RISK MATRIX

			LIKELIHOOD				
			Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
		(description)	May only occur in exceptional circumstances	Could occur at some time	Might occur at some time	Will probably occur in most circumstances	Is expected to occur in most circumstances
CONSEQUENCE	**Severe**	Critical failure(s) preventing core	**HIGH**	**VERY HIGH**	**VERY HIGH**	**EXTREME**	**EXTREME**
	Major	Breakdown of key activities leading to	**HIGH**	**HIGH**	**VERY HIGH**	**VERY HIGH**	**EXTREME**
	Moderate	Impact on the organisation resulting	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**	**VERY HIGH**
	Minor	Some impact on business areas in terms	**VERY LOW**	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**
	Insignificant	Minimal impact on non-core business	**VERY LOW**	**VERY LOW**	**LOW**	**MEDIUM**	**MEDIUM**

Context - Asset(s) that we are trying to protect

The organisation uses Microsoft Active Server with Microsoft SQL server 2000 database. Asset that needs to be protected includes personal identifiable information, financial information and tax.

Risk					Inherent Risk Rating			Current Risk Rating					Target Risk Rating				
ID	Title	Description	Sources or Causes of Risk	Consequences of Risk	Likelihood	Consequence	Risk Level	Existing control measures	Effectiveness of exisitng control measures	Likelihood	Consequence	Risk Level	Additional control measures	Effectiveness of additional control measures	Likelihood	Consequence	Risk Level
R01	Staff	Full time and Part-time	Hackers	Data can easily be stolen	Likely	Major	VERY HIGH	None	**Weak**	Likely	Major	VERY HIGH	**Treat - Staff should be well trained on security measures**	**Excellent - Training staff adds a layer of protection against attach**	Unlikely	Minor	LOW
R02	User System Password	Passwords used for web applications are weak. Attacked can easily guess the password to gain access to the system	Computer Criminals	Access to organisation system by attackers	Possible	Moderate	**MEDIUM**	Password must be 5 characters long	**Moderate**	Possible	Moderate	**MEDIUM**	**Treat - Password should not be less than 8 characters long and should include uppercase, lowercase, special characters and numeric**	**Excellent - This measure will be a bit difficult for attackers to guess the password**	Possible	Moderate	**MEDIUM**
R03	Disaster Recovery plan	No procedure to ensure the ongoing of operation in an event of business disruption	Environment	Business disruption	Possible	Severe	VERY HIGH	Weak backup plan	**Weak**	Possible	Severe	VERY HIGH	**Treat - Develop and test a disater recovery plan**	**Excellent - This will help make sure that there is business continuity**	Possible	Severe	VERY HIGH