Risk Management and Risk Register Policy

Sample policy template. This is a Verivius-authored template anchored to the statutory regulation and current CQC/professional guidance. Tenants must adapt the operational sections to their own organisation, service type, workforce, premises and professional requirements. Where this template and live law or regulator guidance diverge, the live source wins.

Statutory anchor: Regulation 17 (good governance), Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (SI 2014/2936). This policy also engages Regulation 12 (safe care and treatment). **Primary source:** https://www.legislation.gov.uk/uksi/2014/2936/regulation/17 **Last reviewed:** 2026-06-10 **Verivius pack version:** v1, 2026-06-10

Policy owner: Registered Manager. **Applies to:** all staff and all regulated activities carried on by the service.

1. What the regulation says

> Systems or processes must be established and operated effectively to ensure compliance with the requirements in this Part. (Regulation 17(1))
>
> assess, monitor and improve the quality and safety of the services provided in the carrying on of the regulated activity (including the quality of the experience of service users in receiving those services) (Regulation 17(2)(a))
>
> assess, monitor and mitigate the risks relating to the health, safety and welfare of service users and others who may be at risk which arise from the carrying on of the regulated activity (Regulation 17(2)(b))
>
> Regulation 12 adds the safe-care duties that this policy operationalises:
>
> assessing the risks to the health and safety of service users of receiving the care or treatment (Regulation 12(2)(a))
>
> doing all that is reasonably practicable to mitigate any such risks (Regulation 12(2)(b))
>
> The full text is at https://www.legislation.gov.uk/uksi/2014/2936/regulation/17 and https://www.legislation.gov.uk/uksi/2014/2936/regulation/12. Where this policy and the regulation diverge, the regulation wins.

2. Plain-English summary

You have to run effective systems and processes to assess, monitor and improve quality and safety, and to assess, monitor and mitigate risks to people's health, safety and welfare. A live risk register, with owners, actions and review dates, is how a service shows it knows its risks, is acting on them, and is checking whether those actions work. A risk that is known but not acted on can itself become evidence of poor governance.

3. Purpose

The purpose of this policy is to make sure that risks to people using the service, staff, visitors and others are identified, assessed, controlled, reviewed and escalated.

Risk management is not a separate office task. It is part of safe care, good governance and everyday leadership. The service must be able to show that it knows its risks, understands their impact, takes action to reduce them, and checks whether those actions are working.

This policy supports Regulation 12 and Regulation 17 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014.

4. Policy warning

Risks must not be left informal, hidden in manager memory, or discussed repeatedly without ownership and action.

Where a risk could affect the health, safety, welfare, rights or experience of people using the service, it must be recorded, assessed, assigned, monitored and reviewed.

A risk that is known but not acted on may become evidence of poor governance.

5. Scope

This policy applies to risks relating to:

- people using the service
- clinical care and treatment
- medicines
- safeguarding
- staffing
- staff competence
- infection prevention and control
- premises, equipment and vehicles
- information governance

- complaints and incidents
- business continuity
- external providers and contractors
- financial or operational pressures that may affect safe care
- regulatory compliance
- leadership, governance and culture

6. Definitions

A **risk** is something that could cause harm, unsafe care, poor experience, service failure or regulatory non-compliance.

A **control** is something already in place to reduce the likelihood or impact of the risk.

A **risk rating** is the service's judgement of likelihood and impact.

A **risk register** is the live record of significant risks, controls, owners, actions and review dates.

A **closed risk** is a risk that has been removed or reduced to a level the service formally accepts, with evidence and rationale.

7. Responsibilities

All staff are responsible for identifying and reporting risks.

Managers are responsible for assessing risks, agreeing controls, escalating concerns and ensuring actions are completed.

The Registered Manager is responsible for maintaining the risk register and ensuring that significant risks are reviewed through governance meetings.

The Nominated Individual or provider representative is responsible for reviewing high and persistent risks and ensuring that the provider takes action where service-level controls are not enough.

8. Risk identification

Risks may be identified through:

- incidents and near misses
- complaints
- safeguarding concerns
- audits

- staff feedback
- supervision
- service-user or family feedback
- external alerts
- CQC findings
- local authority or commissioner feedback
- professional advice
- environmental checks
- staffing reviews
- training gaps
- changes to service model
- new people admitted, accepted or referred to the service
- changes in people's needs
- business continuity events

Staff must be encouraged to raise risks early. A risk raised in good faith must not be treated as criticism or disloyalty.

9. Risk assessment

Each risk must be assessed by a competent person. The assessment must consider:

- what could happen
- who could be affected
- likelihood
- impact
- existing controls
- gaps in controls
- immediate action needed
- longer-term action needed
- owner
- review date
- escalation route

The assessment must balance safety with the person's rights, choices, preferences and independence where relevant.

10. Risk rating

The service will use a simple risk rating system based on likelihood and impact. Each risk will be rated as:

- low
- moderate
- high
- extreme

The rating must reflect the risk after existing controls have been considered.

High and extreme risks must be escalated to the Registered Manager immediately. Extreme risks must also be escalated to the Nominated Individual or provider representative.

11. Risk register

The risk register must include:

- risk title
- description
- date identified
- source of risk
- people or area affected
- current controls
- likelihood
- impact
- overall rating
- owner
- actions required
- action due dates
- review date
- escalation status
- current status
- closure rationale where closed

The risk register must be kept up to date. It must be a live governance tool, not a document updated only before inspection.

12. Controls and actions

For each risk, the service must decide whether to:

- tolerate the risk with existing controls
- reduce the risk through further action
- transfer or share the risk with another responsible body
- stop the activity creating the risk
- escalate the risk to provider level or an external body

Actions must have an owner, due date and evidence requirement.

Where a control depends on staff behaviour, training or supervision, the service must check whether it is actually being followed in practice.

13. Escalation

A risk must be escalated where:

- it is high or extreme
- people are at immediate risk of harm
- actions are overdue
- controls are not working
- the same risk has repeated
- the risk affects more than one person or service area
- the manager cannot resolve it within existing authority or resources
- external advice or notification may be required
- the risk may affect registration, safety or continuity of service

Escalation may be internal, to the provider or board, or external to safeguarding, CQC, commissioner, professional body, emergency services or another relevant organisation. The escalation decision must be recorded.

14. Review frequency

Risks must be reviewed at a frequency proportionate to their rating:

- extreme risks: at least weekly, or more often while unstable
- high risks: at least monthly
- moderate risks: at least quarterly
- low risks: at least six-monthly or through routine governance review

Risks must also be reviewed after incidents, complaints, safeguarding concerns, staffing changes, new guidance, inspection findings or material changes in the service.

15. Closing a risk

A risk may only be closed where the Registered Manager is satisfied that:

- the risk has been removed, or
- the risk has reduced to an accepted level, or
- the risk has transferred to another appropriate process

The closure record must include:

- reason for closure
- evidence reviewed
- person approving closure
- date closed
- any ongoing monitoring needed

A risk must not be closed simply because an action has been completed. The service must consider whether the risk has actually changed.

16. Links with incidents, complaints, safeguarding and audits

The risk register must link to other governance processes.

The Registered Manager must consider adding or updating a risk where there is:

- a serious incident
- repeated incidents
- safeguarding concern
- complaint theme
- audit failure
- repeated missed action
- staffing instability
- training gap
- CQC finding
- external alert
- business continuity event

The service must be able to show how information from one governance process affects the others.

17. Service-level and person-level risks

Person-level risks must be recorded in the person's care record, risk assessment or care plan.

Service-level risks must be recorded on the risk register.

Where a person-level risk reveals a wider service issue, such as repeated falls, medicine errors or staffing shortage, the wider issue must be added to the risk register.

18. Provider oversight

The provider, Nominated Individual or responsible director must review the risk register at least quarterly. They must pay particular attention to:

- high and extreme risks
- overdue actions
- repeated themes
- risks without clear ownership
- risks requiring investment or staffing change
- risks that may affect regulatory compliance
- risks that have not reduced after repeated review

Provider review must be recorded.

19. Evidence

The service must keep evidence of:

- risk assessments
- risk register entries
- control measures
- completed actions
- escalation decisions
- provider reviews
- external advice
- closure rationale
- communication with staff or people using the service
- audit of whether controls are working

20. Audit

The Registered Manager must audit the risk register at least quarterly. The audit must check:

- whether risks are current
- whether ratings are appropriate
- whether owners are named
- whether actions are overdue
- whether escalation has happened when required
- whether closed risks have evidence
- whether incident and complaint themes are reflected
- whether high risks have provider oversight

Audit findings must be recorded and actioned.

21. Related policies in this pack

This policy should be read with:

- Incident Reporting, Investigation and Learning Policy
- Action Plan and Improvement Tracking Policy
- Good Governance Policy
- Safe Care and Treatment Policy
- Safeguarding Policy
- Complaints Policy
- Clinical Audit and Quality Assurance Policy
- Staffing Policy
- Business Continuity Policy
- CQC Statutory Notifications Policy

22. Review

This policy will be reviewed annually, or sooner following a serious incident, safeguarding concern, CQC inspection finding, significant service change, or repeated failure to manage risk effectively.

23. Sources and further reading

This template is based on CQC's guidance for providers and managers, the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, and other topic-specific legislation and guidance listed below. It is a starting point for adaptation, not a substitute for legal, clinical, HR, safeguarding or specialist professional advice.

- CQC Regulation 17: Good governance

- CQC Regulation 12: Safe care and treatment
- HSE risk assessment guidance
- Local authority safeguarding procedures (where a risk involves abuse or neglect)
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (https://www.legislation.gov.uk/uksi/2014/2936/regulation/17)

24. When to seek further advice

Seek specialist advice where the issue involves serious harm, safeguarding, deprivation of liberty, restraint, children, professional misconduct, controlled drugs, radiation, termination of pregnancy, infection outbreak, water safety, employment dismissal, DBS barring referral, or regulatory enforcement.

25. Document control

Version	Date	Author	Changes
v1	2026-06-10	Verivius (sample)	Initial sample template, conformed to the Verivius policy standard.

This sample policy template was issued by Verivius. It is a template, not a substitute for legal advice or the tenant's own policy-development process. Where this template and live law or regulator guidance diverge, the live source wins.
