NATIONAL EXAMINING BOARD FOR DENTAL NURSES

Risk Management Policy

Policy	Risk Management Policy
Effective Date	October 2014
Date Last Reviewed	*New policy yet to be reviewed*
Scheduled Review Date	October 2015
Supersedes	All previous Risk Registers
Original Author	Phil Hughes
Owned by	Board of Trustees
Monitored by	Governance Committee
Approved by	Board of Trustees on 16 October 2014

Purpose

The purpose of this risk management policy is to:

a. set out the framework on which risk management processes at NEBDN are based;
b. clearly identify roles and responsibilities for managing risk;
c. ensure a consistent, corporate approach is adopted across NEBDN to facilitate the prioritisation of risks and avoid duplication of mitigating action;
d. ensure risk management principles are embedded in all systems and processes;
e. ensure actions are proportionate to identified risks and hence resource use is efficient and effective and achieves a balance between risks and controls.

Scope

The management of risk is the responsibility of everyone who works for the organisation consistent with this policy and the priorities set annually by the Board in the annual risk register.

Policy statement

NEBDN will proactively manage risk in order to be able to continue to provide high quality services to dental nurses, their employers and training providers and through this contribute to providing high quality dental services to the public and patients.

NEBDN has a cautious attitude to risk (ie its preference is for safe options that have a low degree of inherent risk).

Definitions

Risk is defined as an uncertainty of outcome - positive or negative - of actions and events. Risks are assessed by considering the likelihood of something happening and the impact that would arise if it did happen.

Risk Management is the process, by which risks are identified, evaluated and controlled ie:

a. Tolerate the risk - The exposure may be tolerable without any further action being taken. Even if it is not tolerable, ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. In these cases the response may be to tolerate the existing level of risk.

b. Treat the risk - The purpose of treatment is that whilst continuing with the activity giving rise to the risk, action (control) is taken to constrain the risk to an acceptable level. The option to treat can be further analysed into
   - Preventative Controls eg Segregation of duties, Codes of conduct, staff policies.
   - Corrective Controls eg Contingency planning, termination terms in contracts
   - Directive Controls eg ensuring adequate Health and Safety training before being allowed to carry out some activities
   - Detective Controls – eg stock and asset checks

c. Transfer the risk - For some risks the best response may be to transfer them. This might be done by conventional insurance, or by paying a third party to take the risk in another way. This option is particularly good for mitigating financial risks or risks to assets. The transfer of risks may be considered to reduce the exposure of the organisation.

d. Terminate the risk - Do not pursue or continue the course of action, the risk is unacceptable and cannot be economically mitigated to an acceptable level.

e. Internal Control: All measures taken by management to ensure the organisation's objectives are achieved with the optimum use of resources taking into account risks to the organisation.

Risk appetite is the level of exposure which is considered tolerable and justifiable should the risk be realised. In this sense it is about comparing the cost (financial or otherwise) of constraining the risk with the cost of the exposure should the exposure become a reality and finding an acceptable balance.

The risks facing the organisation can be split into strategic and operational risks:

Strategic risks are those which may threaten the achievement of NEBDN's objectives.

Operational risks are those which managers, staff and volunteers may encounter in the daily course of their work.

Responsibilities

The Board of Trustees holds ultimate responsibility for the risk register and ensuring that risks are minimised to meet strategic objectives. The Board must have sufficient grasp of the risks and how they are managed to report with confidence on risk management in its annual report.

The Board of Trustees has delegated the management of the risk policy to the Governance Committee. The responsibilities of the Governance Committee are to:

1. identify and present risks to the Board of Trustees
2. ensure that the risk management strategy is up-to-date and in place
3. continually monitor and review risks
4. ensure that risk management procedures are satisfactorily carried out
5. consider progress on the action plan against the risks identified
6. report to the Board at each meeting on any significant changes and the implications for the risk register, by assessing the description and nature of any new risks and identify an initial risk score for recommendation to the Board
7. review the full risk register annually and report to the Board for its decision.

The Chief Executive (CEO) is responsible for:

1. maintaining the risk register
2. ensuring all staff and volunteers are aware of risk
3. considering the implications of any changes to service delivery or workloads in respect of risk
4. ensuring that identified risks are included in the risk register
5. undertaking the initial risk scoring risk.

Specific actions related to risk will be assigned to a lead owner. The responsibility of the owner is to update the CEO regularly on progress so that the CEO in turn can report to the Governance Committee and the Board.

References

All NEBDN policies and procedures should take into account the management of risk and be consistent with the aims and objectives of this policy.

Questions

If you have any questions about this policy, please email NEBDN at info@nebdn.org and your enquiry will be directed to the appropriate member of staff.

Procedure

In line with best practice, the NEBDN has adopted a seven-step process to support the implementation of risk management as set out below.

1. Identifying risk - Risks will be identified and cross-referenced, where possible to the achievement of strategic objectives.

2. Analysing risk – the CEO will initially assess the probability and impact of the identified risks, the Governance Committee will validate or change the score upon review and subsequently report to the Board for agreement.

3. Profiling risk - The evaluation exercise will result in a risk score made up by multiplying the impact score with the probability score from which significant risks can be recognised.

4. Prioritising action - The risk register will contain both operational and strategic risks and actions to be taken to mitigate the risk, where possible. In some cases these is an inherent risk, which the Board may feel can be tolerated. Any risk scoring more than 15 will be considered to be a Primary Risk and be included in the Risk Register taken to the Board on a regular basis.

5. Determining action - Further actions required to reduce the threat of the risk occurring or minimise its impact will be stated in the risk register. Target dates and assignment of responsibility will also be stated.

6. Controlling risk - The specified actions will be assigned an owner and carried out as stated in the risk register.

7. Monitoring – the CEO and the Governance Committee will keep the risk register under review and progress against the action plan will be reported quarterly to the Board. The register will be updated as actions are achieved and risk scores amended as appropriate. The identification of risks should be a continual process and risks emerging throughout the year should be evaluated and, where necessary, added to the register.

The *risk score* is calculated by multiplying the Likelihood score by the Impact score. Any risks which score above 15 are considered to be Primary Risks and will be reported to the Board at each meeting.

Likelihood takes into account the indicators set out below:

Score	Likelihood	Indicators
1	Improbable	• Has not occurred before • Has not occurred at other awarding bodies • Extremely unlikely to occur (less than 10% chance)
2	Remote	• Remote risk but could happen within next 3 to 10 years • Has not occurred at NEBDN but isolated cases have occurred at other awarding bodies
3	Possible	• Could happen at least once every 1 to 3 years • New circumstances with little data to indicate likelihood of • occurrence • 50 / 50 chance of it happening
4	Probable	• More likely to happen than not • Could occur within next 3 – 12 months • Has occurred in the last five years • Has occurred at some other healthcare awarding body
5	Almost certain	• Has occurred in the last two years • Has occurred at many other awarding bodies • More than an 80% chance of it happening • Likely to happen within next three months or is occurring at present

The matrix used to determine the impact score is as follows:

Score	Impact	Indicators
1	Insignificant	• No impact on achievement of service objectives/delivery • No impact on delivery of project – slight slippage or reduction in quality/scope with no overall impact • Negligible financial impact • No legal/regulatory impact – no sanction or legal action likely • No damage to reputation or will not result in adverse media comment
2	Minor	• Moderate impact on service objectives/delivery - only partially achievable without additional time / resources • Moderate impact on project – slight slippage against targets • Some legal/regulatory impact – complaint possible • No damage to reputation or standing • Financial impact can be contained within budget
3	Moderate	• Service objectives/delivery not achievable without additional time / resources • Moderate affect on project timetable - elements of scope or functionality may not be available • Probable legal/regulatory impact leading to reprimand, sanctions or legal action – avoidable with careful planning • Some public embarrassment leading to limited reputational damage – short term impact • Financial impact cannot be contained within budget and needs additional resourcing.
4	Major	• Significant impact on achievement of service objectives/delivery even with additional resources • Failure to meet key project deadlines or project fails to meet needs of proportion of stakeholders • Serious legal/regulatory impact leading to sanctions or legal action with significant consequences • Loss of credibility and public confidence in the service / Board (of interest to the national press)
5	Disastrous	• Unable to achieve corporate objective or prolonged closure/withdrawal of service • Major project's viability jeopardised through delay or level of quality makes it effectively unusable • Major legal/regulatory impact leading to sanctions or legal action with substantial financial or other consequences • Highly damaging to reputation with immediate loss of beneficiary confidence • Severe financial impact based on current financial status

Risk strategy for NEBDN

The risks that have been relevant to NEBDN are shown in the table below:

STRATEGIC	OPERATIONAL
Political Failure to deliver on key objectives *Economic* The Board's ability to meet its financial commitments The competitiveness of the service/ the ability to deliver best value. *Social* The effects in changes in demographic or socio-economic trends on the organisation's ability to deliver its objectives *Technological* The Board's capacity to deal with technological change or its ability to use technology to meet changing demands *Legislative* Current or potential changes in national or European law Changes to the regulatory environment - education, healthcare, professional regulation *Environmental* The environmental consequences of service delivery (in terms of energy efficiency, pollution, re-cycling, landfill needs, emissions etc) *Competitive* Failure to recognise the changing needs and expectations of the registrants and the public.	*Professional* Competences of staff and volunteers Volunteer willingness and ability to commit time and other resources to the organisation *Financial* Financial planning and control and the adequacy of insurance cover *Legal* Possible breaches of legislation / regulation *Physical* Fire, security, accident prevention and health & safety *Contractual* The failure of contractors to deliver services or goods to agreed costs and specifications *Technological* Reliance on operational equipment (IT systems or equipment and machinery) *Environmental* Pollution, noise or energy efficiency of ongoing service operation.