Risk Assessment Criteria Definition Example 1

HealthTrackApp is a mobile app service that tracks subscribers' health information, sends the data to data analysts, and presents the analysis to subscribers as recommendations for healthier habits. They define their mission as measurably improving the health of their subscribers. Their objectives are to maintain profitability of at least 15%. And their obligations are to protect the confidentiality of their subscribers' data. As they define their impacts, they think through the levels of harm that they or others would accept and not accept. They define what would be high but recoverable, and they define what would be catastrophic to all parties.

IMPACT SCORING WORKSHEET – SOCIAL HEALTH APP

Impact Scores	Impacts Against Mission (The benefit we provide others)	Impacts Against Objectives (Our internal drivers)	Impact Against Obligations (Protecting against harm to others)
Definitions	*HealthTrackApp's purpose. The benefit HealthTrackApp brings to its subscribers* • *Measurably improved health*	*HealthTrackApp business goals. Strategic or tactical success metrics that HealthTrackApp intends to achieve.* • *Year-over-year profit of at least 15%*	*Responsibilities that HealthTrackApp has to subscribers* • *Protect the confidentiality of subscribers' health information.*
1. Negligible	Subscribers realize measurable, improved health within planned results.	Profitability is on plan.	No harm could result.
2. Low	Few subscribers may experience flat results	Profitability is within planned variance (14.5% or higher)	Some subscribers may be concerned.
3. Medium	Data Science department would show significant reduction in subscriber population's health results.	Profitability is off track and may require up to one year to recover.	Few subscribers may be embarrassed.
4. High	Data Science department would show majority of subscriber population's health results are not improved.	Profitability is off track and may require up to three years to recover.	Subscribers would be exploited beyond embarrassment.
5. Catastrophic	We would not be able to help users measurably improve health.	We would not be able to operate profitably.	Thousands or more subscribers would be exploited beyond embarrassment.

HealthTrackApp uses probability analysis to determine percentages of probability, so they define in plain language terms what bands of probability are associated with which likelihood scores.

LIKELIHOOD SCORING

Likelihood Score	Likelihood Definition
1	0%
2	<1%
3	<10%
4	<50%
5	<=100%

RISK ACCEPTANCE CRITERIA – BELOW '6'

Likelihood	1. Negligible	2. Low	3. Moderate	4. High	5. Catastrophic
1	1	2	3	4	5
2	2	4	**6**	8	10
3	3	**6**	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Risk Assessment Criteria Definition Example 2

Because Healthcare University Hospital cares for patients, educates clinical practitioners, and conducts clinical trials-based research, they list three missions. As a nonprofit, they operate to a 10-year strategic plan, they must maintain accreditations, and they must hire and retain leading talent to ensure that they achieve their mission. Finally, they must maintain both the confidentiality and integrity of data, and see those as primary concerns that can harm patients.

IMPACT SCORING WORKSHEET – HEALTHCARE UNIVERSITY HOSPITAL

Impact Scores	Impacts Against Mission (The benefit we provide others)	Impacts Against Objectives (Our internal drivers)	Impact Against Obligations (Protecting against harm to others)
Definitions	*HCU's purpose. The benefit HCU brings to students, faculty, patients, staff, and the public.* • *Patient Care* • *Education of students/professionals* • *Research*	*HCU's business goals. Strategic or tactical success metrics that HCU intends to achieve.* • *10 year Strategic Plan* • *Build and maintain accreditations & certifications* • *Acquisition of leading talent*	*Responsibilities that HCU has to students, faculty, patients, staff, and the public.* • *Protect privacy of personal information (PII, PHI, Etc.)* • *Integrity of information*
1. Negligible	**Patient Care**: No impact to patient care. **Education**: No impact to education. **Research**: No impact to research.	**Strategic Plan**: No impact to accomplishing strategic plan. **Accreditations and Certifications**: No impact to maintaining accreditations and certifications. **Recruitment of Leading Talent**: No reduction in ability to attract leading talent.	**Protected Information**: No impact to confidentiality of personal information. **Information Integrity**: Information integrity is not compromised.
2. Low	**Patient Care**: Inconvenience to patients. **Education**: Ability to educate to desired standards is immaterially reduced. **Research**: Some inconvenience in conducting research, but no reduction in research funding or efficacy.	**Strategic Plan**: Any impact to Strategic Plan is within allowable variance. **Accreditations and Certifications**: Allowable variance of accreditation and certification requirements. **Recruitment of Leading Talent**: May rarely limit the ability to recruit or develop leading talent.	**Protected Information**: A release of some information could not pose foreseeable harm to individuals. **Information Integrity**: Information integrity is compromised, but correctible without harm to others.
3. Medium	**Patient Care**: A near-miss may result. **Education**: Reduced ability to educate to desired standards is noted within HCU. **Research**: Some research cannot be conducted completely, and may be halted.	**Strategic Plan**: Strategic Plan may require investment or reprioritization to recover. **Accreditations and Certifications**: Accreditations or certifications may require corrective actions. **Recruitment of Leading Talent**: Could prevent recruitment of leading talent.	**Protected Information**: A release of a small amount of personal information could pose harm to few individuals. **Information Integrity**: Information integrity is compromised with harm to others who can be made whole within a year.

Impact Scores	Impacts Against Mission (The benefit we provide others)	Impacts Against Objectives (Our internal drivers)	Impact Against Obligations (Protecting against harm to others)
4. High	**Patient Care**: Avoidable harm, short of a sentinel event, may result. **Education**: Reduced ability to educate to desired standards is noted outside of HCU. **Research**: Multiple research projects are halted or cannot occur.	**Strategic Plan**: Strategic Plan may require multi-year investment or reprioritization to recover. **Accreditations and Certifications**: Accreditations or certifications would be jeopardized. **Recruitment of Leading Talent**: Could prevent recruitment of leading talent.	**Protected Information**: A release of a large set of personal information. **Information Integrity**: Information integrity is compromised with harm to others who can be made whole over multiple years.
5. Catastrophic	**Patient Care**: Sentinel events or death may result. **Education**: Accreditations are revoked. **Research**: Large-scale shut-down of research and research funding may result.	**Discovery and Innovation**: HCU not consistently supporting discovery and innovation. **Strategic Plan**: Strategic Plan must be abandoned. **Accreditations and Certifications**: Accreditations or certifications would be lost. **Information Infrastructure**: EIA initiatives would be abandoned. **Recruitment of Leading Talent**: Recruitment of leading talent would be difficult. **Entrepreneurship**: HCU would not be able to support commercial development of discoveries and innovations. **Reputation**: Negative statements or opinions about HCU make it difficult for us to achieve mission, objectives or obligations.	**Protected Information**: Multiple releases of a large set of personal information. **Information Integrity**: Information integrity is repeatedly compromised with harm to others.

LIKELIHOOD SCORING

Likelihood Score	Likelihood Definition
1	Not foreseeable
2	Possible
3	Foreseeable, expected to occur once
4	Foreseeable, expected to occur within the year
5	Foreseeable, expected to occur multiple times per year

RISK ACCEPTANCE CRITERIA – BELOW '6'

Likelihood	1. Negligible	2. Low	3. Moderate	4. High	5. Catastrophic
1	1	2	3	4	5
2	2	4	**6**	8	10
3	3	**6**	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25