Risk and Risk Mitigation Strategies

Privacy risks, such as unauthorized access, collection, use, disclosure or destruction of personal information, can arise from new technologies, upgrades to existing technologies, generation of large amounts of data and changes in business processes when privacy implications are not considered.

PRIVACY RISKS

- Risk 1 – **Strategic Risk:** failure to comply with provisions of the FOIP Act, including unauthorized collection, access, use, disclosure or destruction of personal information
- Risk 2 – **Operational and Strategic Risk:** theft of personal information
- Risk 3 – **People and Strategic Risk:** re-identification and commingling of personal information
- Risk 4 – **People and Strategic Risk:** embarrassment, humiliation, discrimination, health and safety, identity theft or reputational damage (to an individual or to The City)

PRIVACY RISK MITIGATION STRATEGIES

The City mitigates these potential privacy risks by making the following reasonable security arrangements:

Administrative Safeguards

- Administration policies, procedures and practices
- Training for City employees, including contracted service providers
- Privacy Impact Assessments and Threat Risk Assessments

Physical Safeguards

- Access and authorization mechanisms (for example, employee access cards)
- Physical Security Risk assessments for priority sites
- Physical security systems are in place to protect sites and information assets
- Secure filing rooms and cabinets for storage which include access control mechanisms.

Technological Safeguards

- Information assets at The City are controlled and protected, including The City’s technical infrastructure (hardware and software).
- With the extensive use of third-party technologies, services and tools, Information Technology provides:
  - Access controls on devices
  - Access control for applications and databases
  - Risk management
  - Intrusion protection
  - Usage restrictions
  - Virus protection
  - Network security

Information Technology makes use of these technologies to monitor, audit and report on all aspects of our technical environment to ensure compliance to each of the pertinent policies.

Risk mitigation strategies related to the four specific risks outlined above:

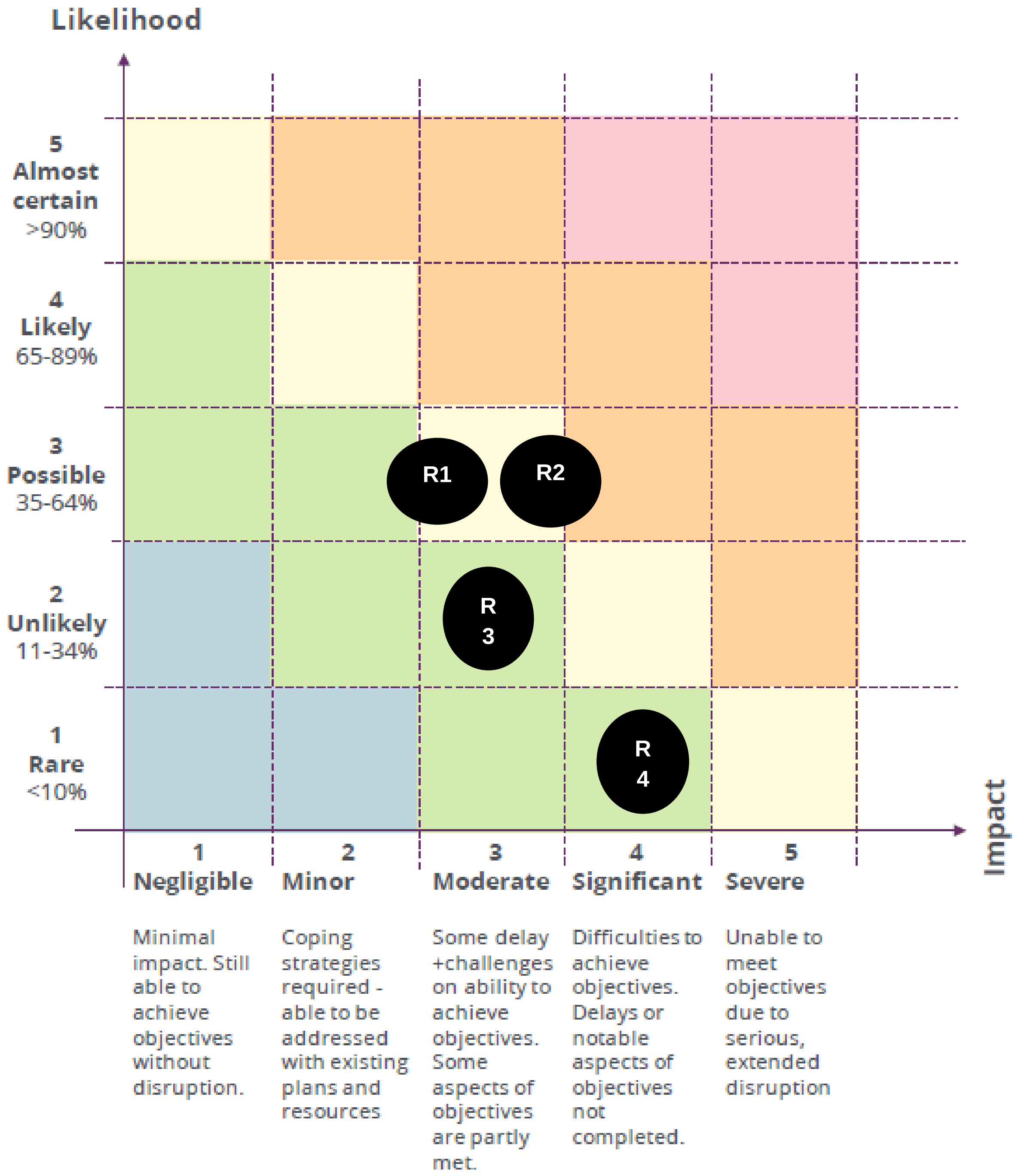
- Risk 1 – **Strategic Risk:** failure to comply with provisions of the FOIP Act, including unauthorized collection, access, use, disclosure or destruction of personal information. Risk mitigation strategies include:
  - Administrative safeguards – Administration policies, procedures and practices; training for City employees, including contracted service providers; and Privacy Impact Assessments and Threat Risk Assessments
  - Physical safeguards – securing confidential information in a locked cabinet or room
  - Technological safeguards – creating strong passwords and changing passwords regularly; and restricting access to confidential information on a need to know basis

- Risk 2 – **Operational and Strategic Risk:** theft of personal information. Risk mitigation strategies include:
  - Administrative safeguards - Administration policies, procedures and practices; training for City employees, including contracted service providers; and Privacy Impact Assessments and Threat Risk Assessments
  - Physical safeguards – securing confidential information in a locked cabinet or room
  - Technological safeguards –
    - Information Technology uses tools to manage The City's hardware, including standardization for how they are built and installed, hard drive encryption, enforcement of security rules, regularly updated security patches, and the ability to lock remotely in case of theft
    - To help ensure business continuity and protection of data, Information Technology keeps The City's third-party technologies and services up to date and stable to ensure the latest security protections are in place.
    - User Authentication: systems and procedures are in place to authenticate users. The City requires a username and password, two-factor authentication (for remote access), certificate, external token, or biometrics before access is granted to systems handling personal information.

- Risk 3 – **People and Strategic Risk:** re-identification and commingling of personal information. Risk mitigation strategies include:
  - Administrative safeguards –
    - Administration policies, procedures and practices; training for City employees, including contracted service providers; and Privacy Impact Assessments and Threat Risk Assessments
    - Partial release or suppressing aggregate records that apply to very few individuals
    - Anonymizing (removing) or pseudonymizing (replacing) fields containing personally identifying information.
    - Generalizing or aggregating data to reduce the risk of re-identifying an individual.

- Risk 4 – **People and Strategic Risk:** embarrassment, humiliation, discrimination, health and safety, identity theft or reputational damage (to an individual or to The City). Risk mitigation strategies include:
  - Administrative safeguards – Administration policies, procedures and practices; training for City employees, including contracted service providers; and Privacy Impact Assessments and Threat Risk Assessments

- Physical safeguards – securing confidential information in a locked cabinet or room; restrict site access to authorized individuals through swipe card access or keys
- Technological safeguards – creating strong passwords and changing passwords regularly; restricting access


Likelihood
5 Almost certain >90%
4 Likely 65-89%
3 Possible 35-64%
2 Unlikely 11-34%
1 Rare <10%
R1
R2
R 3
R 4
Impact
1 Negligible
2 Minor
3 Moderate
4 Significant
5 Severe
Minimal impact. Still able to achieve objectives without disruption.
Coping strategies required - able to be addressed with existing plans and resources
Some delay +challenges on ability to achieve objectives. Some aspects of objectives are partly met.
Difficulties to achieve objectives. Delays or notable aspects of objectives not completed.
Unable to meet objectives due to serious, extended disruption