THE STATE HOSPITALS BOARD FOR SCOTLAND

Risk and Resilience Annual Report 2024-25

Prepared by: Risk Management Team Leader and Acting Director of Security, Estates and Resilience

Approved by: Acting Director of Security, Estates and Resilience

CONTENTS

1. RISK MANAGEMENT DEPARTMENT

1.1 Introduction

The Risk and Resilience Department, situated within the Security Directorate, plays a pivotal role in safeguarding the organisation's operational integrity and ensuring preparedness across a range of critical domains. The department's core functions include:

- **Strategic Risk Management**: Development and ongoing maintenance of both Local and Corporate Risk Registers to ensure alignment with organisational objectives and regulatory requirements.
- **Risk Assessment**: Systematic evaluation of identified risks to inform mitigation strategies and support decision-making at all levels.
- **Resilience Planning**: Design, implementation, and periodic review of Resilience Plans to enhance the organisation's capability to respond to and recover from disruptive incidents.
- **Incident Management**: Oversight of incident reporting processes and facilitation of Enhanced Reviews for Category 1 and 2 incidents, ensuring lessons learned are captured and acted upon.
- **Health and Safety Governance**: Promotion and monitoring of health and safety standards across the organisation, in line with statutory obligations and best practice.
- **Duty of Candour Compliance**: Ensuring transparency and accountability through the effective application of Duty of Candour principles.
- **Datix System Administration**: Management of the Datix incident reporting system to support accurate data capture, analysis, and reporting.
- **Training and Capacity Building**: Delivery of targeted training programmes to embed a culture of risk awareness, resilience, and continuous improvement.

This department's work underpins the organisation's commitment to proactive risk management, regulatory compliance, and operational resilience.

1.2 Aims and Objectives

The Risk and Resilience Department continues to play a vital role in supporting the State Hospital's commitment to safety, quality, and operational continuity. Key areas of focus include:

- **Policy and Procedure Governance**: Development, implementation, and regular review of comprehensive Risk and Resilience policies and procedures to ensure alignment with best practice and regulatory standards.
- **Proactive Risk Identification and Management**: Early identification of emerging risks that may impact the State Hospital, followed by structured management using recognised risk management tools and methodologies.
- **Incident Review and Organisational Learning**: Implementation of robust incident review processes to ensure that significant adverse events are thoroughly investigated. Action Plans are developed to address root causes and promote continuous learning across the organisation.
- **Fostering a Quality Culture**: Supporting the development of a quality-driven culture by enhancing staff competencies and embedding effective risk management practices throughout the State Hospital.
- **Crisis Preparedness and Resilience**: Ensuring the hospital remains resilient and capable of operating beyond normal parameters during times of crisis, through the development and maintenance of comprehensive response frameworks.
- **Partnership and Collaboration**: Building and sustaining strong relationships with partner agencies to foster shared understanding, coordinated responses, and mutual learning opportunities.

2. GOVERNANCE

2.1 Committees/Groups

The Audit Committee holds overarching responsibility for evaluating the effectiveness of the organisation's internal control systems and corporate governance framework. This includes oversight of the Risk Management Strategy and its associated policies and procedures.

Risk management is fully embedded within the State Hospital's governance structure. Members of the Risk and Resilience team actively participate in the majority of hospital committees and groups, ensuring that risk considerations are integrated into decision-making processes at all levels.

Regular reporting is provided to these groups, covering key areas such as:

- Risk activity and emerging threats.
- Incident trends and analysis.
- Progress on adverse event action plans.
- Updates to local and corporate risk registers.
- Operational stability and resilience.

Key Committees and Groups Receiving Risk and Resilience Reports:

- Health and Safety Committee.
- Security and Resilience Group.
- Climate Change and Sustainability Group.
- Security, Risk & Resilience, Health & Safety Oversight Group.
- Audit Committee.
- Organisational Management Team.
- Clinical Governance Group/Committee.
- Corporate Management Team.
- Patient Safety Group.

In addition to these core groups, the Risk and Resilience team maintains a presence across a range of other hospital forums, including:

- Infection Control.
- Information Governance.
- Corporate Governance.
- And other operational and strategic groups as required.

This integrated approach ensures that risk awareness, resilience planning, and safety culture are consistently reinforced across the organisation.

3. KEY WORK ACTIVITIES (2024-2025)

3.1 Risk and Resilience

<u>3.1.1 Changes within Department</u>

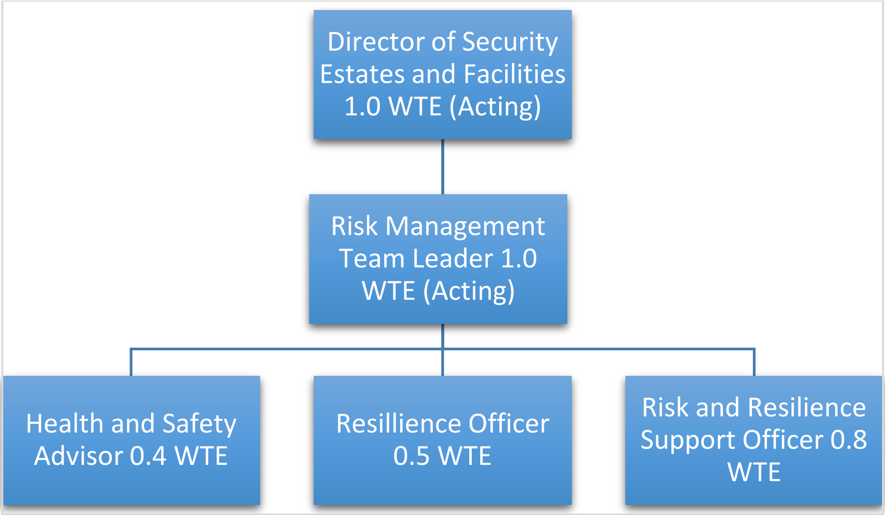
In 2024/25, the team underwent structural changes due to retirements, which created opportunities for staff to take on temporary 'acting up' roles:

- The Head of Risk and Resilience position is currently inactive, with the previous postholder temporarily acting as Director of Security, Risk and Resilience.

- The Risk Manager role from 2023/24 is also inactive. The postholder is currently acting as Risk Management Team Leader, overseeing the team and reporting directly to the Director of Security, Estates and Facilities.

In 2025/26, the team's structure will be reviewed and finalised, with a permanent organisational framework put in place.

Current Model as of March 2025, note that this structure is temporary.



Director of Security Estates and Facilities 1.0 WTE (Acting)

Risk Management Team Leader 1.0 WTE (Acting)

Health and Safety Advisor 0.4 WTE

Resillience Officer 0.5 WTE

Risk and Resilience Support Officer 0.8 WTE

3.1.2 Corporate Risk Register (Appendix 1)

A corporate risk is defined as a potential or actual event that:

- Interferes with the achievement of a corporate objective or target.
- Would have an extreme impact if effective controls were not in place; or
- Is operational in nature but cannot be mitigated to an acceptable level of risk.

Appendix A contains the current Corporate Risk Register, which now includes 25 risks distributed across the six Directorates. Risks are reviewed regularly throughout the year, with updates provided to the Corporate Management Team (CMT) and the Board. Four of the risks are currently graded as High, with the remainder classified as Medium or Low.

As part of a planned project, a comprehensive refresh of all corporate risks was undertaken last year. Each Directorate was reviewed individually. During this process, some risks were redefined, updated, merged with others, or moved to the Local Risk Register. Additional risks were also added to reflect emerging concerns and evolving priorities.

3.1.3 Department/Local Risk Registers

Departmental or Local Risk Registers capture risks specific to individual departments. These are risks that fall within the scope and capability of local managers to manage and are monitored and reviewed by the Head of Service. All departments are expected to maintain a Local Risk Register, supported by relevant risk assessments and action plans where necessary.

The Head of Department is responsible for informing the relevant Executive Director of any departmental risks. They must also identify risks that warrant escalation—particularly those graded as Very High or High—for potential inclusion in the Corporate Risk Register. Additionally, the Head of Department is accountable for the ongoing development, review, and updating of the Local Risk Register.

The Risk Manager continues to oversee the Local Risk Register process. Each department within the hospital maintains an active register, which is reviewed regularly and evolves in response to changes in the hospital environment. This process is supported by members of the Organisational Management Team.

The Corporate Management Team (CMT) is kept informed of progress through updates provided by the Director of Security, Estates and Resilience.

3.2 Resilience

The Director of Security, Estates and Resilience holds overall responsibility for the management of Resilience within the State Hospital. The Director also chairs both the Security, Risk and Resilience, Health and Safety Oversight Group and the Security and Resilience Group.

The Risk and Resilience Department supports these functions by producing an Annual Report for the Board's Audit Committee, as well as providing regular Resilience Reports to the relevant oversight groups.

3.2.1 Resilience Plans

3.2.1.1 Level 2 Plans

Level 2 Plans primarily address Loss of Service scenarios and are managed internally by operational teams. In most cases, services are restored quickly, and recovery is handled within standard operational procedures.

Currently, all Level 2 Plans are up to date. Each plan is subject to a three-year review cycle, during which it will be tested to ensure it remains fit for purpose. This process is coordinated by the Resilience Officer.

All Level 2 Plans are formally approved by the Security and Resilience Group.

3.2.1.2 Level 3 Plans

Our current Level 3 Plans remain fit for purpose, and all partner agencies are satisfied with the existing arrangements. These plans are based on a multi-agency joint working model, involving collaboration with Police Scotland, Scottish Fire and Rescue Service, Scottish Ambulance Service, South Lanarkshire Council, and the West of Scotland Regional Resilience Partnership.

Work is ongoing to redevelop the Level 3 Plans. A first draft has been shared with partner agencies for feedback.

Over the past year, the following documents have been completed and approved:

- Multi-Agency Incident Response Guide (MAIRG).
- MAIRG Contingency Plans.
- State Hospital Roles and Responsibilities.

The final document, outlining action plans, is scheduled for completion by September 2025.

3.2.2 Resilience Related Incidents

In line with the approved Resilience Framework, all resilience related incidents are reported via Datix, with Level 2 and 3 incidents being reviewed directly by the Security, Risk and Resilience, Health and Safety Oversight Group.

The Incident levels are defined within the Resilience Framework as follows:

- **Level 1**: Incidents which cause minor service disruption with one area/department affected which can be contained and managed within the local resources.
- **Level 2**: Incidents which cause significant service disruption, interruption to hospital routine, special deployment of resources and affect multiple areas/departments.
- **Level 3**: A major/emergency situation which seriously disrupts the service and causes immediate threat to life or safety. These incidents will require the involvement of the Emergency Services.

Over the year April 24 – March 25, there have been 3 incidents managed at Level 3 and zero Level 2 incidents out with the staffing issues recorded.

	2020/21	2021/22	2022/23	2023/24	2024/25
Level 2	0	19	8 (+ 3106 staffing resource)	0 (278, All staffing resource, only full closure)	1 (23 full closure incidents were recorded)
Level 3	4	0	0	1	2

One Level 2 incident was recorded this year. The incident occurred in response to a Red Category Storm Warning, which subsequently led to internal and external power supply issues within the State Hospital.

Other incidents that were recorded were in relation to full ward closures due to staffing resource issues. While the number of such incidents remains high, it represents a significant reduction compared to previous years. No other incidents within the State Hospital met the criteria for Level 2 classification; all other events were effectively managed within standard service operations.

Two Level 3 incidents were recorded during the year and both involved the activation of Incident Command following violent behaviour by patients in their rooms, requiring coordinated support for their safe removal.

3.2.3 Training and Exercising

3.2.3.1 Risk Management Training

Datix training was delivered to all new staff during induction and also to 10 staff members in management roles, along with additional personnel supporting the Risk and Resilience Team. The training is designed to:

- Teach staff how to navigate and use the Datix system effectively.
- Ensure quality assurance of all Datix entries.
- Support thorough investigation of incidents recorded in Datix.
- Enable staff to extract and analyse data from the system.

Training is delivered on a continuous basis by the Risk Manager, and in future, will also be supported by the Risk Project Support Officer.

3.2.3.2 Resilience Training

Resilience training is a key component of our strategy to develop and maintain high resilience standards across the organisation. Over the past year, we have continued to strengthen our capabilities through a series of targeted training events, including:

- Completion of Level 3 PPE refresher and accreditation training.
- Delivery of Critical Incident Communicator (CIC) CPD events for the State Hospital CICs.

- One CIC attended the full Negotiator Course at Tulliallan Police College.
- One CIC attended the Negotiator Coordinator (Neg CO) Course at Tulliallan.
- Delivery of Mental Health Awareness sessions to Police Scotland Negotiator Unit and, more recently, the Scottish Prison Service.
- Golden Hour training for Operational Managers.
- Induction training for new nurses (First on the Scene).
- A cyberattack simulation exercise conducted in collaboration with eHealth and an external contractor, involving multiple Heads of Service.

3.2.4 Partner Agency Working

Maintaining and developing strong relationships with our partner agencies is a key component of our resilience strategy, particularly during times of crisis. Our key partners include:

3.2.4.1 Police Scotland

Our relationship with Police Scotland remains strong. Over the past twelve months, the following milestones have been achieved:

- Continued support from a dedicated Police Scotland response team for the hospital, with close liaison with the Security Department.
- Operational site visits for all new response inspectors and sergeants for familiarisation and situational awareness.
- Joint development of our Level 3 and Multi-Agency Incident Response Plans.
- Participation in the Emergency Services Mobile Communications Programme survey of the hospital, involving all emergency services.

3.2.4.2 Scottish Fire and Rescue Service

- The State Hospital has continued to work closely with Scottish Fire and Rescue through the Local Resilience Partnership (LRP) over the past year. Operational site visits continue for all relevant visiting crews. Continued work with operational intelligence (OI) for fire crews and also yearly fire safety visits.

3.3.4.3 Scottish Ambulance Service

Key milestones achieved in collaboration with the Scottish Ambulance Service include:

- Operational familiarisation visits to the hospital with key departments
- Development of flow navigation pathways to support patient care
- Creation of support resources for alternative care options

3.3.4.4 South Lanarkshire Council

As part of the local LRP, we maintain a close working relationship with South Lanarkshire Council. We have facilitated familiarisation visits for new staff to help them understand hospital operations and foster shared learning. This collaborative work will continue.

3.3.4.5 Critical National Infrastructure

The hospital is actively engaged in the Four Nations Critical National Infrastructure database through the Emergency Preparedness, Resilience and Response (EPRR) framework.

3.2.5 Business Continuity Arrangements

Our Business Continuity Policy was revised and approved by PAG in January 2025.

3.3 Health & Safety

3.3.1 Control Book Audits

Health & Safety Electronic Control Books (eCBs) provide the framework for managing Health & Safety arrangements across the State Hospital. The hospital currently operates approximately 30 eCBs, each audited within a two-year cycle to ensure compliance with both organisational and local policies and procedures.

In the 2024/25 period, eight Control Books were audited. A new approach has been introduced whereby the Health & Safety Advisor conducts a pre-audit review of documentation and provides feedback to the Control Book holder before the full audit. This proactive method fosters collaboration, reduces conflict, and has been positively received by staff. It also supports the development of teamwork, confidence, and competence in Health & Safety practices.

During the audit process, an opportunity for improvement was identified in the consistency of Control Book documentation and the application of risk assessments. Staff have welcomed the proposal to standardise and update generic documentation. A comprehensive review is currently underway, led by the Health & Safety Advisor.

All audited areas achieved green scores (above 80%), providing assurance that Health & Safety standards across the hospital remain high. These areas continue to be actively managed by staff and will be formally re-audited in two years, with full engagement from both staff and senior management.

3.3.2 2024/25 Training Plan

Staff Training remains a key priority for the Risk Management team. Since taking up the role in February 2024, the Health & Safety Advisor—supported by the Risk Manager—has focused on engaging with and developing the electronic Control Book holders and their deputies.

This initiative has had a highly positive impact, enhancing staff support and development while significantly increasing confidence and competence in managing the Control Book and its contents.

Looking ahead, the team aims to expand training opportunities across the State Hospital to further strengthen Health & Safety knowledge and awareness among all staff.

3.3.3 Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR)

RIDDOR requires employers to report incidents that arise out of or in connection with work, including:

- The death of any person.
- Specified injuries to employees or hospital treatment for non-employees.
- Employee injuries resulting in more than seven consecutive days of absence.
- Dangerous occurrences.
- Certain occupational diseases.
- In 2024/25, there was an increase of 26 reported RIDDOR incidents compared to the previous year (2023/24). This rise highlights the need for continued focus on incident prevention, staff training, and robust risk assessment practices.

	Q1	**Q2**	**Q3**	**Q4**	**2022/23**	**2023/24**	**2024/25**
‘Specified’ Injuries*	2	4	1	1	**1**	**2**	**8**
Over 7 day lost time Injury	5	11	6	10	**7**	**12**	**32**
Total	7	15	7	11	**8**	**14**	**40**

All RIDDOR incidents were reported to the Health and Safety Executive (HSE) as required. However, during the year, several incidents were not communicated to the Risk and Resilience Team within appropriate timescales. This highlighted a gap in training and internal reporting processes.

To address this, improvement work has been underway and is scheduled for completion in June 2025. The aim is to strengthen internal reporting procedures and ensure timely escalation of incidents.

All individual RIDDOR incidents continue to be monitored and reviewed by the Health and Safety Committee. Following each report, relevant risk assessments are updated to reflect any new findings or required controls.

3.4 Fire

During the year, five fire alarm activations occurred at the State Hospital, all of which received a response from the Scottish Fire & Rescue Service. Importantly, no actual fires were identified. Of the five incidents:

- Three were due to faults within the fire alarm system.
- Two were triggered by smoke caused by bread overheating in toasters.

These events highlight the importance of ongoing maintenance and staff awareness to minimise false alarms and ensure effective emergency response.

3.5 Incident Reporting

Datix is the hospital's electronic incident reporting system, accessible to all staff via the intranet and through a desktop shortcut on every hospital computer.

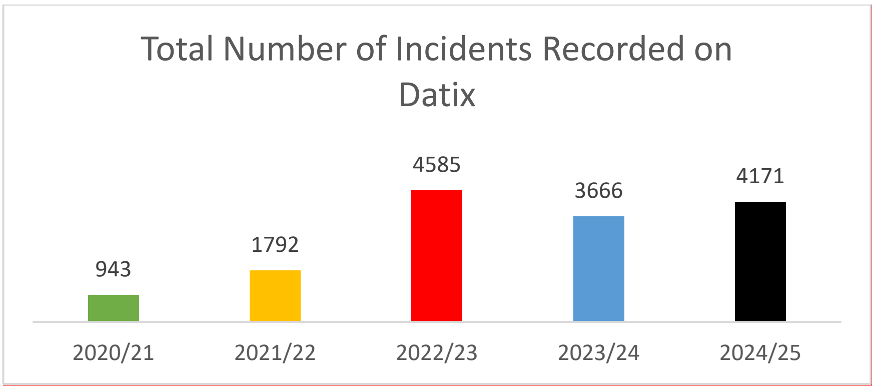
Each reported incident is investigated locally to ensure that appropriate remedial and preventative actions are taken. The system also supports the identification of incident trends and significant individual events through well-defined processes.
Datix classifies incidents into seven overarching types:

1. Health and Safety
2. Security
3. Direct Patient Care
4. Equipment, Facilities & Property
5. Communication / Information Governance
6. Infection Control
7. Other

This classification helps ensure that incidents are appropriately categorised and addressed, supporting continuous improvement in safety and service delivery.

3.5.1 Datix Incidents

4,171 incident reports were finally approved during 2024/25; a significant increase in the number of incidents finally approved in 2023/24 (3666). The chart below shows the changes in the number of incidents reported within Datix over the last five years.



3.5.2 Incident 'Type' Trends over last 5 years

Incident Type	2020/21	2021/22	2022/23	2023/24	2024/25
Staffing Resource	X**	X**	3192	**2296**	**2264**
Health & Safety	413	461	660	**554**	**886**
Security	93	139	277	**297**	**348**
Direct Patient Care	142	146	206	**232**	**386**
Equipment/Facilities/Property	78	75	105	**135**	**171**
Infection Control	55	60	77	**53**	**18**
Communication/Information Governance	48	65	51	**94**	**88**
Other	115	846	11	**5**	**10**
Totals	943	1792	4585	**3666**	**4171**
*Average Patient Population	114	115	110	102	101

* based on bed compliment at end of each quarter/4
** Staffing resource not recorded

Incidents are monitored by relevant groups who are responsible for taking forward any additional actions.

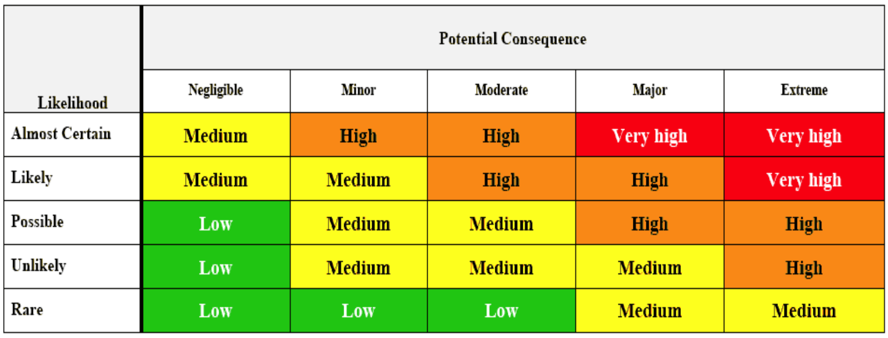
3.5.3 Risk Assessment

The process of risk assessment at the State Hospital involves evaluating two key factors:

- Likelihood of an event occurring (e.g. rare, unlikely, possible).
- Impact or consequence of the event on the organisation (e.g. financial, reputational, operational, regulatory).

The table and chart below illustrate the number of incidents graded as **High** and **Very High** risk from 2020/21 to 2024/25. These figures have substantially decreased from last year, primarily due to a reduction in reported Staff Resource Incidents.

The significant drop in 2024/25 reflects improvements in how staffing is detailed and managed across the hospital, resulting in fewer high-severity incidents and demonstrating the positive impact of proactive workforce planning and risk mitigation strategies.



Likelihood	Potential Consequence				
	Negligible	Minor	Moderate	Major	Extreme
Almost Certain	Medium	High	High	Very high	Very high
Likely	Medium	Medium	High	High	Very high
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Medium	Medium	Medium	High
Rare	Low	Low	Low	Medium	Medium

Year	No. of “High” or “Very High”Graded Risk Incidents
2020/21	0
2021/22	628
2022/23	684
2023/24	2026
2024/25	305

3.5.4 Duty of Candour

The Organisational Duty of Candour is a legal obligation that outlines how healthcare organisations must respond when an unintended or unexpected incident results in harm or death.

Under this duty, organisations are required to:

- Inform those affected that such an incident has occurred.
- Offer a sincere apology.
- Involve the individual or their family meaningfully in a review of what happened.

This process ensures transparency, accountability, and a commitment to learning and improvement in the delivery of care.

Duty of Candour Incidents	2021/22	2022/23	2023/24	2024/25
Considered	103	115	54	170
Investigated	1	0	2	4

- There was a sharp increase in incidents considered in 2024/25, rising to 170 from just 54 the previous year.
- Despite the increase in cases considered, the number of incidents formally investigated remained low across all years, peaking at only 4 in 2024/25.
- This trend may reflect improved identification and reporting processes, while maintaining a high threshold for formal investigation.

In 2024/25, a total of **four** Duty of Candour incidents were formally recorded at the State Hospital.

All four incidents involved serious injuries sustained by patients during the course of their care. Each case was thoroughly investigated through the appropriate internal review processes, in line with statutory Duty of Candour requirements.

Further details and analysis can be found in the Duty of Candour Annual Report 2024/25.

3.6 Serious Adverse Event Reviews (SAER)

SAERs are conducted to identify the contributing factors of an incident, with the aim of reducing the likelihood and/or impact of similar events in the future. The level of review is proportionate to the severity of the incident:

- Category 1 Reviews are the most rigorous and involve a full Root Cause Analysis. These are used for the most serious incidents to ensure comprehensive organisational learning.
- Category 2 Reviews are used for less serious incidents that still require an in-depth investigation to identify learning points and reduce the risk of recurrence.

SAERs are typically commissioned by the Corporate Management Team (CMT), following notification from the Risk and Resilience Department, who monitor Datix for incidents that meet the criteria.

SAERs Commissioned in 2024/25.

Category 1 Review:

- Cat 1 24-01 – Duty of Candour.

Category 2 Reviews:

- Cat 2 24/01 – Fracture.
- Cat 2 24/02 – Delay in Treatment.
- Cat 2 24/03 – Fracture.
- Cat 2 24/04 – Mental Health Act (MHA) Renewal.

3.7 Freedom of Information (FOI) Responses

During 2024/25 the Risk Management Team received 4 FOI requests totalling 18 questions. The team provided data for all of them where it was held by our department.

The Risk and Resilience Team also received 1 Subject Access Request

4. SUMMARY

4.1 Areas of Good Practice

In addition to the positive outcomes highlighted throughout this report, several areas of good practice have been identified across the hospital in relation to risk management:

4.1.1 Hospital-Wide Practices

- Effective monitoring of risk information by relevant groups and committees.
- Regular review of patient-specific risks by clinical teams.
- Strong evidence of learning from incidents, with local actions implemented to minimise recurrence.

4.1.2 Risk Management Department Initiatives

Continued development of the Corporate Risk Register in collaboration with risk owners, resulting in a streamlined and up-to-date register for 2024/25.

Delivery of resilience training programmes across the hospital, including:

- Incident Command.
- Golden Hour Training.
- Level 2 Plan Exercises.
- Redevelopment of the Learning from Events process, enabling the collation, monitoring, and implementation of learning from multiple sources.
- Ongoing work to enhance the SAER process, ensuring a more robust system for commissioning, monitoring, and approvals.
- Updates to the RIDDOR process to ensure full compliance with Health and Safety legislation.

Review and relaunch of the Health and Safety Management System, including:

- Staff training.
- Continuation of audits in 2024/25.
- Development of an updated Control Book process.
- Continued internal development of the Datix Incident Reporting System throughout 2024/25.
- Increased team capability through acting-up opportunities, enhancing experience and resilience.
- Agreement of the InPhase contract, with implementation scheduled for 2025/26.

4.2 Identified Issues and Potential Service Developments

4.2.1 Capacity Challenges in Managing SAERs

During 2024/25, the Risk and Resilience Team experienced difficulties managing the volume of Category 1 and 2 Significant Adverse Event Reviews (SAERs), particularly when multiple reviews were commissioned simultaneously. This issue was raised throughout the year, as only one team member was available to act as an investigator, creating a capacity bottleneck.
To address this, future plans include involving hospital managers more directly in the SAER process. This will be supported by the establishment of a dedicated SAER Group, currently in development, which will oversee commissioning, monitoring, and support for investigations.

4.2.2 Delays in RIDDOR Reporting

In 2024/25, several RIDDOR incidents were not reported to the Risk and Resilience Team within the required timescales, resulting in multiple late submissions and breaches of Health and Safety regulations.

In response, the reporting process was reviewed and revised to ensure timely and compliant reporting going forward. These changes aim to strengthen internal communication and reinforce accountability across departments.

5. NEXT REVIEW DATE

The next annual report will be submitted to the Audit Committee in June 2026.

High Risks

Ref No.	Category	Risk	Initial Risk Grading	Current Risk Grading	Target Risk Grading	Owner	Action officer	Next Scheduled Review	Governance Committee	Monitoring Frequency	Movement Since Last Report
Corporate MD 30	Medical	Failure to prevent/mitigate obesity	Major x Likely	Major x Likely	Moderate x Unlikely	Medical Director	Lead Dietitian	May 25	Clinical Governance Committee	Monthly	-
Corporate ND 70	Service/Business Disruption	Failure to utilise our resources to optimise excellent patient care and experience	Major x Likely	Moderate x Likely	Minor x Unlikely	Director of Nursing & AHP	Director of Nursing & AHP	May 25	Clinical Governance Committee	Monthly	-
Corporate FD 90	Financial	Failure to implement a sustainable long term model	Major x Almost Certain	Major x Possible	Moderate x Rare	Finance & Performance Director	Finance & Performance Director	May 25	Finance and Performance Group	Monthly	-
Corporate SD57	Health & Safety	Failure to complete actions from Cat 1/2 reviews within appropriate timescale	Moderate x Likely	Moderate x Likely	Moderate x Unlikely	Finance & Performance Director	Head of Corporate Planning and Business Support	May 25	Security, Risk and Resilience Oversight Group	Monthly	-

Medium Risks

Ref No.	Category	Risk	Initial Risk Grading	Current Risk Grading	Target Risk Grading	Owner	Action officer	Next Scheduled Review	Governance Committee	Monitoring Frequency	Movement Since Last Report
Corporate CE 10	Reputation	Severe breakdown in appropriate corporate governance	Extreme x Possible	Major x Rare	Major Rare	Chief Executive	Board Secretary	May 25	Corporate Governance Group	Quarterly	-
Corporate CE 11	Health & Safety	Risk of patient injury occurring which is categorised as either extreme injury or death	Extreme x Possible	Extreme x Rare	Extreme x Rare	Chief Executive	Head of Risk and Resilience	May 25	Clinical Governance Committee	Quarterly	-
Corporate CE 12	Strategic	Failure to utilise appropriate systems to learn from prior events internally and externally	Major x Possible	Moderate x Possible	Negligible x Unlikely	Chief Executive	Head of Risk and Resilience	May 25	Security, Risk and Resilience Oversight Group	Quarterly	-
Corporate MD 34	Medical	Lack of out of hours on site medical cover	Major x Likely	Major x Unlikely	Major x Unlikely	Medical Director	Associate Medical Director	May 25	Clinical Governance Committee	Quarterly	-
Corporate SD 51	Service/Business Disruption	Physical or electronic security failure	Extreme x Unlikely	Major x Unlikely	Major x Rare	Security Director	Security Director	May 25	Security, Risk and Resilience Oversight Group	Quarterly	-
Corporate SD 52	Service/Business Disruption	Resilience arrangements that are not fit for purpose	Major x Unlikely	Moderate x Unlikely	Moderate x Rare	Security Director	Security Director	May 25	Security, Risk and Resilience Oversight Group	Quarterly	-
Corporate SD 54	Service/Business Disruption	Implementing Sustainable Development in Response to the Global Climate Emergency	Major x Likely	Moderate x Possible	Moderate x Rare	Security Director	Head of Estates and Facilities	May 25	Security, Risk and Resilience Oversight Group	Quarterly	-
Corporate ND 71	Health & Safety	Serious Injury or Death as a Result of Violence and Aggression	Extreme x Almost Certain	Moderate x Possible	Minor x Unlikely	Director of Nursing & AHP	Director of Nursing & AHP	May 25	Clinical Governance Committee	Quarterly	-
Corporate FD 96	Service/Business Disruption	Cyber Security	Moderate x Likely	Moderate x Unlikely	Moderate x Unlikely	Finance and Performance Director	Head of eHealth	May 25	Information Governance Committee	Quarterly	-
Corporate FD 98	Reputation	Failure to comply with Data Protection Arrangements	Moderate x Likely	Moderate x Unlikely	Moderate x Unlikely	Finance and Performance Director	Head of eHealth/ Info Gov Officer	May 25	Information Governance Committee	Quarterly	-
Corporate HRD 111	Reputation	Deliberate leaks of information	Major x Possible	Major x unlikely	Major x unlikely	HR Director	HR Director	May 25	HR and Wellbeing Group	Quarterly	-

Ref No.	Category	Risk	Initial Risk Grading	Current Risk Grading	Target Risk Grading	Owner	Action officer	Next Scheduled Review	Governance Committee	Monitoring Frequency	Movement Since Last Report
Corporate HRD 112	Health & Safety	Compliance with Mandatory PMVA Level 2 Training	Major x Possible	Moderate x Possible	Moderate x Rare	HR Director	Training & Professional Development Manager	May 25	Clinical Governance Group	Quarterly	-
Corporate HRD 113	Service/Business Interruption	Job Evaluation and impact on services in the State Hospital	Major x Possible	Moderate x Possible	Negligible x Unlikely	HR Director	HR Director	May 25	HR and Wellbeing Group	Quarterly	-

Low Risks

Ref No.	Category	Risk	Initial Risk Grading	Current Risk Grading	Target Risk Grading	Owner	Action officer	Next Scheduled Review	Governance Committee	Monitoring Frequency	Movement Since Last Report
Corporate CE15	Reputation	Impact of Covid-19 Inquiry	Extreme x Likely	Moderate x Rare	Moderate x Rare	Chief Executive	Board Secretary	May 25	Covid Inquiry SLWG	6 Monthly	-
Corporate SD 50	Service/Business Disruption	Serious Security Incident or Breach	Extreme x Likely	Moderate x Rare	Moderate x Rare	Security Director	Security Director	Aug 25	Security, Risk and Resilience Oversight Group	6 Monthly	-
Corporate SD 56	Service/Business Disruption	Water Management	Moderate x Unlikely	Moderate x Rare	Moderate x Rare	Security Director	Head of Estates and Facilities	Aug 25	Security, Risk and Resilience Oversight Group	6 monthly	-
Corporate FD 91	Service/Business Disruption	IT system failure	Moderate x Likely	Negligible x Possible	Negligible x Possible	Finance & Performance Director	Head of eHealth	Oct 25	Finance and Performance Group	6 Monthly	-
Corporate FD 97	Reputation	Unmanaged smart telephones' access to SH information and systems.	Major x Likely	Moderate x Rare	Moderate x Rare	Finance and Performance Director	Head of eHealth	Aug 25	Information Governance Committee	6 Monthly	-
Corporate FD 99	Reputation	Compliance with NIS Audit	Major x Likely	Moderate x Rare	Moderate x Rare	Finance and Performance Director	Head of eHealth	Oct 25	Information Governance Committee	6 Monthly	-
Corporate HRD 110	Resource	Failure to implement and continue to develop the workforce plan	Moderate x Possible	Moderate x Rare	Moderate x Rare	HR Director	HR Director	Oct 25	HR and Wellbeing Group	6 Monthly	-