5 Oversight

Rate the following areas from 0 to 10 in terms of the extent to which they are understood and assessed as part of the risk management process.

Item	*Rate*
Oversight defines, updates, and maintains a list of duties to protect.	
Laws and regulations are reviewed to help define the legally mandated duties to protect associated with jurisdictions.	
All laws of all jurisdictions in which an enterprise operates have are considered in order to make prudent determinations as to duty to protect.	
The owners play an active role in defining the duties to protect.	
Owners assure their investment is not lost by electing proper boards of directors.	
For public companies regulatory requirements are scrupulously met.	
The board of directors takes their legal and moral responsible to assure that the CEO and other officers are doing their jobs seriously.	
The board of directors define additional duties to protect things like employee privacy in keeping with their responsibilities.	
The board actively oversees information protection issues on behalf of the shareholders to assure that shareholder value is protected.	
Auditors effectively provide independent and objective feedback to the shareholders, board of directors, CEO, and others on the effectiveness of the protection program.	
Auditors effectively provide evidence to demonstrate the risk management decisions are effectively carried out.	
The CEO effectively defines and assures that duties to protect are in place and fulfilled.	
The CEO actively participates in risk management activities on a regular basis.	
The CEO helps to identity business consequences associated with the business model, understands that model, and makes reasonable and prudent risk management decisions by applying that model.	
The CEO measures the performance of the duties to protect and assures the the CISO has adequate power and influence to operate the protection program effectively.	
The CEO keeps costs as low as possible without undertaking inappropriate levels of risk.	
TOTAL (sum the ratings and divide by 16)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
3	8	5	8	10

5.1 Duty to protect

5.1.1 Externally imposed duties

Rate the following areas from 0 to 10 in terms of the extent to which they are understood and assessed as part of the risk management process.

Item	*Rate*
Legal and regulatory mandates are derived from laws, regulations, protective orders, judicial determinations, and ordinances at all jurisdictional levels.	
Legal mandates associated with all businesses in jurisdictions are considered.	
Legal mandates involving special duties like public health and safety duties of drug or chemical manufacturers are considered.	
Legal mandates associated with fiduciary duties to shareholders by officers are considered.	
TOTAL (sum the ratings and divide by 4)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
5	10	5	10	10

5.1.2 Internally imposed duties

Rate the following areas from 0 to 10 in terms of the extent to which they are understood and assessed as part of the risk management process.

Item	*Rate*
The enterprise has decided to protect private information.	
The enterprise has decided to protect safety of workers by protecting their information.	
The enterprise has decided to protect against the release of information to third parties.	
The enterprise has decided to protect other similar information or assets beyond the levels imposed by government.	
Self-defined duties are protected at the same level of diligence as externally mandated duties.	
TOTAL (sum the ratings and divide by 5)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
n/a	2	n/a	n/a	n/a

5.1.3 Contractual duties

Rate the following areas from 0 to 10 in terms of the extent to which they are understood and assessed as part of the risk management process.

Item	*Rate*
Contractual obligations are defined in duties to protect and contracts reflect the binding nature of these obligations.	
Safe harbor agreements are reflected in identified duties to protect.	
Confidentiality and non-disclosure agreements are reflected in identified duties to protect.	
Trade secret agreements are reflected in identified duties to protect.	
Licensing agreements for patented or copyrighted material are reflected in identified duties to protect.	
All legal agreements include terms and conditions that reflect the ability of the enterprise to meet duties to protect and are reflected in the identified duties to protect.	
TOTAL (sum the ratings and divide by 6)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0	10	5	8	10