

Ref:	NR/L2/RSK/001
Issue:	1
Date:	05 March 2016
Compliance date:	04 June 2016

Level 2

Business Process

Enterprise Risk Management

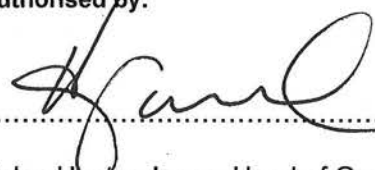
Endorsement and Authorisation

Endorsed by:



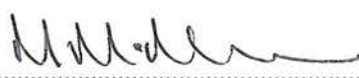
Dean Harrison, Working Group Chair

Authorised by:



Helen Hunter-Jones, Head of Group Risk

Accepted for issue by:



Mick McManus, National Standards Manager

This document is the property of Network Rail. It shall not be reproduced in whole or part nor disclosed to a third party without the written permission of Network Rail.
© Copyright 2016 Network Rail.

Uncontrolled copy once printed from its electronic source.

Published and Issued by Network Rail, 2nd Floor, One Eversholt Street, London, NW1 2DN.

Ref:	NR/L2/RSK/001
Issue:	1
Date:	05 March 2016
Compliance date:	04 June 2016

User information

This Network Rail document contains colour-coding according to the following Red–Amber–Green classification.

Red requirements - no variations permitted

- Red requirements are to be complied with and achieved at all times.
- Red requirements are presented in a red box.
- Red requirements are monitored for compliance.
- Non-compliances will be investigated and corrective actions enforced.

Amber requirements - variations permitted subject to approved risk analysis and mitigation

- Amber requirements are to be complied with unless an approved variation is in place.
- Amber requirements are presented with an amber sidebar.
- Amber requirements are monitored for compliance.
- Variations can only be approved through the national non-compliance process.
- Non-approved variations will be investigated and corrective actions enforced.

Green guidance - to be used unless alternative solutions are followed

- Guidance should be followed unless an alternative solution produces a better result.
- Guidance is presented with a dotted green sidebar.
- Guidance is not monitored for compliance.
- Alternative solutions should be documented to demonstrate effective control.

Amendment marks

- First document amendments are presented with a single black line to the right of the affected text.
- Second document amendments are presented with a double black line to the right of the affected text.

Ref:	NR/L2/RSK/001
Issue:	1
Date:	05 March 2016
Compliance date:	04 June 2016

Issue record

Issue	Date	Comments
01	March 2016	Update of NR/L2/RSK/000001

Compliance

This Network Rail standard is mandatory and shall be complied with by Network Rail and its contractors if applicable from 4th June 2016.

Reference documentation

Network Rail Risk Policy	NR/L1/RSK/001
ISO 31000:2009	International Organisation for Standardisation
ERM Guidance: Enterprise Risk Record	Group Risk Connect Page
ERM Guidance: Risk Assessment Guidance	Group Risk Connect Page
ERM Guidance: Risk Appetite	Group Risk Connect Page
ERM Guidance: Risk Controls	Group Risk Connect Page
ERM Guidance: Early Warning Indicators	Group Risk Connect Page
Corporate Risk Assessment Guidance	Group Risk Connect Page
Business Assurance Committee TOR	Group Risk Connect Page

Disclaimer

In issuing this document for its stated purpose, Network Rail makes no warranties, express or implied, that compliance with all or any documents it issues is sufficient on its own to ensure safe systems of work or operation. Users are reminded of their own duties under health and safety legislation.

Supply

Copies of documents are available electronically, within Network Rail's organisation. Hard copies of this document may be available to Network Rail employees on request to the relevant controlled publication distributor. Other organisations may obtain copies of this from an approved distributor.

Ref:	NR/L2/RSK/001
Issue:	1
Date:	05 March 2016
Compliance date:	04 June 2016

Contents

1 Purpose	5
2 Scope	5
Figure 1 – Risk Hierarchy	5
3 Roles and their Key Accountabilities	6
4 Definitions	7
5 Risk Management Process	9
5.1 General	9
Figure 2 – ERM process diagram	9
5.2 Understanding context, objectives and value	9
5.3 Identification of risk	10
5.4 Approval of new risks	10
5.5 Risk analysis	10
Figure 3 – Bowtie methodology	11
5.6 Risk evaluation	12
Figure 4 – Control effectiveness ratings	13
5.7 Risk appetite	14
5.8 Management response	14
6 Risk governance	16
6.1 Initial sign off	16
6.2 Ongoing monitoring of risks	16
6.3 Early warning indicators	16
6.4 Reviewing and reporting	17
6.5 Changes to risk levels	18
7 Monitoring and Reporting Compliance	18
8 Continuous improvement	19

Ref:	NR/L2/RSK/001
Issue:	1
Date:	05 March 2016
Compliance date:	04 June 2016

1 Purpose

This standard sets out a principle based approach for the management of Enterprise Risks in Network Rail to enable:

- the effective and consistent management of all risks to strategic objectives;
- risks to be managed in accordance with the Risk Management Policy and Board approved corporate risk appetite statements;
- the identification, prioritisation and management of interrelated risks to support successful delivery of the Company's strategic objectives; and
- strategic objectives to be managed in accordance with the UK Corporate Governance Code and governance requirements under licence condition 15 of the Network Licence.

2 Scope

This standard applies to all parts of the business that own and / or manage Level 0 to Level 2 enterprise risks as shown in Figure 1.

The risk management principles detailed in this standard may also be applied to risks at L3, L4 and L5.

NOTE: In these areas further standards or specialist risk management tools and techniques might be more suitable to the management of specific business risks.

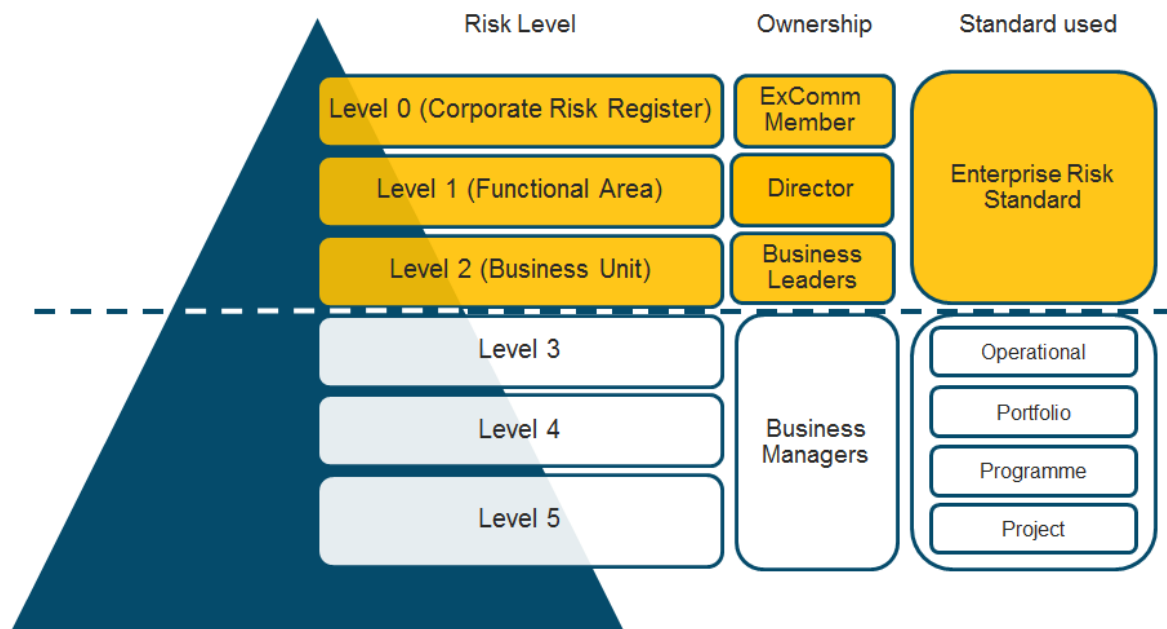


Figure 1 – Risk Hierarchy

Ref:	NR/L2/RSK/001
Issue:	1
Date:	05 March 2016
Compliance date:	04 June 2016

3 Roles and their Key Accountabilities

	Role	Key Accountabilities
Risk Governance	Accounting Officer	Overall accountability to the Network Rail Board and the Department for Transport for the oversight and management of risk at Network Rail.
	Audit and Risk Committee Members	a) Oversee and challenge the effectiveness of risk management activities of Network Rail; b) Review Network Rail's risk profile on behalf of the Network Rail Board.
	Executive Committee Members	a) Define the organisations strategic objectives; b) Act as a risk committee to provide challenge and assurance of risk management in accordance with the Company's risk appetite; c) Provide management assurance to Audit and Risk Committee on the management of risk in Network Rail.
	Business Assurance Committee Members	a) Act as a risk committee to provide challenge and assurance of risk management activities within business functions; b) Be responsible for approving the escalation / de-escalation of a function's risks.
Risk Management	Risk Owners	a) Be accountable for the management of the risk and risk response; b) Approve changes to the Enterprise Risk Record prior to reporting; c) Assign a Enterprise Risk Manager to risks within their accountability.
	Enterprise Risk Managers	a) Be responsible for the management of the risk and risk response; b) Manage the implementation of the risk response, including checking all control owners and action owners are aware of their responsibilities; c) Engage with all parts of the business that are either contributing to the management of a risk or could potentially be affected by a risk if it were to materialise; d) Be responsible for the recording of risk data to Enterprise Risk Records or designated risk management system.
	Risk Co-ordinators	a) Support their Executive Directors, Senior Leaders and Enterprise Risk Managers in the assessment and management of risks to the Company's strategic objectives; b) Act as a focal point for the co-ordination of risk activities with the Group Risk team; c) Be a local expert in Network Rail's ERM framework; d) Support their Executive Directors, Senior Leaders and Enterprise Risk Managers in the collation and monitoring of risk information.

Ref:	NR/L2/RSK/001
Issue:	1
Date:	05 March 2016
Compliance date:	04 June 2016

	Role	Key Accountabilities
Specialist Risk Support	Group Risk Team	a) Own and operate Network Rail's ERM Framework; b) Monitor compliance to the ERM Standard; c) Resolve disputes over risk ownership; d) Provide ERM training and awareness; e) Provide technology solutions for the recording, maintaining, escalating and reporting of risk; f) Report strategic risks to the Board and its Committees; g) Co-ordinate assurance to the Board and its Committees that risks to strategic objectives are being assessed and managed.

4 Definitions

Term	Definition
Action owner	Individual with accountability for completing a risk improvement activity or action plan
Business Assurance Committee (BAC)	Forum within which risk and assurance information is discussed as part of overall performance governance and monitoring
Business objective	Targets/goals that are aligned to Network Rail corporate strategy
Cause	Factual background conditions that give rise to uncertain risk events
Control	Recognised activity within a process or system that is designed to prevent a risk event from occurring or mitigate the potential impact should it occur: - Preventative controls – Designed to prevent a risk event from occurring; - Mitigating controls – Designed to mitigate the potential impact should a risk event occur Reward to recognised activity within a process or system
Control rating	A measure of the effectiveness of controls. Control ratings apply to two key areas in relation to Enterprise Risk: - Overall control rating of the risk, taking into account the framework of controls in place (all controls) - Specific control rating looking at how effectively an individual control is operating
Enterprise Risk	A risk which could impact the achievement of objectives e.g. at a company or functional level, and that is enterprise wide in either in its impact or management.
Enterprise Risk Record (ERR)	Tool used to manage record and report enterprise level risks