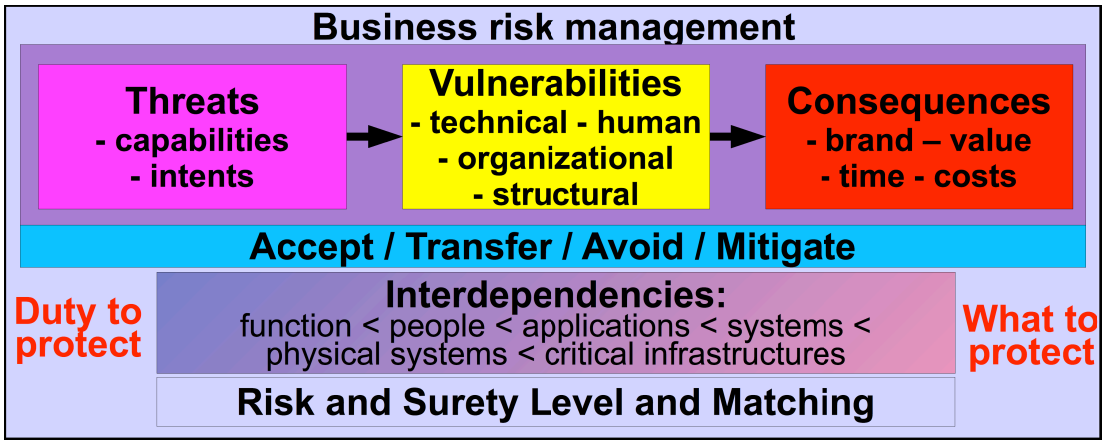
6 Business risk management



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*
Risk management is a formally defined business function within the enterprise with the CEO directly involved.	
Risk management transforms duty to protect into what to protect and how well to protect it.	
Risk management selects between risk acceptance, transfer, avoidance, and mitigation.	
For risk mitigation, risk management attempts to match surety of mitigation with desired risk reduction.	
TOTAL (sum the ratings and divide by 4)	

6.1 Risk evaluation

Item	*Rate*
Risks are systematically identified and evaluated based on the business model.	
Risk evaluation identifies event sequences with potentially serious negative consequences based on the business model.	
TOTAL (sum the ratings and divide by 2)	

6.1.1 Consequences

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*
Consequences are identified from the business model and rated, into low, medium, and high levels or into other levels based on a management-defined scheme.	
The scheme differentiates consequences typical of business risks like slip and fall accidents and similar readily insurable things from public relations problems, loss of substantial amounts of trust or money, inability to perform on select important contracts, and so forth from consequences that involve loss of life, great harm to the environment, collapse of the business, and/or jail time to executives.	
Consequences are identified in terms of brand or reputation.	
Consequences are identified in terms of value, which codifies a variety of financial implications ranging from loss of cash to destruction of stock to loss of information value for periods of time	
Consequences are identified in terms of time which is lost due to people not being as effective at their jobs or the business losing opportunities.	
Consequences are identified in terms of the direct costs associated with dealing with the incident and its aftermath.	
Consequences are identified and categorized based on the assumption that business processes fail regardless of any mitigating factors that may be in place.	
TOTAL (sum the ratings and divide by 7)	

6.1.2 Threats

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*
For event sequences involving medium or high consequences, threats are assessed with increasing attention and detail for higher consequences.	
As threats are identified, their capabilities and intents are taken into consideration in assessing their ability to cause consequences.	
Capabilities considered include but are not limited to funding, location, attack mechanisms available, group size, available resources, skill sets, training levels, allies, and access.	
Intents are assessed in light of group history, motives, group behaviors, group rewards, typical targets, leadership, and declared objectives.	
TOTAL (sum the ratings and divide by 4)	

6.1.3 Vulnerabilities

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*
For systems with identified high or medium consequences and whose threats have been assessed as having the capabilities and intents to induce those consequences, vulnerability analysis and mitigation is considered.	
Vulnerability assessment includes technical vulnerabilities most commonly associated with computer security.	
Vulnerability assessment includes human vulnerabilities that are covered under a variety of topic areas in the psychological literature.	
Vulnerability assessment includes structural vulnerabilities that have to do with overall network and infrastructure architecture and dependencies.	
Vulnerability assessment includes organizational vulnerabilities that have to do with weaknesses in the way things are organized and how people interact with each other within the structure.	
Vulnerability assessment identifies event sequences that permit identified threats to invoke sequences of vulnerabilities that they have identified capabilities to invoke in order to induce identified medium or high consequences that they have intents to induce.	
TOTAL (sum the ratings and divide by 6)	

6.1.4 Interdependencies and risk aggregation

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*
Interdependency analysis is undertaken for all identified medium and high consequences.	
Interdependency analysis considered the implementation of information systems over vast distances and the short time frames associated with the transfer of information over those distances.	
Interdependency analysis considers dependency on people.	
Interdependency analysis considers dependency on users.	
Interdependency analysis considers dependency on administrators.	
Interdependency analysis considers dependency on support personnel.	
Interdependency analysis considers dependency on the ability of these people to breath, perform their work, drink, eat, sleep, and live their lives.	
Interdependency analysis considers dependency on application programs.	

Item	Rate
Interdependency analysis considers dependency on data files.	
Interdependency analysis considers dependency on input and output systems.	
Interdependency analysis considers dependency on operating systems.	
Interdependency analysis considers dependency on libraries.	
Interdependency analysis considers dependency on configurations.	
Interdependency analysis considers dependency on domain name services.	
Interdependency analysis considers dependency on identity management systems.	
Interdependency analysis considers dependency on back-end processing facilities.	
Interdependency analysis considers dependency on protocols that are used to communicate with external capabilities.	
Interdependency analysis considers dependency on computing platforms.	
Interdependency analysis considers dependency on networks.	
Interdependency analysis considers dependency on wires.	
Interdependency analysis considers dependency on routing protocols.	
Interdependency analysis considers dependency on accessibility.	
Interdependency analysis considers dependency on power.	
Interdependency analysis considers dependency on cooling.	
Interdependency analysis considers dependency on heat.	
Interdependency analysis considers dependency on air.	
Interdependency analysis considers dependency on communications.	
Interdependency analysis considers dependency on political stability.	
Interdependency analysis considers dependency on environmental conditions and controls.	
Interdependency analysis considers dependency on supplies.	
Interdependency analysis considers dependency on the safety and health of workers, customers, vendors, partners, and their families.	

Item	Rate
Risk aggregation through interdependencies is considered in risk management.	
Risk aggregation is revisited whenever changes are made to systems that interact with other systems.	

TOTAL (sum the ratings and divide by 33)

6.1.4.1 Single points of failure

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
All single points of failure for medium or high consequence situations are identified as part of risk management.	
Except as approved on a case by case basis by the CEO, no single points of failure are permitted to exist for medium or high consequences situations.	
Except as approved on a case by case basis by the CEO, no key individual can be allowed to exist without whom medium or high consequences will occur.	
Except as approved on a case by case basis by the CEO, no single facility can be permitted to act as a single point of failure for medium or high consequences.	
High consequence single points of failure risk acceptance is reviewed by the CEO at least once every 6 months.	
Medium consequence single points of failure risk acceptance is reviewed by the CEO at least once every year.	
TOTAL (sum the ratings and divide by 4)	

6.1.4.2 Radius-driven common mode failures

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
Except as approved on a case by case basis by the CEO, within a radius of effect associated with the attack mechanisms within the capabilities of the threats identified in threat assessment, no single event is able to cause medium or high consequences.	
Natural effects within reasonably expected and historically supported radii are taken into account in risk management.	

Item	Rate
Redundant data centers in the same Earthquake zone or flood zone are not used to support the claim to have no single point of failure.	
Redundancy within a single building or location is not used to claim no single point of failure for a medium or high consequence situation.	
High consequence radius-based risk acceptance is reviewed by the CEO at least once every 6 months.	
Medium consequence radius-based risk acceptance is reviewed by the CEO at least once every year.	
TOTAL (sum the ratings and divide by 4)	

6.1.4.3 Other sorts of common mode failures

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
Common mode failures, i.e., failures modes resulting from commonalities between systems or components, with medium or high consequences are identified in risk analysis efforts.	
The CEO determines whether the cost of reducing or eliminating common mode failures with medium or high consequences is justified on a case by case basis.	
Common hardware, software, or operating systems are considered common mode failure candidates.	
Common protocols, power, gas, or supply chain dependencies are considered common mode failure candidates.	
High consequence common mode failure risk acceptance is reviewed by the CEO at least once every 6 months.	
Medium consequence common mode failure risk acceptance is reviewed by the CEO at least once every year.	
TOTAL (sum the ratings and divide by 6)	

6.1.4.4 Key individuals

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
Any single individual who controls a substantial enough portion of information or infrastructure to produce a medium or high risk from their action is identified as a key individual as part of risk management.	
The CEO must approve any key individual who exist for whom there is no backup at least once every six months and must explicitly accept the risks associated with this individual on a case by case basis.	

Item	Rate
But for any substantial enterprise a key individual without backup is not permitted to continue for more than one approval cycle by the CEO.	
All key individuals have had sufficient background checks to justify the high level of trust being placed in them.	
High consequence key individual risk acceptance is reviewed by the CEO at least once every 6 months.	
Medium consequence key individual risk acceptance is reviewed by the CEO at least once every year.	
Key individuals have privileges temporarily suspended on reasonable suspicion until such time as suspicion is settled and the issue resolved.	
Upon termination of key individuals special review is undertaken to assure that undue residual risks do not remain.	
Actions taken by key individuals are always audited and reviewed in detail at least twice per year.	
Relationships between key individuals are explicitly tracked to determine and mitigate potentials for defeating of dual controls and other collaborative attack potentials.	
TOTAL (sum the ratings and divide by 10)	

6.2 Risk treatment

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
Risks that are worthy of attention are managed and risks not worthy of consideration are accepted.	
A risk treatment plan is identified for all risks identified.	
TOTAL (sum the ratings and divide by 2)	

6.2.1 Risk acceptance

Item	Rate
For risks that are too low to bother protecting against or for which insurance and due diligence are adequate, risk is accepted.	
For risks that are to be mitigated but where mitigation cannot be done instantaneously or for which rapid mitigation is too expensive to justify, risks are accepted for periods during which mitigation is undertaken.	
TOTAL (sum the ratings and divide by 2)	

6.2.2 Risk avoidance

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
Risk avoidance is used as a business strategy for risks too high to justify the return on investment.	
Other similar avoidance strategies such as not opening offices in war zones or not doing business in certain localities are used.	
TOTAL (sum the ratings and divide by 2)	

6.2.3 Risk transfer

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
Risk transfer for low consequences is done via insurance where feasible.	
Risk transfer for medium and high consequences is only used in cases where the worst case loss is not sustainable and an adequate outside insurance capacity is willing to take on the risk.	
Contractual risk transfer is used when feasible but only identified as meaningful in risk reduction when the external party has deep enough pockets to justify trusting it for risk reduction associated with identified consequences it is intended to mitigate.	
Contractual risk transfer is used for medium risk or low risk when feasible but is not trusted for high consequence mitigation.	
TOTAL (sum the ratings and divide by 4)	

6.2.4 Risk mitigation

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
Risk mitigation is used to reduce residual risk to management identified acceptable levels.	
The CISO oversees mitigation efforts at an enterprise management level.	
Risk mitigations is prioritized by consequence with higher consequences having higher priority.	
Risk mitigation is designed to mitigate event sequences that can cause serious negative consequences.	
Risk mitigation of lower risk systems is undertaken primarily to meet perceived due diligence and digital community health and safety needs.	
Top management is directly involved in decisions to apply techniques to reduce threats.	
Public relations and corporate communications are directly involved in threat reduction efforts.	
Operations security is used to reduce the linkage between threats and vulnerabilities.	
Computer security is directly involved in the reduction of vulnerabilities to information systems.	

Item	Rate
Physical security is an active participant in vulnerability reduction.	
Design is used to reduce high and medium risks.	
Security architecture is used to reduce high and medium risks.	
Risk mitigation efforts are commensurate with risks.	
Higher surety mitigation methods are used for higher consequences.	
Residual risk remaining after mitigation is identified to top management and accepted, transfered, or further mitigated based on their guidance.	
Cost is considered in decisions to mitigate, transfer, or accept risk and residual risk and this information is provided to top management along with residual risk information.	
TOTAL (sum the ratings and divide by 16)	

6.3 What to protect and how well

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
Risk management produces decisions of what to protect and to what extent it should be protected.	
Executive security management (the CISO) is tasked with carrying out the duty to protect the things that should be protected to the extent appropriate to the need.	
The CISO has access to all information necessary to get this task done.	
The CISO has adequate influence and power to cause the duties to protect to be carried out across the enterprise.	
The CISO reports on progress against risk management objectives to the CEO and other responsible parties at least once per quarter.	
TOTAL (sum the ratings and divide by 5)	

6.3.1 The risk management space

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 risk management process starts in the middle of the risk picture with protection posture assessments to provide a medium-cost way to get a handle on the overall situation.	
The protection posture assessment process identifies low, medium, and high risk situations and additional work is done for higher risks.	
Risk levels lead to different management rates and complexity, change management mechanisms, and risk assessment techniques.	
For the low risk, due diligence approaches and vulnerability testing are considered adequate to the risk assessment process.	

Item	Rate
For medium risk situations sound change control and accreditation processes are invoked.	
For medium risk situations configurations are closely managed.	
For medium risk situations probabilistic risk analysis is not used except for natural threats.	
For medium risk situations covering approaches, protection posture assessments, and expert facilitated analysis are used as threats increase.	
For medium risk situations periodic oversight is acceptable at low threat levels, management must keep tighter reins and review at a higher rate for higher consequence systems.	
When risks reach into the high end, systemic change management comes into play with system-wide testing associated with every significant change.	
Management rates increase with risks.	
Scenario-based analysis and, at the highest risk levels, systems analysis are used.	
Surety is matched to risk.	
TOTAL (sum the ratings and divide by 13)	

6.4 Elements of the risk management process

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
Processes to be used in the overall risk management process are defined.	
Guidance on when to apply them is defined.	
There is a defined process for identifying the issues to be addressed in risk management.	
There is a defined process for determining when to use more in-depth processes.	
There is a defined process for deciding when to accept risks and not further pursue risk management.	
There is a defined process for determining how to treat medium risks and what to analyze.	
There is a defined process for determining how to identify consequences and how to differentiate them.	
There is a defined process for determining how and when to identify threats and how to analyze them.	

Item	*Rate*
There is a defined process for determining how and when to do vulnerability assessments.	
There is a defined process for making risk management choices and when to choose which of accept, avoid, transfer, and mitigate.	
There is a defined process for risk mitigation approaches for cases when mitigation is chosen.	
There is a defined process for mapping of policy elements into specific risk management mandates.	
There is a schedule for risk management.	
The schedule includes initial conditions required for risk management.	
The schedule includes management actions required for operation.	
The schedule includes when to do what activity.	
TOTAL (sum the ratings and divide by 16)	

Acceptable	Transferable	Reducible	Action
No	No	No	Do not engage in this—avoid the risk
No	No	Yes	Propose reduction and re-evaluate
No	Yes	No	Insure or avoid the risk
No	Yes	Yes	Balance reduction with insurance cost
Yes	No	No	Accept or avoid the risk
Yes	No	Yes	Balance reduction vs. acceptance cost
Yes	Yes	No	Accept or avoid the risk
Yes	Yes	Yes	Balance all three and optimize

	Low Consequence	Medium Consequence	High Consequence
Low Threat	Mid-level mgmt updates annually	6-month review cycle, top mgmt update annually	Should not occur – threats are higher
Medium Threat	Mid-level mgmt update 9-12 months	3-9-month review cycle, top mgmt update quarterly	Continuous top mgmt updates monthly
High Threat	Should not occur—not worth operating	3-6-month review cycle, top mgmt update quarterly	Continuous top mgmt updates monthly

6.4.1 Threat assessment

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
Pre-employment checks are part of employee threat assessment. Additional investigation and review is used for positions of higher trust.	
Case investigation is used in response to incidents.	
Detailed intelligence is undertaken against specific threats that are known to exist and that are targeting the company for high valued consequence.	
Regional intelligence is used when moving into a region or when operating in a region under substantial regional threat.	
Local intelligence is used whenever making determinations about placement of facilities, offices, routes, or housing, and when ranking locations for determining where to go and what to do there.	
Investigative intelligence is used for clearances associated with government jobs, for investigations of employees for high-level-of-trust jobs, and for verification of lifestyle conditions such as rapid changes in wealth.	
The table below reflects use of threat assessment techniques.	
TOTAL (sum the ratings and divide by 7)	

Assessment method	Consequence	Time	Threat	Cost
By type generic	Medium	Short	Medium	Low
By type, classes within groups	Medium-high	Medium	Medium-high	Medium
By type with classes and detailed high relevancy	Medium-high	Medium-long	Medium-high	High
Known vulnerability indications and warnings	Medium	Short	Low	Low
Detailed intelligence analysis	High	Long	High	High
Investigation-based	Medium-high	Medium	Medium-high	Medium-high

6.5 Fulfilling the duties to protect

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
At an enterprise level, a systematic approach is used to identify, codify, and fulfill duties to protect.	
The CISO is tasked with fulfilling the duty to protect and has adequate access to information and power and influence to fulfill those duties.	
A protection architecture is used to implement the duties to protect.	
Information assets are inventoried and controlled per the duty to protect.	
Inventory control is used to identify and associate duties to protect with information and information systems.	
Specific methods used to carry out duties to protect depend on the duties, the situation and the notion of "best practice" is not used as a decision tool.	
TOTAL (sum the ratings and divide by 6)	

6.6 Risk management roll-up

Area	*Rate*
Risk management	
Risk evaluation	
Consequences	
Threats	
Vulnerabilities	
Interdependencies and risk aggregation	
Single points of failure	
Radius-driven common mode failures	
Other common mode failures	
Key individuals	
Risk treatment	
Risk assessment	
Risk avoidance	
Risk transfer	
Risk mitigation	
What to protect and how well	
The risk management space	
0	
Threat assessment	
Fulfilling the duties to protect	
Total (sum the ratings and divide by 20)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1	7	4	8	9