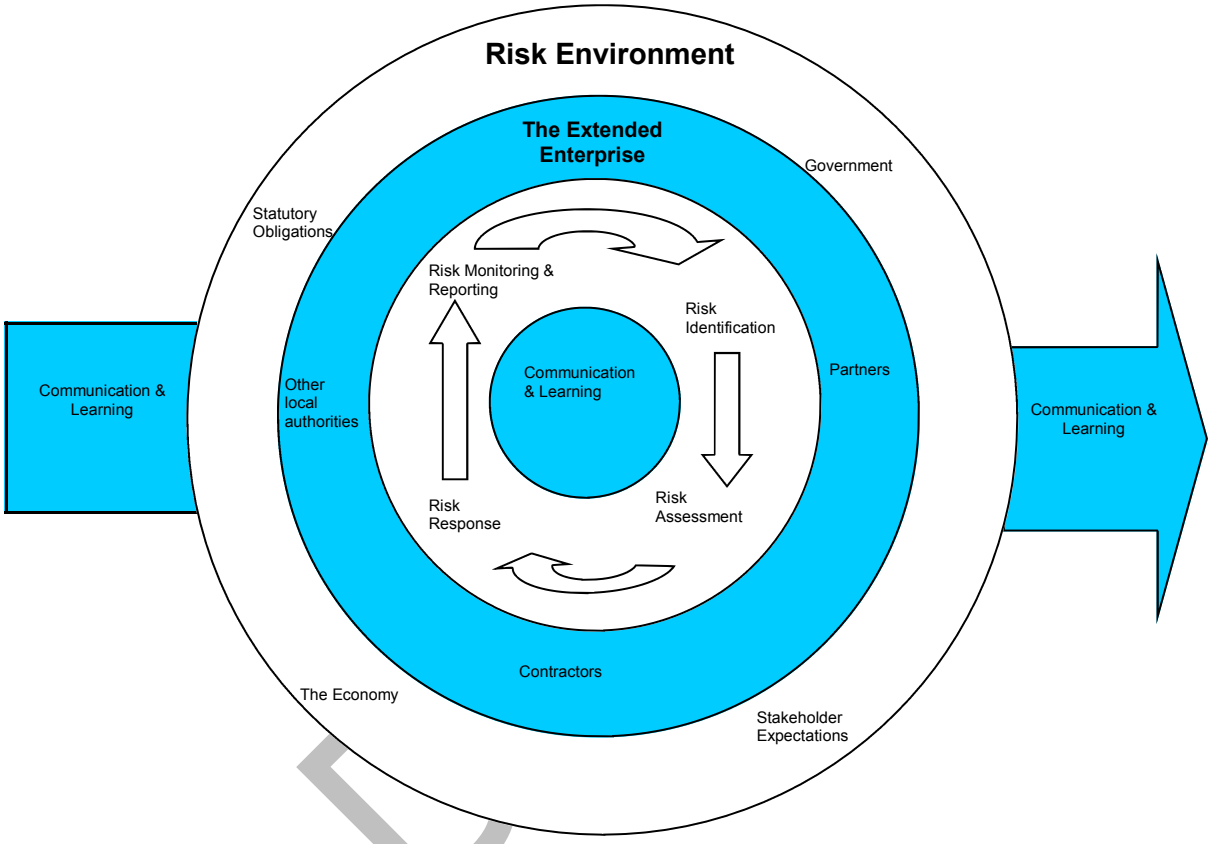
Appendix B - Risk Management Process

1.0 The risk management process

1.1 The process used will incorporate the following steps:
a. Identification of the risk
b. Assessment of the risk
c. Address the risk – the risk control mechanism
d. Assignment of risk ownership
e. Reviewing and reporting the risk
f. Providing assurance



2. Identification of the risk

2.1 There is no single solution to identify risks. Here are some examples:-

a. Where risk management is becoming established, e.g. corporate risks, existing risks are reviewed quarterly and amended according to changes in the corporate plan priorities.
b. Other risks, e.g. when considering new activities, risks may be identified by comparison against the categories listed in appendix C.
c. Business continuity will be identified by events that can be foreseen which prevent service delivery, based around Lincolnshire's community risk register and internal business risks.
d. Health and safety risks are usually, but not exclusively, identified by trained health & safety assessors within the authority.

3.0 Assessment of risk

3.1 Risk is assessed by the combination of two factors, the likelihood of something happening and the impact if it does happen. This can be represented graphically on a simple 4 x 4 matrix as shown below.

IMPACT

CRITICAL	4	4	8	12	16
MAJOR	3	3	6	9	12
MINOR	2	2	4	6	8
NEGLIGIBLE	1	1	2	3	4
		1	2	3	4
		ALMOST NEVER	UNLIKELY	LIKELY	ALMOST CERTAIN

LIKELIHOOD

3.2 As an alternative the authority could adopt a 5 x 5 matrix for a more sophisticated assessment.

- Impact – insignificant / minor / moderate / major / catastrophic
- Likelihood – rare / unlikely / possible / likely / almost certain

3.3 Definition of risk level

KEY		
9-16	High	Unacceptable level of risk exposure which requires extensive management
4-8	Medium	Risk management measures need to be put in place and monitored
1-3	Low	Acceptable level of risk subject to regular monitoring

- High Risk
  These risks will have an extreme effect on the operation of the business or its service delivery, resulting in significant financial loss, major service disruption or significant impact on the pubic e.g. major system failure, major flood or fire. These risks require immediate comprehensive action with senior management involvement,

- Medium Risk
  Managed by specific monitoring or response procedures. These risks will have a noticeable effect on service provision, causing a degree of disruption and impinging on budgets e.g. fraud/theft, system failure or fire. Consequences of the risk materialising would be severe but not extreme. Some immediate action is required and the development of an action plan.

- Low Risk
  The consequences of these risks are not severe and they will be managed using routine monitoring procedures, unlikely you need specific or significant application of resources. Individually such risks will have a negligible effect on service provision and any associated loss is relatively small, but if left untreated these risks could have a more significant cumulative effect e.g. missed deadlines, minor incidents or service disruption.

4.0 Addressing the risk

4.1 There are three key stages to be taken when addressing a risk, they are:

a. Decide how you are going to deal with the risk (see 5.1 for definition)
b. If necessary what action is going to be taken to treat or control the risk (see 5.2 for definition)
c. Identify the person responsible for controlling the risk (see 5.3 for definition)

5.0 Deal with the risk

5.1 There are five courses of action for dealing with the risk:-

a. Tolerate the risk and take no further action
b. Treat the risk. This is the most used option (see below for ways to treat risk)
c. Transfer the risk by taking out insurance or involving a third party
d. Terminate the risk by stopping doing what is causing the risk
e. Take the opportunity. This encourages thoughts about additional opportunities that may arise if you decide to tolerate, treat or transfer the risk.

5.2 Treat/Control the risk

a. If you decide to treat the risk a control mechanism must be put in place. You should consider four types of control:-

- Preventative controls – Designed to limit the possibility of something undesirable happening e.g. separation of duties in a financial system to reduce the risk of fraud occurring
- Corrective controls – Designed to limit the damage/impact should the risk arise e.g. effective contingency planning
- Directive controls – Designed to ensure a particular outcome is achieved e.g. insistence that workers wear protective clothing to help reduce the likelihood of harm
- Detective controls – designed to identify an undesirable outcome that has arisen e.g. stock takes alert to the fact theft has possibly taken place

5.3 Identify the owner

The owner of the risk should be the person who is best placed to inform and monitor the risk. Delegation for monitoring the risk and any associated /resulting actions may be undertaken however, overall responsibility for the risk remains with the risk owner. All risks must have an owner to ensure they are controlled effectively.

6.0 Monitor and review

6.1 Risks need to be reviewed and reported upon

a. To identify if risks are changing
b. To gain assurance that risk management is effective.

7.0 Assurance

7.1 Assurance will be provided that the Council's approach to risk management is working by:

a. Setting up systems which include the reporting of :
   - risks identified
   - risk owners
   - risk treatment
   - reporting mechanism

b. Review of the risk management system by:
   - Governance and Audit Committee
   - Internal audit
   - Risk Management Group
   - External audit