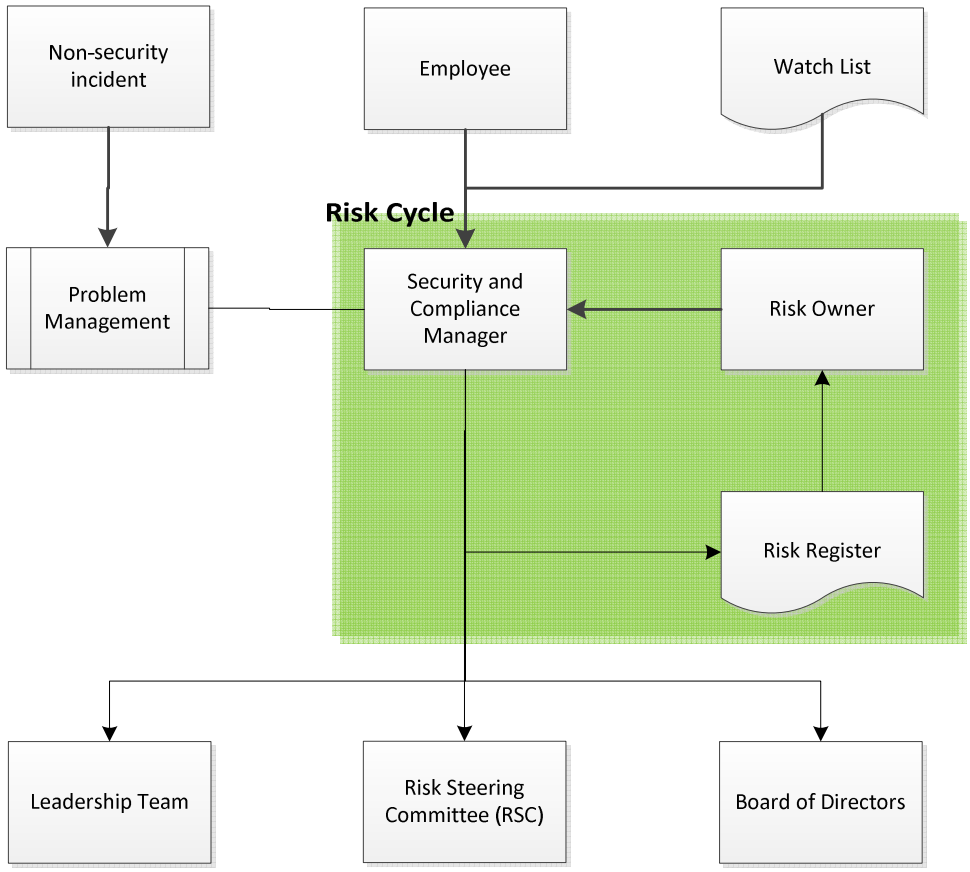
8. Risk Management



- **Risk Management Group**
  - Chairperson
    - Paul Cocker – *Head of Security and Compliance*
  - Participants
    - Ben Hood – *CEO*
    - Christian Berthelsen – *CTO*
    - Adrian Chalmers – *Director of Fourth Connect and Data Services*
    - Stuart Goldblatt – *CFO*
    - Mhairi Weir – *General Counsel*

8.1. Risk flow

- **Non-security incident**
  - Feeds into the Problem Management procedure
- **Problem Management**
  - Identify common root causes of incidents
  - Raise problems

    - Flag problems which represent a new risk to the Head of Security and Compliance
- **Employee**
    - Report suspected risks, information security events and information security incidents to the Head of Security and Compliance
- **Head of Security and Compliance**
    - Risks, information security events and information security incidents should be raised with the Risk Management Group
    - Maintain the Risk Register
    - Chair the Risk Steering Committee
    - Manage day-to-day running of the ISMS
- **Risk Owner**
    - Propose risk treatment
    - Implement risk treatment
    - Regular meetings with Head of Security and Compliance
- **Risk Register**
    - A record of all known risks to Fourth, their risk rating, their controls, agreed treatments and current treatment status
- **Risk Steering Committee**
    - Meets quarterly
    - Examine business risk profile
    - Review priority risks
    - Review and approve new company-wide polices, standards, procedures and guidelines
    - Discuss information security incidents
    - Agree direction of the risk management programme
    - Assign resources to meet risk profile goals

9. Risk Measurement

It is not necessary for Fourth employees to read this section unless they are part of the Risk Management Group or acting as a risk owner.

9.1. Risk scoring

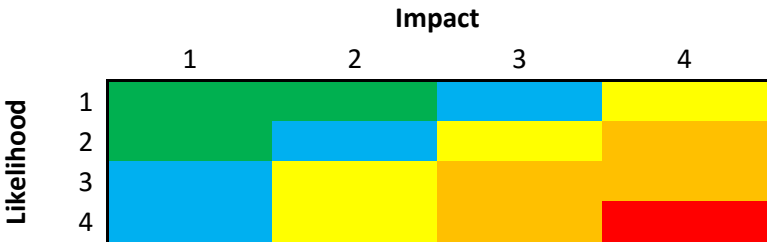
Two factors are combined to generate a risk score: the likelihood of the risk occurring and the impact to the business should it occur.

Likelihood:

1. Extremely unlikely to occur
2. Unlikely to occur
3. Likely to occur
4. Expected to occur

Impact:

1. Minimal impact
2. Moderate loss of revenue/damage to brand
3. Major loss of revenue/damage to brand
4. Major impact to the company's ability to do business



Green: Minimal risk
Blue: Low risk
Yellow: Medium risk
Orange: High risk
Red: Critical risk

See section 9.4 for how the risk score is adjusted according to control effectiveness.

9.2. Risk treatment

Once a risk has been identified and scored an agreement must be reached as to how to approach the risk. There are a number of different naming conventions, but all cover the same ground so here they will be referred to as the four Ts:

Tolerate: Retaining the risk where the cost of treatment is higher than the impact of the risk.

Treat: Making changes to reduce the probability of a vulnerability being exploited and/or putting in place a system of procedures to deal with the consequences if it is.

Transfer: Transfer the risk by making changes to contractual arrangements e.g. getting a different company to undertake the work that incurs the risk (such as insurance).

Terminate: Ceasing the activity responsible for the vulnerability thus removing the risk.

Each risk will be assigned a risk treatment. A risk which falls into the acceptable zone will automatically be assigned the tolerate treatment.

9.3. Risk register

Once a risk has been identified, scored and assigned a risk treatment it will then be presented to the Risk Management Group for approval. Once signed-off it will be entered onto the Risk Register.

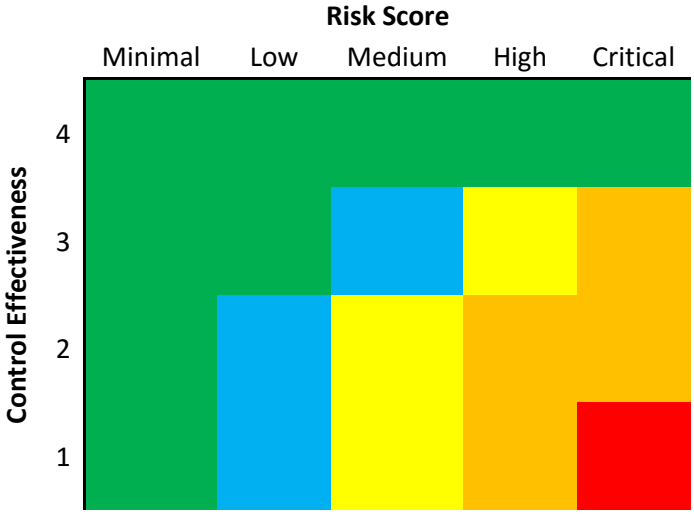
Where a disagreement over a risk occurs this will be discussed and, where possible, resolved within the Risk Management Group. If necessary it will go back to the relevant risk owner for further evaluation before being resubmitted.

9.4. Residual risk

When a control has been applied to a risk as part of a risk treatment its effectiveness must be measured to generate a residual risk score, this will allow Fourth to see whether further work is necessary to mitigate the risk to an acceptable level.

Control effectiveness is measured as follows:

1. Ineffective
2. Partially effective
3. Mostly effective
4. Completely effective



Green: **Acceptable risk**
Tolerate the risk

Blue: **Low risk**
Treatment required

Yellow: **Medium risk**
Treatment required

Orange: **High risk**
Treatment required
Include in board report

Red: **Critical risk**
Treatment required
Risk Steering Committee to be informed immediately

Document History

Version	Date of Issue	Author	Changes
0.1	01/03/13	Paul Cocker	Initial draft.
0.2	12/03/13	Paul Cocker	Added policy principles and management statement.
0.3	22/03/13	Paul Cocker	Updates to management statement, expanded definitions and content reordered and improvements to document wording.
0.4	27/03/13	Paul Cocker	Linked policy to Fourth principle requirements and added our documentation framework.
0.5	28/03/13	Paul Cocker	Minor wording changes and sign-off of management statement.
0.6	03/04/13	Paul Cocker	Added wording around third parties to 7.5 along with other minor wording changes.
1.0	16/04/13	Paul Cocker	Approved for distribution.
1.1	04/07/13	Paul Cocker	Grammatical changes and classification changed to PUBLIC.
1.2	18/07/13	Paul Cocker	Wording changes to 7.4.3, formatting change to Purpose and corrected participant list of Risk Management Group
1.3	18/07/14	Paul Cocker	Revised risk management structure and updated relevant laws
1.4	15/03/16	Paul Cocker	Defined “process” and updated the membership of the Risk Steering Committee
1.5	27/09/17	Paul Cocker	Updated risk structure, committee membership, critical risk action and relevant legislation
1.6	13/12/17	Paul Cocker	Changed risk meeting schedule
1.7	01/03/18	Paul Cocker	Add GDPR to list of legislation