemination by restricting the use of the results.

**2440.C1** – The chief audit executive is responsible for communicating the final results of consulting engagements to clients.

**2440.C2** – During consulting engagements, governance, risk management, and control issues may be identified. Whenever these issues are significant to the organization, they must be communicated to senior management and the board.

### 2450 – Overall Opinions

When an overall opinion is issued, it must take into account the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.

#### Interpretation:

*The communication will identify:*

- *The scope, including the time period to which the opinion pertains;*
- *Scope limitations;*
- *Consideration of all related projects including the reliance on other assurance providers;*

## **International Standards for the Professional Practice of Internal Auditing (Standards)**

- *The risk or control framework or other criteria used as a basis for the overall opinion; and*
- *The overall opinion, judgment, or conclusion reached.*

*The reasons for an unfavorable overall opinion must be stated.*

### **2500 – Monitoring Progress**

The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

**2500.A1** – The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

**2500.C1** – The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.

### **2600 – Communicating the Acceptance of Risks**

When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

#### **Interpretation:**

*The identification of risk accepted by management may be observed through an assurance or consulting engagement, monitoring progress on actions taken by management as a result of prior engagements, or other means. It is not the responsibility of the chief audit executive to resolve the risk.*

## **International Standards for the Professional Practice of Internal Auditing (*Standards*)**

### **Glossary**

#### **Add Value**

The internal audit activity adds value to the organization (and its stakeholders) when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management, and control processes.

#### **Adequate Control**

Present if management has planned and organized (designed) in a manner that provides reasonable assurance that the organization's risks have been managed effectively and that the organization's goals and objectives will be achieved efficiently and economically.

#### **Assurance Services**

An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

#### **Board**

The highest level of governing body charged with the responsibility to direct and/or oversee the activities and management of the organization. Typically, this includes an independent group of directors (e.g., a board of directors, a supervisory board, or a board of governors or trustees). If such a group does not exist, the "board" may refer to the head of the organization. "Board" may refer to an audit committee to which the governing body has delegated certain functions.

#### **Charter**

The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities.

#### **Chief Audit Executive**

Chief audit executive describes a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the Definition of Internal Auditing, the Code of Ethics, and the *Standards*. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title of the chief audit executive may vary across organizations.

#### **Code of Ethics**

The Code of Ethics of The Institute of Internal Auditors (IIA) are Principles relevant to the profession and practice of internal auditing, and Rules of Conduct that describe behavior expected of internal auditors. The Code of Ethics applies to both parties and entities that provide internal audit services. The purpose of the Code of Ethics is to promote an ethical culture in the global profession of internal auditing.

#### **Compliance**

Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

## **International Standards for the Professional Practice of Internal Auditing (*Standards*)**

### **Conflict of Interest**

Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.

### **Consulting Services**

Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

### **Control**

Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

### **Control Environment**

The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- Integrity and ethical values.
- Management's philosophy and operating style.
- Organizational structure.
- Assignment of authority and responsibility.
- Human resource policies and practices.
- Competence of personnel.

### **Control Processes**

The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.

### **Engagement**

A specific internal audit assignment, task, or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.

### **Engagement Objectives**

Broad statements developed by internal auditors that define intended engagement accomplishments.

## **International Standards for the Professional Practice of Internal Auditing (*Standards*)**

### **Engagement Opinion**

The rating, conclusion, and/or other description of results of an individual internal audit engagement, relating to those aspects within the objectives and scope of the engagement.

### **Engagement Work Program**

A document that lists the procedures to be followed during an engagement, designed to achieve the engagement plan.

### **External Service Provider**

A person or firm outside of the organization that has special knowledge, skill, and experience in a particular discipline.

### **Fraud**

Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

### **Governance**

The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

### **Impairment**

Impairment to organizational independence and individual objectivity may include personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations (funding).

### **Independence**

The freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner.

### **Information Technology Controls**

Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.

### **Information Technology Governance**

Consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology supports the organization's strategies and objectives.

### **Internal Audit Activity**

A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.

## **International Standards for the Professional Practice of Internal Auditing (*Standards*)**

### **International Professional Practices Framework**

The conceptual framework that organizes the authoritative guidance promulgated by The IIA. Authoritative Guidance is comprised of two categories – (1) mandatory and (2) strongly recommended.

#### **Must**

The *Standards* use the word “must” to specify an unconditional requirement.

#### **Objectivity**

An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others.

#### **Overall Opinion**

The rating, conclusion, and/or other description of results provided by the chief audit executive addressing, at a broad level, governance, risk management, and/or control processes of the organization. An overall opinion is the professional judgment of the chief audit executive based on the results of a number of individual engagements and other activities for a specific time interval.

#### **Risk**

The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

#### **Risk Appetite**

The level of risk that an organization is willing to accept.

#### **Risk Management**

A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization’s objectives.

#### **Should**

The *Standards* use the word “should” where conformance is expected unless, when applying professional judgment, circumstances justify deviation.

#### **Significance**

The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors, such as magnitude, nature, effect, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives.

#### **Standard**

A professional pronouncement promulgated by the Internal Audit Standards Board that delineates the requirements for performing a broad range of internal audit activities, and for evaluating internal audit performance.

## **International Standards for the Professional Practice of Internal Auditing (*Standards*)**

### **Technology-based Audit Techniques**

Any automated audit tool, such as generalized audit software, test data generators, computerized audit programs, specialized audit utilities, and computer-assisted audit techniques (CAATs).

\*\*\*

## REGULAMENTO

CÓDIGO: **REG.021.HML**  
EDIÇÃO Nº: **001**  
REVISÃO Nº: **001**  
DATA DE HOMOLOGAÇÃO: **17/01/2013**

Documento Aprovado (Assinatura Digital)

---

### SERVIÇO DE AUDITORIA INTERNA

---

**CRITÉRIOS DE REFERÊNCIA:** 1.28; 2.7; 3.16 a 3.19; 35.14; 35.16

---

**ÂMBITO:** Aplicável ao Serviço de Auditoria Interna do Hospital de Magalhães Lemos, EPE

---

### ANEXO III

#### *Organograma do Serviço de Auditoria Interna*

**SERVIÇO DE AUDITORIA INTERNA**

**CRITÉRIOS DE REFERÊNCIA:** 1.28; 2.7; 3.16 a 3.19; 35.14; 35.16

**ÂMBITO:** Aplicável ao Serviço de Auditoria Interna do Hospital de Magalhães Lemos, EPE

**Organograma do Serviço de Auditoria Interna**

