PSI
The Pharmacy Regulator
An Rialtóir Cógaisíochta

Pharmaceutical Society of Ireland

Risk Management

Framework

Contents

1. Scope

The Pharmaceutical Society of Ireland (PSI), in common with all organisations must deal with a range of uncertainties. These uncertainties may be positive, (opportunity), or negative, (threats).

The PSI addresses these uncertainties by means of enterprise risk management which seeks to ensures our strategic objectives, core processes and functions, as well as our stakeholders' expectations, are delivered effectively, and in a timely manner.

2. Purpose

This document is intended for use by PSI staff, and officeholders, including members of the PSI's Advisory Committees, and its Council, and describes the risk management framework in operation at the PSI, outlining its three key components;

- Risk Architecture;
- Risk Strategy; and
- Risk Protocols and Processes.

The Framework underpins risk management at the PSI, ensuring it is;

- Proportionate to the level of risk faced by the PSI;
- Aligned to the PSI's activities;
- Comprehensive and systematic;
- Embedded across the organisation; and
- Responsive to emerging and changing risks.

Through its implementation, the PSI endeavours to deliver desired outcomes, by reducing the volatility or variability of those outcomes, and ensuring effective risk management informs the way it leads, directs, manages, and operates, generating efficiencies, informed decision making, stakeholder assurance, and compliance with its governance and legal requirements.

To achieve this the PSI embraces a culture of transparency, and welcomes critical challenge, as the most effective means of evaluating uncertainties, their implications, and potential impact on the organisation.

3. Risk Architecture

The PSI's risk architecture sets out the lines of communication for reporting risk management issues, and seeks to provide a clear statement of the risk management responsibilities within the organisation, ensuring that roles are clearly defined and understood.

3.1 Risk Management Roles and Responsibilities in the PSI

Council

The role of Council is to:

- Approve the Risk Management Framework and monitor its effectiveness with assistance, and advice from the Audit and Risk Committee.
- Set the PSI's risk appetite, profile, and culture.
- Report on the effectiveness of the PSI's risk management systems to its stake holders, including confirmation in the Annual Report that it has carried out an assessment of the PSI's principal risks, to include a description of those risks, and the measures in place to mitigate them.
- Ensuring risk management is discussed at each Council meeting and the PSI Corporate Risk Register is reviewed as a standing item on the agenda.

Registrar

The Registrar reports to Council and is responsible for:

- Determining the PSI's strategic approach to risk.
- Integrating the process for managing risk into the PSI's governance, strategy, planning, management, reporting processes, policies, values and culture.
- Ensuring the PSI risk management procedures, processes and protocols are embedded and being complied with across the organisation.
- Making necessary resources available for managing risk across the organisation.
- Ensuring an effective system of internal control is in place.

Executive Leadership Team (ELT)

The PSI's Executive Leadership Team is responsible for:

Developing specialist contingency and recovery plans for the PSI's five Business Areas which are:

1. Corporate Services,
2. Practitioner Assurance,
3. Governance and Programme Delivery,
4. Strategic Policy and Communication,
5. Community Pharmacy Assurance.

- Supporting investigations of risk incidents and near misses.
- Preparing Business Area risk reports when required, for the Audit and Risk Committee.
- Maintaining, and updating on a monthly basis a risk register for their Business Area.
- Collectively reviewing and advising on the update of the PSI Corporate Risk Register on a monthly basis.
- Owning risk located in their Business Area, or if appropriate, delegating risk ownership to heads of teams, or a member of their team.

Chief Risk Officer (CRO)

The CRO reports to Council and the Audit and Risk Committee and is responsible for:

- Maintaining and, in consultation with the ELT and the Registrar, updating the PSI's Corporate Risk Register.
- Embedding a risk-aware culture across the PSI.
- Designing risk management processes in the PSI.
- Compiling risk management data, and reporting to Council, and the Audit and Risk Committee on the findings.
- Co-ordinating the identification, prioritisation, and management of the PSI's risks.
- Ensuring that risk management training is provided to PSI staff, Committee, and Council members.

Risk Owners

The role of a PSI risk owner is to manage risk controls for each risk, once they have been agreed, and monitor and report on their efficacy to their head of Business Area, or if the risk owner is a head of a Business Area , to the Registrar.

Staff

PSI staff report to their line manager and/or head of Business Area. The role of each member of PSI staff is to act as a risk champion by supporting the PSI in applying its risk management processes and procedures, as well as increasing risk awareness across the organisation, in order to improve outcomes for all PSI stakeholders through;

- Implementing PSI risk management processes.
- Pro-actively identifying risk issues and bringing these to the attention of colleagues.
- Monitoring the effectiveness of controls, identifying gaps in controls and reporting inefficient, unnecessary, or unworkable risk controls to their manager.
- Reporting loss events and/or near-miss incidents when they become aware of them.
- Co-operating on risk incident or near miss investigations.
- Ensuring that visitors and contractors comply with risk management procedures.

Internal Audit

The PSI's Internal Auditors;

- Provide independent assurance to the PSI, and its stakeholders, including members of the public, patients, the pharmacy profession, and the Government, regarding the efficacy of the PSI's risk management framework and system of internal controls.
- Validate the procedures in place to manage risk at the PSI.
- Ascertain whether or not the PSI is in compliance with the governance, and legal requirements to which it is subject.

- Report to the Audit and Risk Committee on its findings and recommendations for action, incorporating the response it has received from the PSI's Executive Leadership Team to the internal audit report.

External Audit

The PSI's External Auditors;

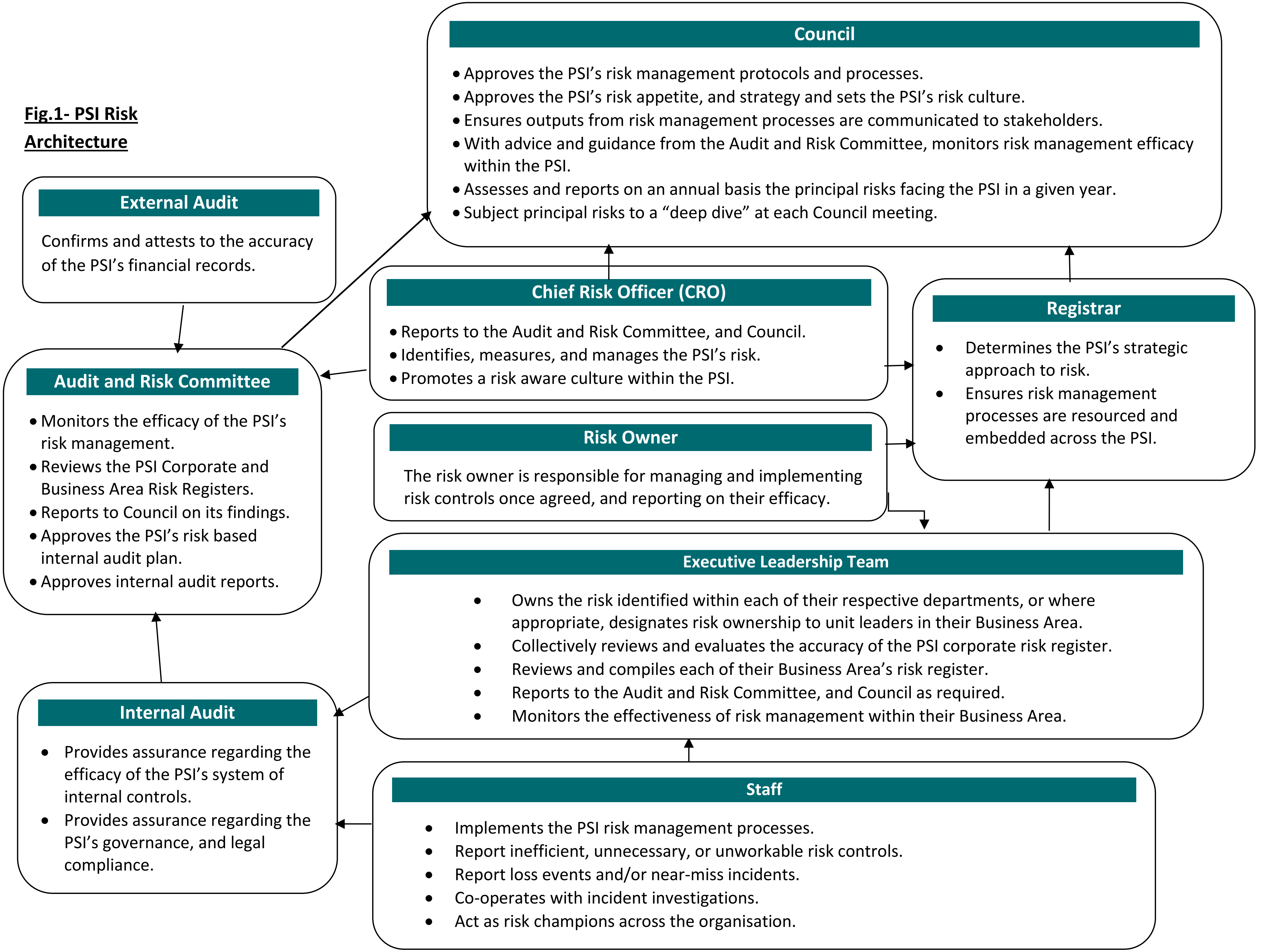
- Verify and attest as to the accuracy of the PSI's financial statements and accounts.

Audit and Risk Committee

The Audit and Risk Committee evaluates governance within the PSI, seeking assurance with regard to its levels of compliance, as well as the efficacy of its risk management. It acts independently in the interest of the PSI's stakeholders, and reports to the PSI Council on its findings. The Audit and Risk Committee is responsible for;

- Reviewing risk reports and monitoring the effectiveness of risk management and reporting to Council on a quarterly basis;
- Reviewing Business Area, and the Corporate Risk Register;
- Monitoring, and if it deems necessary, critically challenging the efficacy of PSI risk management processes and system of internal controls;
- The approval of the risk based annual Internal Audit Plan;
- The approval of internal audit reports received from the Internal Auditor;
- The approval of the External Auditor's Report; and
- The approval of the annual statement of internal control.

Fig.1- PSI Risk Architecture



Council

- Approves the PSI’s risk management protocols and processes.
- Approves the PSI’s risk appetite, and strategy and sets the PSI’s risk culture.
- Ensures outputs from risk management processes are communicated to stakeholders.
- With advice and guidance from the Audit and Risk Committee, monitors risk management efficacy within the PSI.
- Assesses and reports on an annual basis the principal risks facing the PSI in a given year.
- Subject principal risks to a “deep dive” at each Council meeting.

External Audit

Confirms and attests to the accuracy of the PSI’s financial records.

Chief Risk Officer (CRO)

- Reports to the Audit and Risk Committee, and Council.
- Identifies, measures, and manages the PSI’s risk.
- Promotes a risk aware culture within the PSI.

Registrar

- Determines the PSI’s strategic approach to risk.
- Ensures risk management processes are resourced and embedded across the PSI.

Audit and Risk Committee

- Monitors the efficacy of the PSI’s risk management.
- Reviews the PSI Corporate and Business Area Risk Registers.
- Reports to Council on its findings.
- Approves the PSI’s risk based internal audit plan.
- Approves internal audit reports.

Risk Owner

The risk owner is responsible for managing and implementing risk controls once agreed, and reporting on their efficacy.

Executive Leadership Team

- Owns the risk identified within each of their respective departments, or where appropriate, designates risk ownership to unit leaders in their Business Area.
- Collectively reviews and evaluates the accuracy of the PSI corporate risk register.
- Reviews and compiles each of their Business Area’s risk register.
- Reports to the Audit and Risk Committee, and Council as required.
- Monitors the effectiveness of risk management within their Business Area.

Internal Audit

- Provides assurance regarding the efficacy of the PSI’s system of internal controls.
- Provides assurance regarding the PSI’s governance, and legal compliance.

Staff

- Implements the PSI risk management processes.
- Report inefficient, unnecessary, or unworkable risk controls.
- Report loss events and/or near-miss incidents.
- Co-operates with incident investigations.
- Act as risk champions across the organisation.

4. Risk Management Strategy

The PSI's risk management strategy sets out the way in which its risk management processes and protocols are aligned to the organisation's strategic objectives and regulatory remit, and includes its current risk appetite and risk statement.

4.1 Risk Appetite

The PSI's risk appetite refers to the amount, and type of risk, which the organisation is willing to accept, or retain, in pursuit of its business objectives. Depending on the category, and magnitude of the risk in question, the PSI's appetite for the risk may elicit one of the following responses:

Averse - Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is paramount. Activities undertaken will only be those considered to carry virtually no risk.

Cautious - Willing to accept / tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where the Registrar following consultation with Council has identified scope to achieve significant reward and/or realise an opportunity. Activities undertaken may carry a high degree of risk magnitude but it is deemed to be controllable.

Open - Undertakes activities by seeking to achieve a balance between a high likelihood of successful delivery and a high degree of reward and value for money. Activities themselves may potentially carry, or contribute to, a high degree of residual risk.

4.2 PSI Risk Appetite Statement

This statement sets out how the PSI balances risk, and opportunity, in pursuit of its business objectives.

The PSI Council has considered the principal risks to which the PSI is currently exposed, and their potential impact on the PSI's ability to meet its strategic objectives and regulatory remit. The Council has considered the risk appetite of the organisation in the context of stakeholder expectation, (foremost amongst them being the expectation that it will protect patients and public), the PSI's risk culture, the sector it regulates, as well as the PSI's three current strategic pillars:

1. Advancing the role of pharmacy and pharmacists in an integrated healthcare system.

2. Evolving a more effective regulatory model for community pharmacies.

3. Building the PSI's capability and performance as a regulator.

The PSI is not averse to taking risk where innovation and change may result in demonstrable improvements to its performance as a regulator.

The PSI is averse to any risk which has the potential to erode trust in its capacity to function effectively as a regulator, including any risk which threatens the PSI's own compliance with the law, or the discharge of its remit to protect public and patient safety.

The PSI is cautious with regard to sustaining its operational capacity and systems, which support the delivery of its remit, and which must be adequate to this task at all times.

In this context, the PSI;

- Recognises that it may treat, tolerate, transfer, and if necessary, terminate risk, in order to successfully deliver its strategic objectives and its regulatory remit.
- Acknowledges it must be prepared to avail of opportunities should they arise, where the potential reward justifies the acceptance of a specified level of risk.
- Will review its risk appetite annually in order to address changing circumstances in its operating environment, and in its organisational capacity.

4.3 PSI Risk Statement

The PSI views an integrated and holistic approach to risk management as the most effective means of responding to risk.

To this end;

- The PSI's management of risk is conducted systematically, iteratively, and collaboratively, drawing on expert knowledge, and stakeholders' views, and will always seek to be evidence based.
- The PSI's communication relating to risk is continuous.
- As the PSI is a public body which acts under the aegis of the Department of Health, the PSI acknowledges that a mutual understanding with the Department, of the risks faced by the PSI, is of critical importance, including timely escalation if necessary.

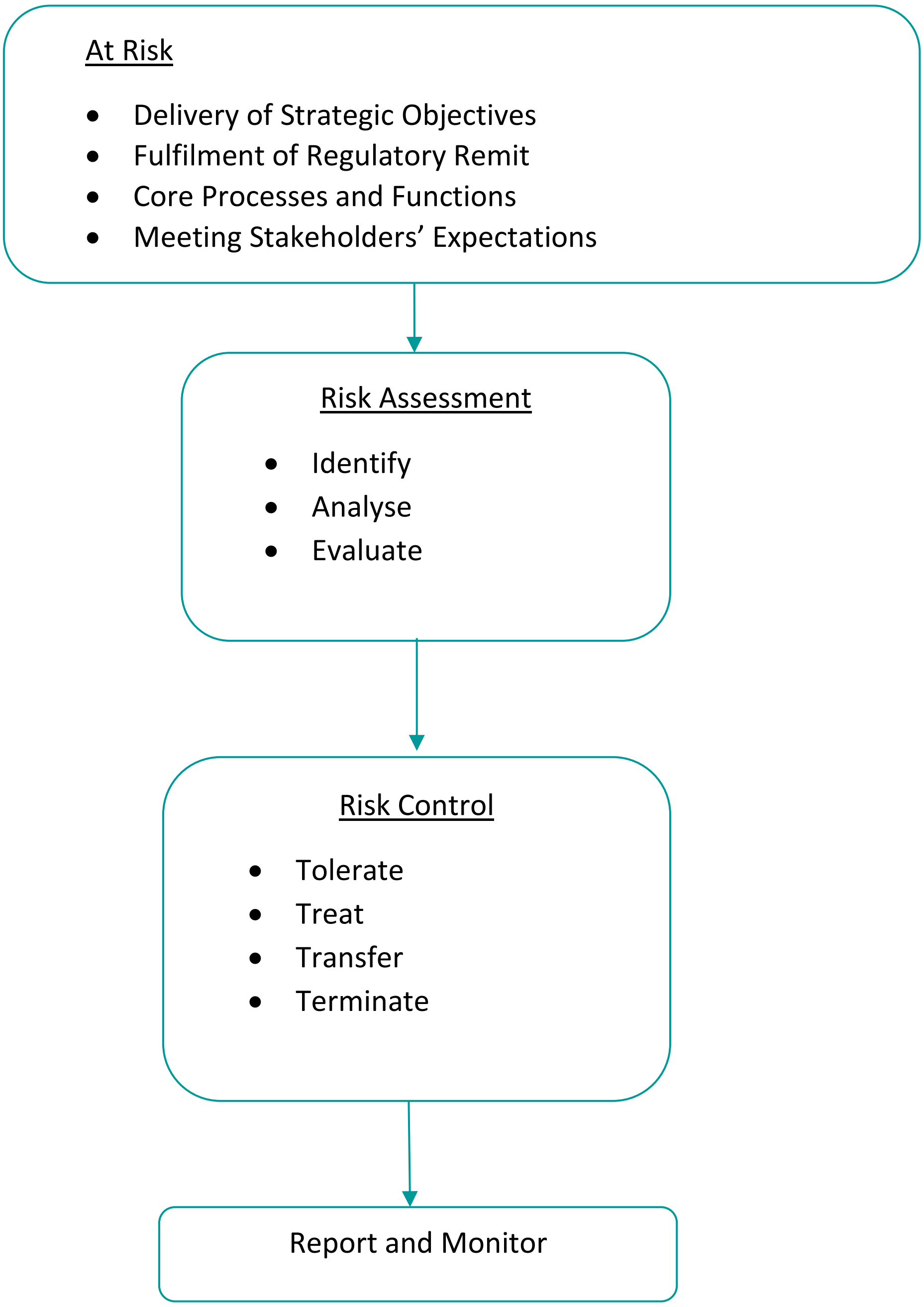
The PSI has three governance meetings a year with the Department and a copy of the Corporate Risk Register is provided to the Department before each meeting and discussed as part of the agenda.

- In its Regulatory Risk Statement, the PSI defines regulatory risk, as ‘the risk of harm arising to the public from the actions, or inactions of those we regulate’. The management of regulatory risk by the PSI is focused on identifying, analysing, evaluating, and responding to risk which may cause harm to the public arising from the actions or inactions of pharmacists, or pharmacies.
- The measures the PSI has in place to protect the health and safety of its employees, and office holders, and the management of risks to which they may be exposed in the course of their work for the PSI, is set out in its Safety Statement .

5. Risk Management Processes, Procedures, and Protocols

The PSI's risk management processes, procedures, and protocols refer to the organisation-wide practices undertaken by the PSI, which seek to ensure its risk strategy is implemented, and risk consequence is mitigated.

Fig.2 - PSI Risk Management Process


At Risk
Delivery of Strategic Objectives
Fulfilment of Regulatory Remit
Core Processes and Functions
Meeting Stakeholders' Expectations
Risk Assessment
Identify
Analyse
Evaluate
Risk Control
Tolerate
Treat
Transfer
Terminate
Report and Monitor

5.1 Risk Assessment

Risk assessment may be broken down into the following components:

- Identifying risk;
- Analysing the likelihood of the risk materialising; and
- Evaluating the consequences should the risk materialise.

5.2 Risk Identification

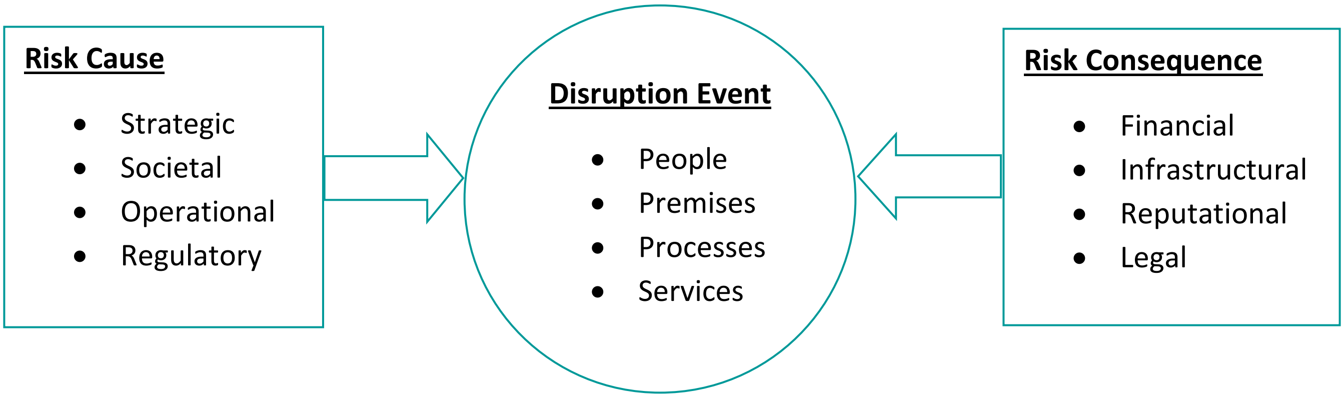
The PSI adheres to four guiding principles to assist it in identifying risk:

1. We seek to identify emerging risks as soon as possible, as well as detecting change to existing risks which are already known to us.
2. We are vigilant, and alert to the possibility of risks which are not yet known to us.
3. We seek to identify risk, irrespective of whether or not its source is under the PSI's control.
4. We ensure risk identification, both positive (opportunity), and negative (threat), takes place at every level of the organisation.

The process of identifying new risk is a standing item for discussion, once a month, at ELT, Business Area, and Team meetings, when their respective risk registers are updated.

As part of the risk register update, the cause or source of each risk, the nature of its impact or what is referred to as the disruption event, which is any occurrence that could inhibit, enhance, or cause doubt about the efficacy or efficiency of one or more of the PSI's core processes, and the consequence for the PSI and/or its stakeholders, will be considered, and together will form the risk narrative.

Fig.3 - Risk Narrative: Cause, Event, Consequence



Risk Cause

- Strategic
- Societal
- Operational
- Regulatory

Disruption Event

- People
- Premises
- Processes
- Services

Risk Consequence

- Financial
- Infrastructural
- Reputational
- Legal

The strategic objectives, core process, or stakeholder expectation, on which the risk could impact should it materialise, is clearly stated as part of the risk identification narrative and may fall under any of the following categories of risk;

Opportunity risk – risk which if taken may result in a gain for the PSI, but which could result in a loss.
Strategy risk – Risk arising from the pursuit by the PSI of strategic objectives, which are poorly defined, and/or based on flawed or inaccurate data.

Governance risk – Risk arising from non-compliance by the PSI with Government directives, and/or Codes ofPpractice. Risk arising from unclear accountabilities, and/or ineffective oversight of decision-making within the PSI.

Operations risk – Risk arising from inadequate, poorly designed, or ineffective internal processes, resulting in fraud, error, or impaired customer service including quality and/or quantity of service.

Legal risk – Risk arising from a legal event occurring resulting in a liability for the PSI, or a failure by the PSI to meet the statutory and legal requirements to which it is subject, exposing it to the possibility of legal sanction.

Financial risk – Risk arising from not managing finances in accordance with requirements and financial constraints, resulting in poor returns from investments, failure to manage assets/liabilities, or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.

Commercial risk – Risk arising from weaknesses in the management of commercial contracts, supply chains, and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and /or failure to meet the PSI's business requirements.

People risk – Risk arising from ineffective leadership, suboptimal organisational culture, inappropriate behaviours, insufficient workforce capacity and/or capability, industrial action and/or non-compliance with relevant employment legislation/HR policies, resulting in negative impact on the PSI's performance.

Technology risk – Risk arising from technology not delivering the expected services due to inadequate or deficient system development, or performance, or inadequate resilience.

Security risk – Risk arising from a failure to prevent unauthorised access to PSI House, unauthorised use, damage, or theft of PSI property, including PSI virtual assets, such as data the PSI holds in its IT systems.

Project risk – (Also known as control risk) Risk arising should a project not deliver the intended benefit(s) on time, within budget, and/or to the required specification.

Hazard risk – Risk arising from threats to the safety and/or health of PSI employees or office holders in the course of their work for the PSI, at any location, or to any person who may have a legitimate reason to be present in PSI House.
Regulatory risk – Risk to the safety of patients and/or the public arising from the actions or inactions of pharmacists, or pharmacies.

5.3 Risk Analysis

Risk Analysis measures the likelihood of a risk materialising.

In the PSI, it is measured using the following scale:

Risk Analysis Score	**Risk Analysis Definition**
1-2	**Unlikely:** Can reasonably be expected not to occur, or has only occurred once in the past 10 years in the PSI, or similar organisations.
3	**Possible:** Has occurred in the PSI more than 3 times in the past 10 years, or occurs regularly in similar organisations, or is considered to have a reasonable likelihood of occurring in the next five years.
4	**Likely** Occurred more than 7 times over 10 years in the PSI or in similar organisations, or circumstances are such that it is likely to happen in the next five years.
5	**Almost Certain:** Has occurred in the PSI or other organisations 9 or 10 times in the past 10 years, or circumstances have arisen that will almost certainly cause it to happen.

5.4 Risk Evaluation

Risk evaluation is the point at which the PSI decides whether or not to respond to a risk, once the likelihood of a risk materialising has been measured. An evaluation is made of the potential consequences for the PSI, should the risk materialise, and is measured as follows:

Risk Evaluation Score	Risk Evaluation Definition
1	**<u>Negligible:</u>** The PSI accepts this risk as the impact would be insignificant. The status of the risk should be reviewed occasionally.
2	**<u>Minor:</u>** The consequences of this risk materialising would have a minor impact on the PSI. No immediate action is required, but an action plan should be actively considered. The status of the risk should be monitored periodically.
3	**<u>Moderate:</u>** The consequences of this risk materialising would have a moderate impact on day-to-day operational delivery in the PSI. Some immediate action might be required to address risk impact, and the development of an action plan considered.
4	**<u>Major :</u>** The consequences of this risk materialising would be severe but not disastrous for the PSI. Some immediate action is required to mitigate the risk, as well as the development of a comprehensive action plan.
5	**<u>Substantial:</u>** The consequence of this risk materialising would have a disastrous impact on the PSI's reputation and business continuity. Comprehensive action is required immediately to mitigate the risk.

When evaluating a risk, the score for the most credible worst consequence, should be assigned to the risk. On the balance of understating or overstating risk consequence, of the two, understating risk consequence leads to the poorer risk management outcome.

Each risk is then given a risk rating by multiplying the risk analysis (likelihood) score, by the risk evaluation (consequence) score.

The result is recorded as the risk rating on the relevant risk register, either Business Area or Corporate, and the risk magnitude based on the score, is given a red, amber, green (RAG) classification.

Fig.4 - Risk Matrix

Risk Evaluation
(Consequence)

Low → High

Risk Analysis (Likelihood)

Low

High

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Fig.5 - Risk Magnitude

High	Risk score of 12 to 25
Medium	Risk score of 5 to 11
Low	Risk score of 1 to 4

5.5 Risk Controls

Once risks have been identified, analysed, and evaluated, appropriate risk controls are considered;

> **Tolerate:** The exposure to risk may be deemed tolerable without any further action being taken by if the risk has a low likelihood of materialising, and if it does so, would be likely to have negligible or minor consequences for the PSI.

Treat: Risk treatment should be considered when a risk may have moderate or significant consequences for the PSI should it materialise, but have a low likelihood of materialising.

Transfer: Risk transfer to another body, if the option is available, would also be appropriate when a risk may have moderate or significant consequences for the PSI should it materialise, but have a low likelihood of materialising.

Terminate: Risk termination, or elimination, where it is possible to cease an activity which gives rise to a risk, should be considered when the risk is deemed to be substantial and have a high likelihood of materialising.

5.6 Opportunity Risk

Opportunity risks are speculative in nature, and unlike other risk, are intentionally taken by the PSI in order to obtain a positive outcome for the organisation, where the benefits obtained from taking the risk are assessed to be greater than the benefits that would have resulted in not taking the risk. In other words, the level of risk associated with not taking the opportunity, should be greater than the level of risk associated with taking the opportunity.

A positive outcome is not however a certainty , and a risk versus reward analysis should always be undertaken prior to a decision to pursue an opportunity risk. In the case of opportunity risk, the following mitigation options will be considered by the PSI.

Exploit the opportunity risk if it falls within the PSI's risk appetite.

Ignore the opportunity risk if it exceeds the PSI's risk appetite.

Share the opportunity risk with a partner organisation to reduce the PSI's level of risk exposure, in return for the risk benefit materialising, or a shared but reduced risk benefit materialising.

5.7 Risk Registers

The purpose of the PSI's risk registers, both Corporate, and Business Area, is to provide an agreed record of significant risks which have been identified, and the actions proposed to mitigate each risk, including identifying the risk owner, and recording the risk controls which have been put in place. Any risk which may impact on more than one Business Area or are of such magnitude should be considered for listing on the PSI's Corporate Risk Register.

The PSI risk registers contains the following information on each registered risk:

- **Risk Category:** The PSI's current risk categories are**;** financial, opportunity, operational, legal, regulatory, governance, hazard, project, people, strategy, technology, security, commercial.
- **Risk Description:** This is a brief statement of what the risk is, and will include; the date it was first logged on the risk register, reference to its context, or the source from which it has emerged; indication of the evidence base being used to assess it e.g., 'research indicates that', 'intelligence received suggests that' etc.
- **Risk Analysis:** The likelihood of the risk materialising**.**
- **Risk Evaluation:** The consequence of the risk if it materialises**.**
- **Risk Rating:** This is the risk analysis score (likelihood) multiplied by the risk evaluation score (consequence). It provides a numerical indication of the significance of the risk, on a scale of 1 to 25, and positions it on the risk matrix. The risk rating also positions the risk within the hierarchy of total cumulative risk to which the PSI is exposed at any given point. This is refered to as the PSI's risk exposure.
- **Risk Magnitude**: (Also known as absolute, inherent, or gross risk.) Refers to the risk in its unmitigated state, that is to say, the scale of the risk for the PSI if nothing is done.
- **Risk Controls:** are the actions undertaken or measures put in place, (including the dates by which they are to be implemented), to reduce the likelihood of the risk materialising, or the impact of the risk's consequence, should the risk materialise.
- **Residual Risk:** (Also known as net, or current risk). Refers to the risk to the PSI once risk controls have been agreed, and put in place. The same risk which appears as red in the risk magnitude column, would ordinarily, but not always, be expected to appear as amber or green in the residual risk column, as the likelihood of the risk materialising, or its impact should it materialise, will have reduced if the risk controls are effective. A judgement is made regarding the appropriate RAG classification for the residual risk, however, that judgment is not fixed. It is critically important the residual risk classification is kept under constant review, and updated at each Business Area or ELT meeting at which risk registers are being reviewed. The RAG classification may have to be changed depending on the reports received from the risk owner, regarding changes, if any, to the nature risk, or the efficacy of the risk controls in place to mitigate the risk.
- **Risk Owner:** Is the relevant job title of the risk owner who is the person responsible for managing and implement the risk controls once they have been agreed, and monitoring and reporting on their efficacy to the ELT or Head of Business Area.

Fig.6 - PSI Risk Registers - Example

Ref no.	Risk Category	Risk Description	Risk Analysis (Likelihood)	Risk Evaluation (Consequence)	Risk Rating	Risk Magnitude	Risk Controls	Residual Risk	Risk Owner
1.	Security	28.01.21 Reports received from the PSI’s IT security partners indicate there has been an increase in the last month of the number of attempts by hostile actors to penetrate the PSI’s IT systems.	There is no indication that current levels of attack will reduce, and there is a possibility that they may increase. The risk is therefore deemed likely to continue to pose a threat. **The score is set at 4.**	The potential impact of a successful cyber-attack on the PSI IT systems are deemed to be significant for the PSI's business continuity. **The score is set at 4.**	16	🟥	The risk will be treated as follows: 1. Training module for all staff on phishing emails to be completed by 04.04.21 2. Security essentials alignment report re: Microsoft 365 conducted by PSI’s ICT support and hosting vendor, with actions to be completed by 03.03.21 3. Breach attack simulation to be completed by PSI IT systems security vendor by end of Q3.	🟧	ICT Manager

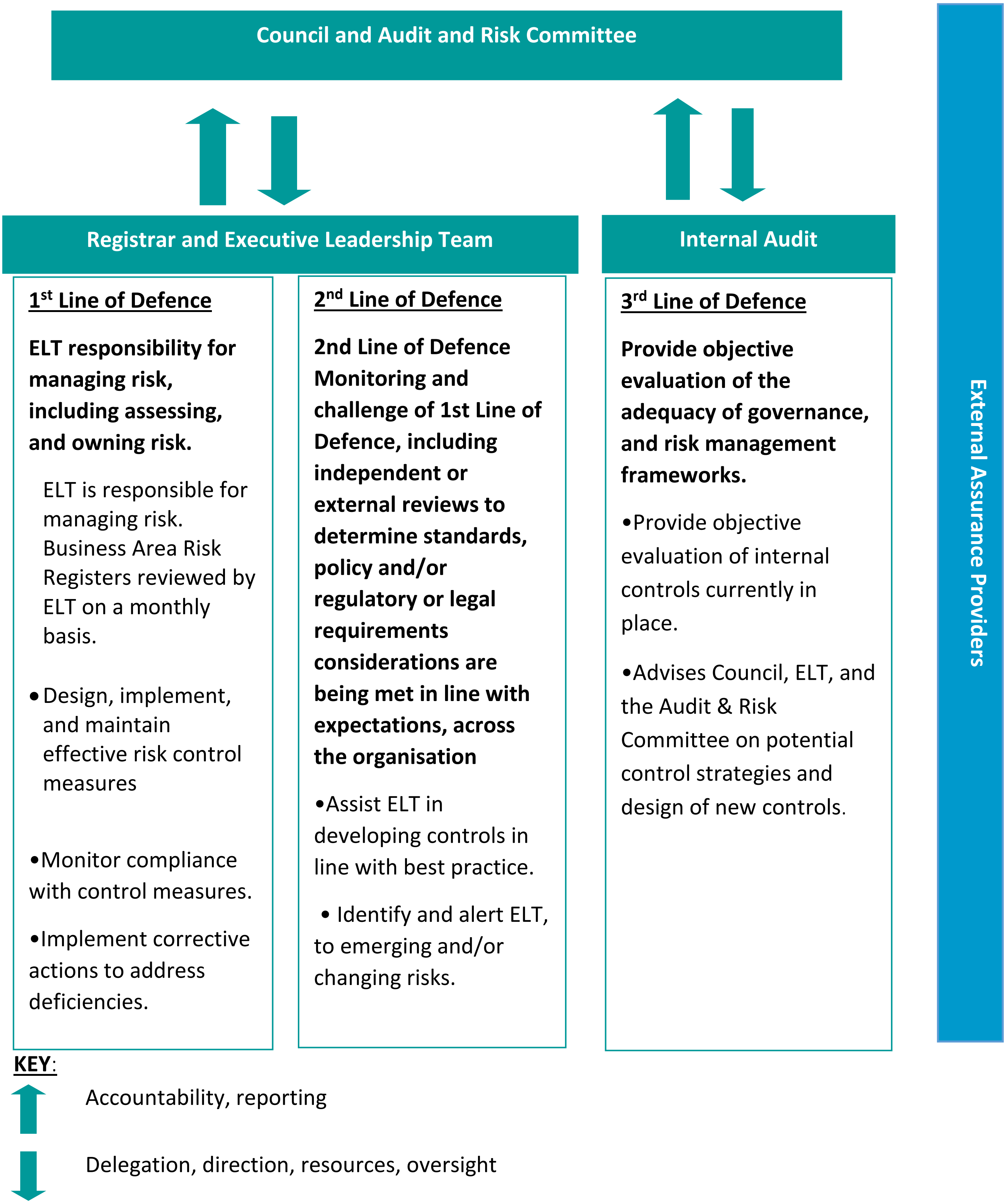
5.8 Risk Monitoring and Reporting

The PSI views integrated, timely and accurate risk monitoring, and reporting as an essential requirement of effective risk management, which will enhance the PSI's quality of decision-making, and support it in delivering its strategic objectives, and meeting its regulatory remit.

Monitoring takes place before, during, and after implementation of risk controls. Ongoing and continuous monitoring supports understanding of any change to a risk which has been identified, and the extent to which risk controls are operating as intended. The assumptions underpinning the efficacy of risk controls already in place, are subject to continuous review and interrogation.

To this end, the PSI will communicate risk management activities and outcomes across the organisation. The "three lines of defence" model to which the PSI adheres, seeks to ensure that the Registrar and the Council receive unbiased information about the PSI's significant risks, how the Executive Leadership Team is responding to those risks, and the contribution risk management is making to achieving objectives, and to creating and protecting value.

Fig.7 - The Three Lines of Defence



Council and Audit and Risk Committee

Registrar and Executive Leadership Team

Internal Audit

External Assurance Providers

1st Line of Defence

ELT responsibility for managing risk, including assessing, and owning risk.

ELT is responsible for managing risk. Business Area Risk Registers reviewed by ELT on a monthly basis.

- Design, implement, and maintain effective risk control measures

•Monitor compliance with control measures.

•Implement corrective actions to address deficiencies.

2nd Line of Defence

2nd Line of Defence Monitoring and challenge of 1st Line of Defence, including independent or external reviews to determine standards, policy and/or regulatory or legal requirements considerations are being met in line with expectations, across the organisation

•Assist ELT in developing controls in line with best practice.

- Identify and alert ELT, to emerging and/or changing risks.

3rd Line of Defence

Provide objective evaluation of the adequacy of governance, and risk management frameworks.

•Provide objective evaluation of internal controls currently in place.

•Advises Council, ELT, and the Audit & Risk Committee on potential control strategies and design of new controls.

KEY:

↑ Accountability, reporting

↓ Delegation, direction, resources, oversight

Council, supported by the Audit and Risk Committee, specifies the nature, source, format, and frequency of the information it requires.

Factors Council consider for its reporting requirements include;

- The information needs of different stakeholders;
- Frequency and timeliness of reporting; and
- Relevance of information to strategic objectives and organisational decision-making.

This information assists Council in assessing whether or not the decisions being taken by the PSI are within its risk appetite, and whether any of the following are required;

- Re-assessment of its strategic objectives;
- Change to its policies;
- Reprioritisation of its resources; and
- Improvement to its system of internal controls.

Risk Reports to Council and/or the Audit and Risk Committee should include qualitative and quantitative information, and where appropriate, highlight trends, or relevant key risk indicators.

Council's understanding and decision-making should be supported through the presentation of information in summary form, and where possible, with the use of graphics and visual aids.

Risk reports should seek to support Council's understanding of how, and if, the level of the PSI's risk exposure is changing, and the extent to which internal controls are operating as intended.

The PSI will adapt its risk management framework if necessary, to address external and internal changes, improve its adequacy and effectiveness, through the consideration of lessons based on experience and, at least annually, review of the performance outcomes it achieves.

6. Approval of the Risk Management Framework

	Date	Description	Approved by
ÉÓL	30.07.2021	Version 0.1	NB/CS/CD
NB/CS	09/09/2021	Version 0.2	ELT
A&R Committee	30/11/2021	Version 0.3	PSI Council

This risk management framework will be reviewed on an annual basis.

7. References

ISO 31000: Risk Management Guidelines – International Organization for Standardization (ISO) 2018

Risk Management Guidance for Government Departments and Offices - Department of Public Expenditure and Reform, (DPER) 2016

Enterprise Risk Management – Integrating Strategy with Performance - The Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2017

Risk Management Policy & Guidelines 2017- Pharmaceutical Society of Ireland (PSI) 2017

A Structured Approach to Enterprise Risk Management and the Requirements of ISO 31000 - Institute of Risk Management (IRM) 2010

The Three Lines of Defense in Effective Risk Management – Institute of Internal Auditors (IIA) 2013

The Three Lines Model- An update of the Three Lines of Defense- Institute of Internal Auditors (IIA) 2020