Information Technology Risk Management Policy

Revised: 03-20-2015

1. Policy

Formal Information Technology ("IT") risk assessments shall be performed at least annually or at planned intervals and should document the likelihood and impact of all identified risks using qualitative and quantitative methods. The IT risk assessments should be performed by a qualified third party independent from the Information Communications and Technology ("ICT") Department. Risks identified in the assessments shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and executive approval. The risk assessment results shall be reported to executive management.

2. Scope

This Policy applies to all Crawford entities globally, excluding Garden City Group.

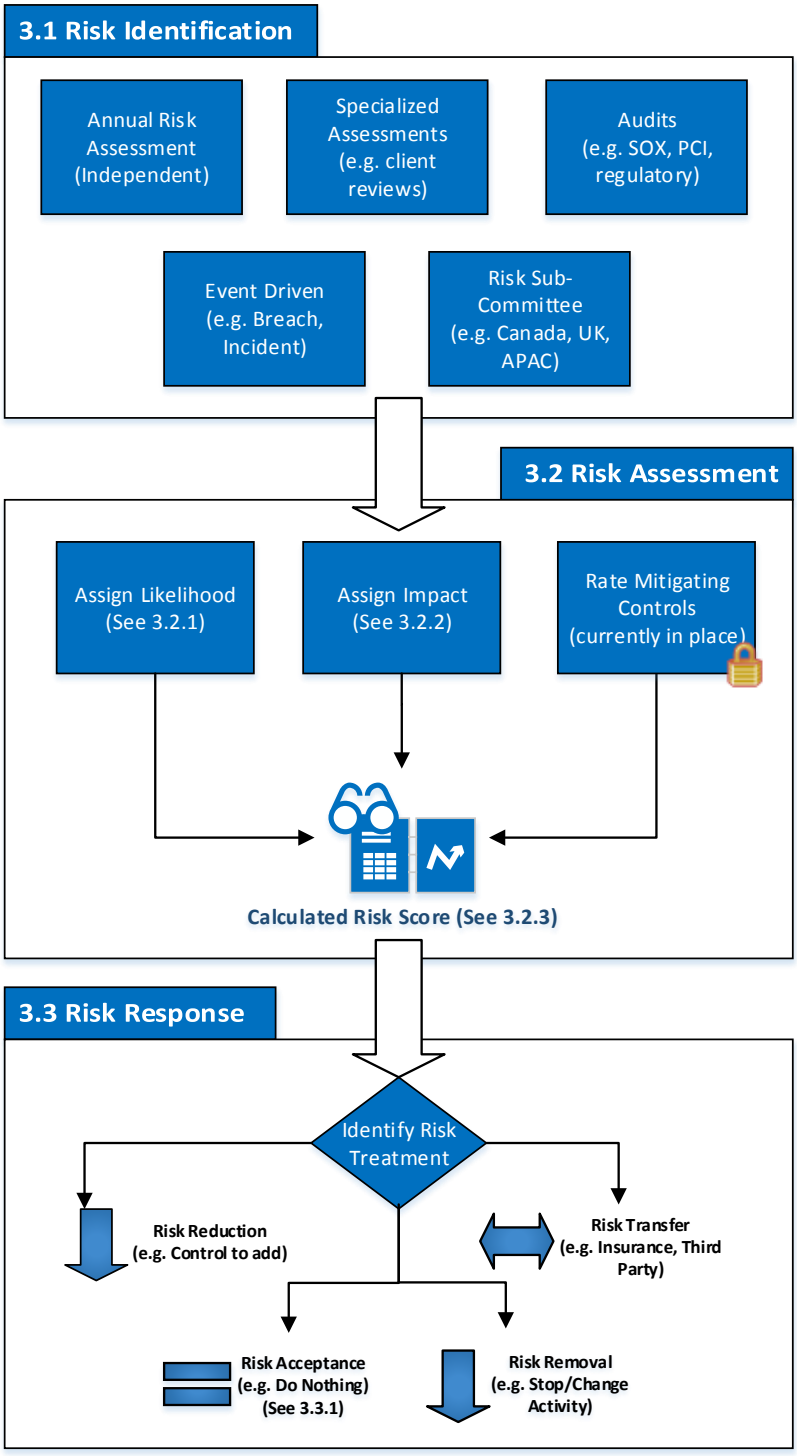
3. Implementation

Crawford's IT risk management process seeks to proactively identify, prioritize, and treat the technology risks that could impact the Company's strategic and financial goals. Executive management uses the information to align its risk management strategies with long term strategic goals.

Following is an overview of the IT risk management process.

(See diagram on next page)

IT Risk Management Process Overview



3.1 Risk Identification

An annual global IT risk assessment based on NIST 800-30 and ISO 27005 is performed by an external third party specializing in Information Security. Existing risks identified in past assessments are reevaluated to determine if mitigating factors or technologies have changed that would impact the risk ranking it previously received. New risks are reviewed and approved by the CTRO or designee and then added to the risk register. Results are formally presented to the Information Security and Privacy Steering Committee, ICT leadership, Global Executive Management, and the Board of Directors.

Risks can be identified by several different methods or channels apart from the annual global IT risk assessment. The following mechanisms for identifying risks are acceptable; however, each new risk that is identified outside of the annual IT risk assessment process must be vetted and approved by the CTRO or designee before being added to the risk register. Further, acute risks have typically lower relative impacts when compared to risks impacting an entire business unit or region.

Specialized Assessments

Targeted assessments (e.g., regulatory or compliance assessments, privacy impact assessments, application security reviews, vulnerability assessments, penetration tests, or client risk assessments) may identify risks specific to a specialized business unit, application or process that would not have been identified during the Global IT Risk Assessment due to scoping considerations.

Internal and External Audits

Assessments or substantive testing procedures executed during internal and external audits (e.g., SOX compliance testing) may provide information that can change existing risk ranking scores. Further, all risks that were considered when control activities were established should be included in the risk register.

Event Driven Risks

Information security related events (e.g., a potential data breach) may drive the identification of new risks that should be evaluated. Typically, events that occur should result in a reevaluation of the existing risks and their risk ranking scores.

Regional Risk Committees

Regional risk committees should not only discuss the current applicable risks, but also attempt to identify new risks that may be significant enough to add to the risk register in the interim of the annual risk assessment process.

3.2 Risk Assessment

Note: For detailed definitions of the ranking criteria noted in the following section, see the Risk Definitions section below.

Crawford's technology risks are scored using a standard methodology to rank risks within a region. Risks

are given an impact and likelihood score. The impact score is a composite of four impact types, financial, strategic and operational, regulatory and compliance, and reputational, with financial impacts weighted higher than the other three impacts. The composite impact and likelihood scores are combined to calculate the Inherent Risk score for each risk. Risk mitigation factors (i.e., technical controls, policies and procedures, and support staffing levels/competencies) are also scored resulting in a residual risk score. Risks are prioritized globally by applying a weighting factor that is based on the region or business unit's percentage of global revenue.

3.2.1 Likelihood

Risk Likelihood measure the probability that an event associated with the risk occurs. Likelihood is scored with the following criteria:

Rating	Probability	Criteria
Almost Certain (5)	≥90%	Event is expected to occur this year.
Likely (4)	60% - 89%	Event will likely occur this year.
Possible (3)	30% - 59%	Event may occur this year and/or prior experience.
Unlikely (2)	10% - 29%	Event could occur this year.
Rare (1)	<10%	Event may only occur in exceptional circumstances.

3.2.2 Impact

Risk impacts are evaluated using four categories (see the detailed descriptions of each below).

Impact Category	Impact Description
Strategic & Operational	Business operations are disrupted. The Company's growth and innovation are impeded.
Financial	Significant loss of revenue or increased expenditures related to recovering from an incident.
Compliance & Regulatory	Incident could result in a large monetary fine, termination of a significant strategic/client contract, or a qualified/adverse audit opinion or third-party assessment.
Reputational	Significant media coverage. Clients, claimants, auditors, regulators or other third parties may require assurances

Each impact type is given a rating (Severe, Major, Moderate, Minor, or Insignificant) utilizing the following criteria:

Category	Severe	Major	Moderate	Minor	Insignificant
Strategic & Operational	Catastrophic business disruption with prolonged ramifications, adversely impacting services provided to clients and/or claimants (>1 week impact)	Significant core business process disruption to a business unit adversely impacting service to clients and/or claimants (<1 week impact)	Core business process disruption to a business unit with only minor service impact to clients and/or claimants (Max 2 day impact)	Disruption to non-core business processes and does not impact service to clients and/or claimants	Inconsequential business disruption
Financial	Greater than 30% of total global revenue	Between 30% and 10% of total global revenue	Between 10% and 5% of total global revenue	Between 5% and 1% of total global revenue	Less 1% of total global revenue
Compliance & Regulatory	Incident results in a criminal offence or a regulator order to restrict certain business activities	Incident could result in a significant fine, termination of a significant strategic/ client contract, or a qualified/ adverse audit opinion or third-party assessment	Incident could result in a moderate fine due to non-compliance with regulations/laws or the termination of a client contract or associate	Incident reportable to board/ authorities/ auditors/ clients/ claimants and no penalty for non-compliance	Incident is non-reportable with limited interest outside of business unit and/or minor exception to internal policy
Reputational	National attention of incident/issue causes clients and/or claimants to sever relationships	Significant media coverage. Clients, claimants, partners, auditors, regulators or other third parties may require assurances	Moderate media coverage. Client and/or claimant awareness of incident/issue becomes more widespread	Limited media coverage or public interest. Few clients or claimants are aware of incident/issue	No media coverage or public interest. Clients and claimants are unaffected

3.2.3

3.2.4 Risk Score

All risks receive a score, which is calculated based on the assessed impact, likelihood, and risk mitigation ratings and factors. The following risk levels are established to facilitate prioritization and to drive remediation timelines:

Risk Level
Critical
High
Moderate
Low

3.3 Risk Response

Risk Response is the strategy Crawford chooses to employ to lower the likelihood an incident does occur and reduce the overall exposure/impact should one occur. If the Company, decides to accept the known risk then only certain groups or individuals can accept the liability the risk is creating (see Section 3.3.1).

Response	Action
Risk Reduction	The level of risk should be reduced through the selection of controls so that the residual risk can be reassessed as being acceptable.
Risk Acceptance	The organization has knowingly and objectively chosen to move forward with the inherent risk and the associated impacts and likelihood. For example, the costs associated with implementing new controls to reduce the risk or transfer the risk are significantly higher than the costs associated with the effects of the risk.
Risk Removal	The activity or condition that gives rise to the particular risk should be avoided or removed. When the identified risks are considered too high, or the costs of implementing other risk treatment options exceed the benefits, a decision may be made to remove or avoid the risk completely, by withdrawing from a planned or existing activity or set of activities, or changing the conditions under which the activity is operated. For example, for risks caused by nature it may be most cost effective alternative to physically move the information processing facilities to a place where the risk does not exist or is manageable.
Risk Transfer	The risk should be transferred to another party that can most effectively manage the particular risk depending on risk evaluation. Risk transfer involves a decision to share certain risks with external parties. Risk transfer can create new risks or modify existing, identified risks. Therefore, additional risk treatment may be necessary. Transfer can be done by insurance that will support the consequences, or by sub-contracting a partner whose role will be to monitor the information system and take immediate actions to stop an attack before it makes a defined level of damage. It should be noted that it may be possible to transfer the responsibility to manage risk but it is not normally possible to transfer the liability of an impact. Customers will usually attribute an adverse impact as being the fault of the organization.
Combination	Multiple methods detailed above are utilized to address the risk

All risks are assigned a risk owner, a responsible individual or department to increase accountability of the tasks associated with risk treatment. The risk owner proposes a risk treatment strategy which is reviewed by the applicable member of the Office of the Chief Information Officer ("OCIO"), i.e., direct reports to the Global Chief Information Officer ("CIO") followed by the Information Security & Privacy Steering Committee.

The risk response should include at a minimum: proposed costs (e.g., estimated work hours and financial costs), estimated time of completion, potential drawbacks/roadblocks, and customer impacts. All risk responses should be reevaluated by the Global CIO, and remediation delays should be communicated to the Information Security & Privacy Steering Committee.

3.3.1 Risk Acceptance

Crawford may choose to accept / retain / tolerate the residual risk level if the costs associated with reducing or transferring the risk outweigh the benefits of risk mitigation. Depending on the residual risk level, the following levels may be accepted by the following parties:

Risk Level	Approved by
Critical	Information Security & Privacy Steering Committee
High	Global CIO
Moderate	Chief Technology Risk Officer
Low	Applicable OCIO member

All risk acceptance decisions must be reported to the Chief Technology Risk Officer, Global CIO, and Information Security & Privacy Steering Committee.

3.4 Risk Matrix

The Risk matrix is a spreadsheet that contains the following:

- A Risk Register – A comprehensive list of each unique risk applicable to the Company
- A Risk Scoring Matrix – Each risk is evaluated for each region (if applicable) and scores for impact, likelihood, risk mitigation, and risk response summaries are captured. The Inherent risk and Residual risk values are also calculated
- Risk Rankings and Heat map – A visual representation of the Impacts and Likelihood rankings associated with risks across the globe.

The spreadsheet is accessible by a limited number of individuals via the following link INSERT LINK.

3.5 Risk Governance Structure

Crawford's IT risk management governance structure is designed and will be adapted as necessary to meet the continuous needs of the business. Committees are in place to oversee the management of technology risks across the Company. Crawford seeks to apply operating principles consistently to each committee.

IT Risk Management Communication Structure

3.5.1 Information Security & Privacy Steering Committee

Objective: The Information Security & Privacy Steering Committee is a forum for executive management members to discuss and set the Company's information security and privacy risk appetite, growing or emerging threats and risks, significant changes to the environment or business processes that may change risk rankings and scores.

Members: The committee is made up of the following:

- Global Chief Information Officer
- Chief Technology Risk Officer (Committee Chair)
- ERM Council representative
- Global Business Development representative
- Global Strategy representative
- Senior management representatives from each territory

Tasks: The committee is charged with the following activities:

- Reviewing current global risk rankings and updating any scores or ratings;
- Discuss any emerging security threats or trends or new business processes that may impact technology risks;
- Adding and approving any new risks that were identified during approved channels (see Section 2.2);
- Discussing any remediation or implementation delays associated with risk treatment response plans within each region or business unit.

3.5.2 Regional Risk Committees

Objective: The Regional Risk Committees are created for each business unit/division/geographic region. The Regional Risk Committees provide tactical information related to the risks identified within the Risk Matrix to ensure risk ratings and scores are accurate. In addition, the committee members drive their business unit's respective risk responses and subsequent remediation plans.

Members: The sub-committee is made up of the following:

- ICT Leader (Regional or Division CIO) – Committee Chair
- ICT Managers that can articulate the details behind noted risks and remediation (no more than three)

Tasks: The Regional Risk Committees are charged with the following activities:

- Reviewing current region/business unit's rankings and updating any scores or ratings;
- Discuss any emerging security threats or trends or new business processes that may impact technology risks;
- Documenting any new risks that may have been identified by the committee or by an approval channel (see Section 2.2);
- Discussing any remediation or implementation delays associated with risk treatment response plans within each region or business unit.

Note: The applicable ICT Compliance group member chairs the Regional Risk Committee and should document notes and meeting minutes to ensure they are communicated to the Information Security & Privacy Working Group.

4. Policy Governance

As the Company develops business objectives and strategies and reacts to a changing business environment and other internal and external factors, amendments, additions and deletions to this Policy may be deemed appropriate. Therefore, it is important to establish the governance processes for policy administration, review, approval and revisions, as well as the process by which exceptions to this Policy may be sought and granted.

4.1 Policy Administration

Administration of this Policy is the responsibility of the Chief Technology Risk Officer ("CTRO"). The CTRO is responsible for maintaining the content of this Policy subject to the policy review/approval, revision and exception requirements outlined below.

4.2 Policy Review and Approval

The Global Chief Information Officer ("CIO") reviews and formally approves this Policy annually, or more frequently as appropriate (e.g., when material changes are required).

4.3 Policy Revisions

Proposed policy revisions will be developed by the CTRO for review and evaluation by the Information Security & Privacy Steering Committee. The CTRO recommends revisions for approval by the Global CIO.

4.4 Policy Exceptions

Exceptions to this Policy will be reported to and approved by Global CIO.

Policy Name	Information Technology Risk Management
Policy Number	Global IT Policy 00002
Effective Date	03-20-2015
Approved By	Global CIO
Last Approval Date	03-20-2015