SEng 460 / ECE 574
Practice of Information Security and Privacy

Week 4:

Risk Management, Risk Assessment

Asset Security, Information Classification

Supply Chain, Third Parties, Cyber Insurance

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

Questions the CEO/Board are asking security teams:

1. do you know what our critical systems and data are?

2. what are the security controls in place?

3. are the controls sufficient to mitigate risk to an acceptable level?

University of Victoria

Questions the CEO/Board should be able to answer:

1. what are the key cybersecurity risks affecting your industry/organization?
2. is your organization aligned with an existing industry security standard (ie. ISO or NIST)
3. what is your current capability/maturity rating?
   (0 – Not Implemented, 1 – Initial, 2 – Repeatable, 3 – Defined, 4 – Managed, 5 – Optimized)
4. what is your desired capability/maturity rating?
5. do you have a plan to reach the desired level?
6. how frequently do you receive plan updates?
7. is security a recurring item on the board agenda?

University of Victoria

Vulnerability

- an absence or weakness of a countermeasure in place, weakness in a system
- weakness that could be used to endanger or cause harm to an info asset
- exposed to the possibility of being attacked or harmed
- weakness that can be exploited by threats to gain unauthorized access
- flaws or weaknesses in security systems, software, or procedures
- eg. systems may be vulnerable to SQL injection, XSS, others
- factors in prioritizing: criticality of the system, sensitivity of information, severity of the vulnerability, exposure of the vulnerability (what would they need to exploit it)

University of Victoria

Threat

- **threat**:
  - any potential danger associated with the exploitation of a vulnerability
  - anything that has the potential to do harm
  - something that could have a negative impact to the organization

- **threat agent**:
  - entity that takes advantage of a vulnerability

Risk

- **risk**:
  - probability that a vulnerability will be exploited and the impact if it does
  - likelihood that someone bad will happen that causes harm
  - potential for loss, damage, destruction of an asset as a result of a **threat** exploiting a **vulnerability**

"what happens when a threat meets a vulnerability"

Risk Formula

- risk formula (many different variations)
  - **risk = probability * impact**
  - risk = probability * frequency * impact
  - risk = probability * loss
  - risk = likelihood * consequence
  - risk = likelihood/probability * loss/consequence/impact
  - risk = asset + threat + vulnerability + risk

Risk Assessment

- **2 kinds of risk assessments**

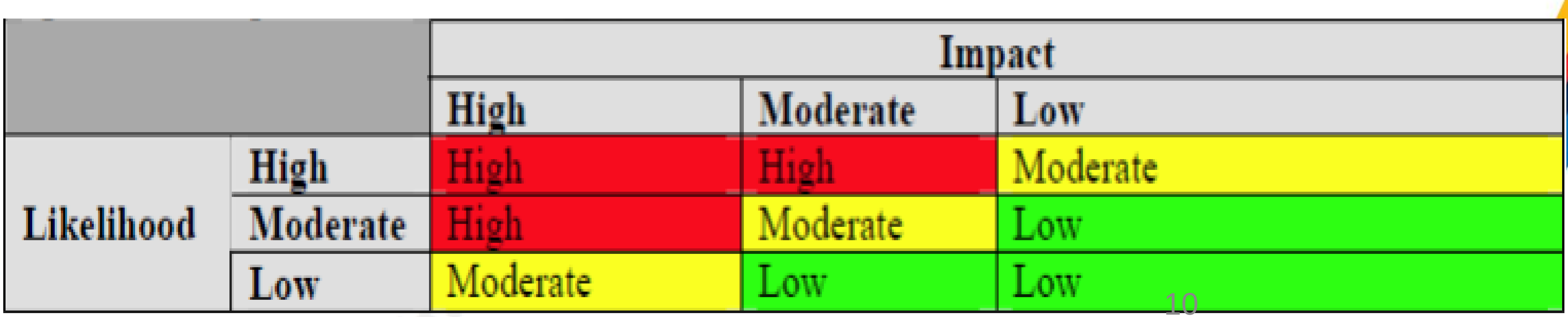
1) quantitative
2) qualitative

Risk Assessment

- **quantitative risk assessment** **objective, calculated**
  1) determine AV for each asset (asset value)
  2) identify threats
  3) determine EF (exposure factor)
  4) calculate SLE, ARO, ALE

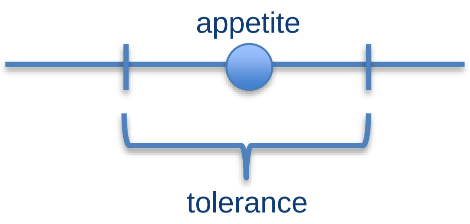
Risk Assessment

- **qualitative risk assessment** **subjective**
  - ranks seriousness of threats by standard
    - low
    - medium
    - high



		Impact		
		High	Moderate	Low
Likelihood	High	High	High	Moderate
	Moderate	High	Moderate	Low
	Low	Moderate	Low	Low

Risk Terms



- risk appetite
  - amount of risk an entity is willing to accept in pursuit of value
- risk tolerance
  - includes upper and lower limits, variation
  - consider how much risk you’re able to take and how much you’re willing to take
- risk register
  - inventory of risks to an organization
- risk assessment
  - identifying and prioritizing risks to the business
  - determines risk by assessing qualitative and quantitative factors

Risk Terms

- threat:
  - anything that can exploit a vulnerability, potential negative occurrence
- exploit:
  - successfully executing on a vulnerability
- incident
  - an exploited vulnerability
- risk owner
  - individual responsible for ensuring a risk is managed appropriately

Single Loss Expectancy (SLE)

AV x EF = SLE

- AV: asset value
  - how much the organization could lose
- EF: exposure factor
  - how long the asset will stay in failure or how much time to repair
- single loss expectancy (SLE):
  - value you lose when the risk becomes real
- Example: $1M asset value website

DDOS = 10% loss in value = $100k

Annual Loss Expectancy (ALE)

SLE x ARO = ALE

- ALE: annualized loss expectancy (cost of loss due to risk over a year)
- SLE: single loss expectancy
- ARO: annualized rate of occurrence
  - chance the risk turns real
- annual loss expectancy:
  - value you will measure if risk becomes real in one year
- Example: DDOS happens once every 2 years:

$100K x 0.5 = $50k

Annual Loss Expectancy (ALE)

(AV x EF) x ARO = ALE

- example:
  - AV: $1M
  - EF: 10% loss in value
  - ARO: once every 2 years (1 over 2 or ½)
- ALE = $50k

Controls

- **many different names often referring to the same or similar things:**
  - eg. controls, compensating controls, countermeasures, safeguards, mitigations
  - control or mechanism that reduces the potential risk
  - implemented to bring risk to an acceptable level
  - mechanism to restrain/regulate/reduce vulnerabilities
  - **measure taken to reduce risk**
- countermeasure value = ALE previous – ALE now
- total cost of ownership: cost of a safeguard
- return on investment: money saved by deploying safeguard

University of Victoria

Inherent, Residual Risk

- **inherent risk:**
  - natural level of risk; level of raw or untreated risk
  - rating exposure in absence of controls
  - existing risk before controls are applied

- **residual risk:**
  - remaining risk as it is impossible to identify all risks or fully mitigate or eliminate all risks
  - risk remaining after controls are applied
  - risk left over after countermeasures

Risk Register

Risk	Definition	Inherent risk	Risk trend	Key risk mitigation strategies	Residual risk	Owner
Network Security	Insufficiently proactive approach on identification of threats and vulnerabilities in network infrastructure and timely mitigation may result in network outages and exposure					
Data Security	Insufficient application of adequate security controls, heightened by increased risks from ransomware and profit-driven cyber criminals results in an inability to identify and mitigate unauthorized access, disclosure, modification, deletion of sensitive data					
Physical						

University of Victoria

Risk Register

Risk	Definition	Inherent risk	Risk trend	Key risk mitigation strategies	Residual risk	Owner
Network Security	Insufficiently proactive approach on identification of threats and vulnerabilities in network infrastructure and timely mitigation may result in network outages and exposure	**High**	↑	• firewalls • intrusion prevention • anti-DDoS • web content filtering • email content filtering • strong authentication • encrypted protocols	**Moderate**	Mary
Data Security	Insufficient application of adequate security controls, heightened by increased risks from ransomware and profit-driven cyber criminals results in an inability to identify and mitigate unauthorized access, disclosure, modification, deletion of sensitive data	**Moderate**	↑	• encryption at rest • encryption in transit	**Moderate**	Steve
Other						
Other						

Risk Treatment

- risks can be

ignored/rejected	
accepted	risk acceptance
avoided	risk avoidance
transferred	risk transference
mitigated/reduced/treated	risk mitigation

- risks often can’t be eliminated
- threats and vulnerabilities impact likelihood or consequence of risk

Risk Treatment

- ignored/rejected: hope it won’t occur
- accepted: understood and evaluated; benefits outweigh the risk
- avoided: change plans, avoiding an activity that has the risk
- transferred: to third party; obtain insurance
- mitigated/ reduced/treated: eg. install firewall

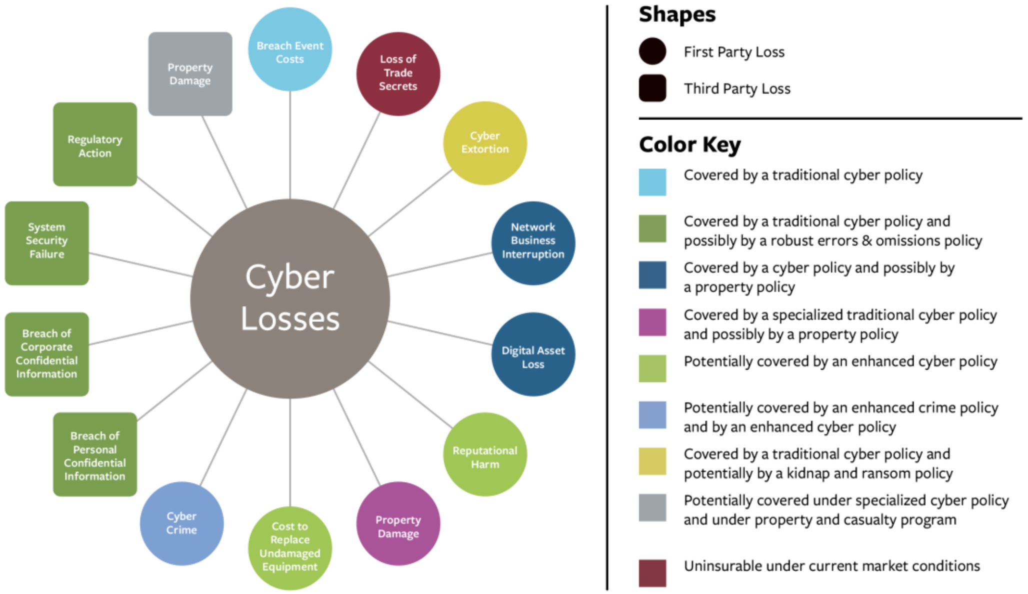
Cyber Insurance

- insurance you buy against cyber attacks
- relatively immature market
- often there are minimum requirements you must meet
- difficult to make claims
  - what if the attack was successful because you didn't maintain the minimum
- must demonstrate it was a cyber attack or..?
- financial compensation does not address the damage to reputation

Cyber-insurance is a specialty lines insurance product intended to protect businesses, and individuals providing services for such businesses, from Internet-based risks, and more generally from risks relating to information technology infrastructure, information privacy, information governance liability, and activities related thereto. Risks of this nature are typically excluded from traditional commercial general liability policies or at least are not specifically defined in traditional insurance products. Coverage provided by cyber-insurance policies may include first-party coverage against losses such as data destruction, extortion, theft, hacking, and denial of service attacks; liability coverage indemnifying companies for losses to others caused, for example, by errors and omissions, failure to safeguard data, or defamation; and other benefits including regular security-audit, post-incident public relations and investigative expenses, and criminal reward funds. ~ Wikipedia

Cyber Insurance

- read the fine print
- if you make a claim you may find that there are terms in the contract that say you must retain the services of the company specified
- including incident handling/response or cyber breach hostage negotiator
- who is in control then?
- often companies think they can transfer the risk by buying cyber insurance and/or do so because they are confused on what to do so ‘give up’ or perhaps they have invested in security and thought they were done and then surprised by the fact they need to continue investing in this ‘cyber arms race’


Cyber Losses
Breach Event Costs
Loss of Trade Secrets
Cyber Extortion
Network Business Interruption
Digital Asset Loss
Reputational Harm
Property Damage
Cost to Replace Undamaged Equipment
Cyber Crime
Breach of Personal Confidential Information
Breach of Corporate Confidential Information
System Security Failure
Regulatory Action
Property Damage
Shapes
First Party Loss
Third Party Loss
Color Key
Covered by a traditional cyber policy
Covered by a traditional cyber policy and possibly by a robust errors & omissions policy
Covered by a cyber policy and possibly by a property policy
Covered by a specialized traditional cyber policy and possibly by a property policy
Potentially covered by an enhanced cyber policy
Potentially covered by an enhanced crime policy and by an enhanced cyber policy
Covered by a traditional cyber policy and potentially by a kidnap and ransom policy
Potentially covered under specialized cyber policy and under property and casualty program
Uninsurable under current market conditions

https://www.fdd.org/analysis/2020/09/02/the-time-for-cyber-insurance/

Cyber Insurance

- remember – security is not an IT problem
- insure against security incidents the same way you would other risks
- if you self-insure against other risks then consider doing the same
- if you buy 3rd party insurance for other risks consider doing the same
- consider what you will get - will it make you ‘whole’?

Risk

- **risk treatment**
  - selection and implementation – one of the measures to modify risk
- **risk remediation**
  - fix or correction to a vulnerability decreasing or eliminating risk
- **risk transference**
  - measures to place responsibility on another entity (eg. insurance)
- **risk mitigation/deterrence**
  - measures put in place to protect against a risk

Risk

- **types of controls**

deterrent	reduce likelihood of attack, discouraging violation
preventive	protect vulnerabilities and make attack unsuccessful
detective	determine whether controls are working; detect errors
corrective	remedying violations and improving
recovery	restoring systems and information
compensating	put in place of another control alternative ways of achieving tasks

RISK STATEMENT EXAMPLE

CONSIDER THE THREAT WHICH ACTS
ON THE VULNERABILITY (WEAKNESS)

THREAT

malicious person or software →

VULNERABILITY

e.g.
remote code execution

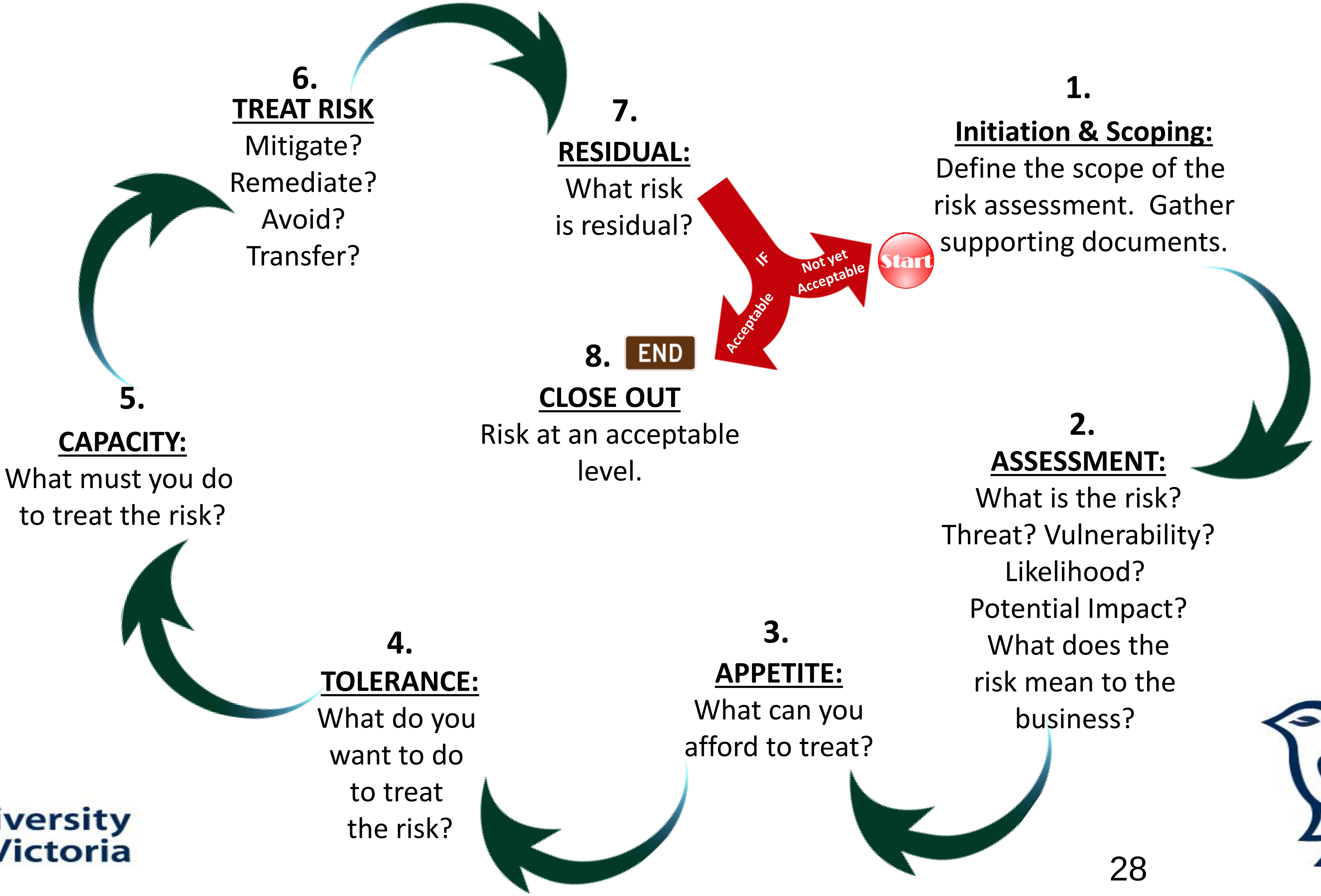
weakness

RISK STATEMENT

stolen data, system damage, and unavailability **caused by** a malicious person or software **leveraging** a remote code execution vulnerability.

University of Victoria

Risk Management Life Cycle



1. **Initiation & Scoping:**
Define the scope of the risk assessment. Gather supporting documents.

2. **ASSESSMENT:**
What is the risk?
Threat? Vulnerability?
Likelihood?
Potential Impact?
What does the risk mean to the business?

3. **APPETITE:**
What can you afford to treat?

4. **TOLERANCE:**
What do you want to do to treat the risk?

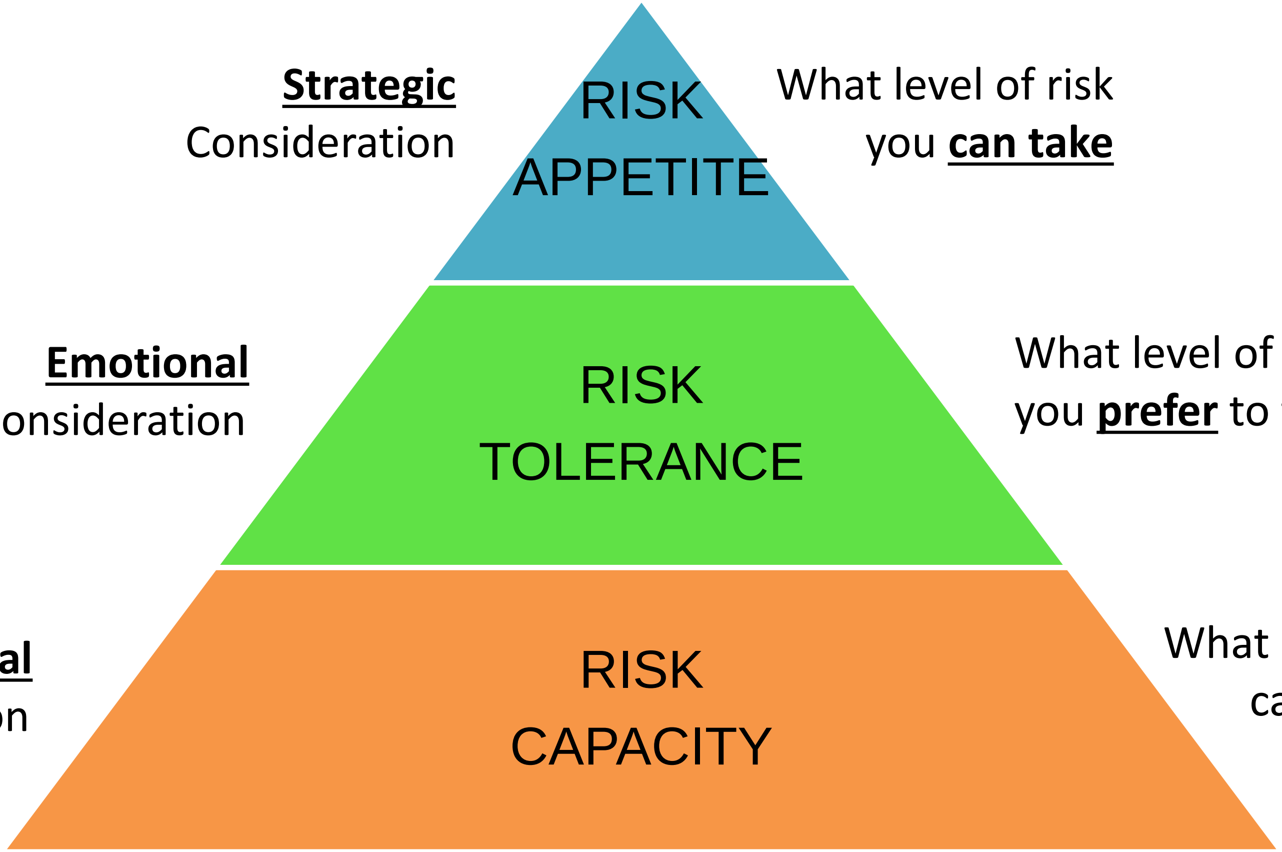
5. **CAPACITY:**
What must you do to treat the risk?

6. **TREAT RISK**
Mitigate?
Remediate?
Avoid?
Transfer?

7. **RESIDUAL:**
What risk is residual?

8. END
CLOSE OUT
Risk at an acceptable level.

Understand your risk appetite, tolerance, and capacity



<u>Strategic</u> Consideration

RISK APPETITE

What level of risk you **<u>can take</u>**

<u>Emotional</u> Consideration

RISK TOLERANCE

What level of risk you **<u>prefer</u>** to take

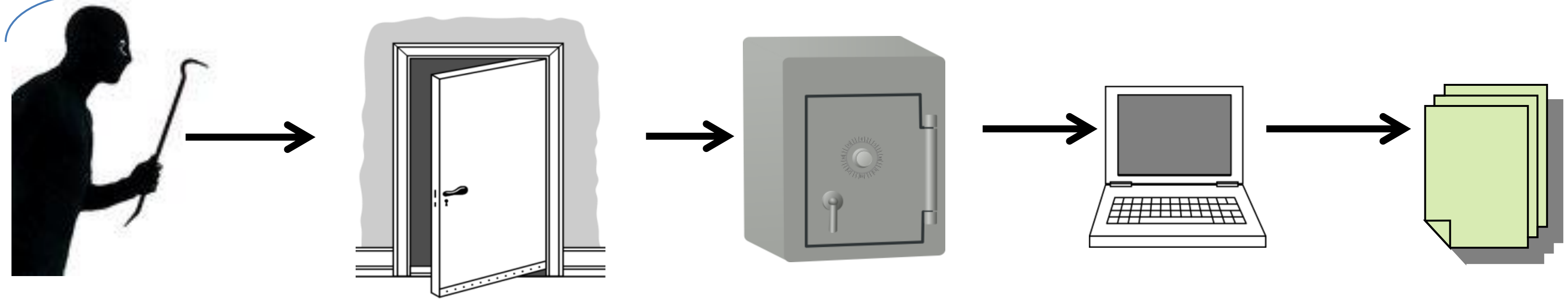
<u>Financial</u> Consideration

RISK CAPACITY

What level of risk you can **<u>afford</u>** to take

Consider this risk scenario…

Understanding these elements helps you to identify what is needed to treat risk



THREAT (PERSON, GROUP, PROCESS, OR TECHNOLOGY)

PRIMARY **VULNERABILITY** (WEAKNESS)

EFFECTIVENESS OR LACK OF EFFECTIVENESS OF **COMPENSATING CONTROL(S)**

SYSTEM

INFORMATION

What needs protection

Likelihood that threat will use the vulnerability

Helps you to understand potential impact

Likelihood that threat will use the vulnerability and what the potential impact looks like if that occurs

Likelihood * Potential Impact = Risk Rating

Very low, low, medium, high, critical

University of Victoria

Risk Assessment

- when should you do a risk assessment?
  1) when introducing a new system
  2) material change to an existing one

- eg. implementing new system or website often increases risk

- it rarely stays the same or decreases unless it’s a security device…

Risk Assessment

- steps
  1) identify target/scope, stakeholders, background
  2) identify criticality

     - what is the sensitivity of the data?

     - maximum level of harm if disclosed, changed, unavailable
  3) identify vulnerabilities and threats
  4) identify risks
  5) identify actions
  6) obtain approvals/signatures

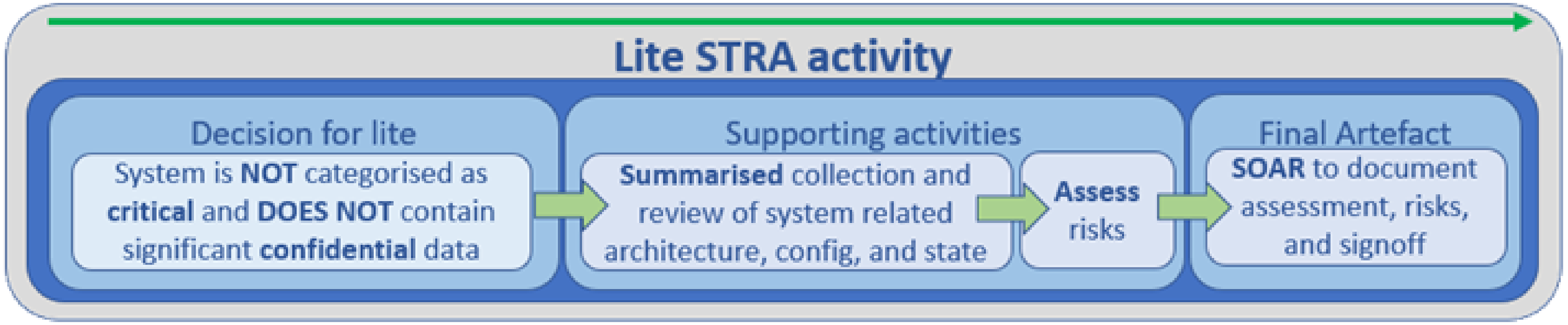
Risk Assessments

- what is the risk assessment on
- is it a new system or material change to existing one?
- who are the stakeholders?
- what does the system do?
- does it hold confidential information?
- maximum level of harm if info. disclosed?
- maximum length of time system can be unavailable?

Risk Assessments

STRA Process

- A SOAR is needed to complete the STRA process and is the final artefact. An STRA is conducted for new systems and material changes to existing ones. An STRA must be conducted for all information systems during planning, development and implementation. A review and update to the STRA and SOAR must be conducted throughout the life of an existing information system.
- Security risks need to be considered at every stage of a system's lifecycle. The Information Security Policy, Information Security Standard, and Security Threat and Risk Assessment Standard define specific triggers and situations for when an STRA should be conducted.
- A comprehensive STRA with its additional detail, evidence, and artefacts is not always required. The supporting activities for a lite STRA are much faster to work through and the only artefact required is the SOAR. Depending on the system to be assessed the

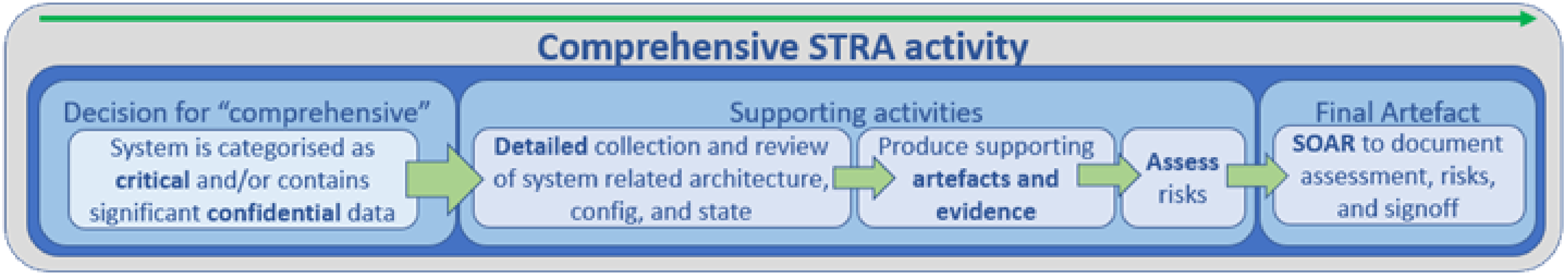


Lite STRA activity

Decision for lite: System is **NOT** categorised as **critical** and **DOES NOT** contain significant **confidential** data

Supporting activities: **Summarised** collection and review of system related architecture, config, and state → **Assess** risks

Final Artefact: **SOAR** to document assessment, risks, and signoff



Comprehensive STRA activity

Decision for "comprehensive": System is categorised as **critical** and/or contains significant **confidential** data

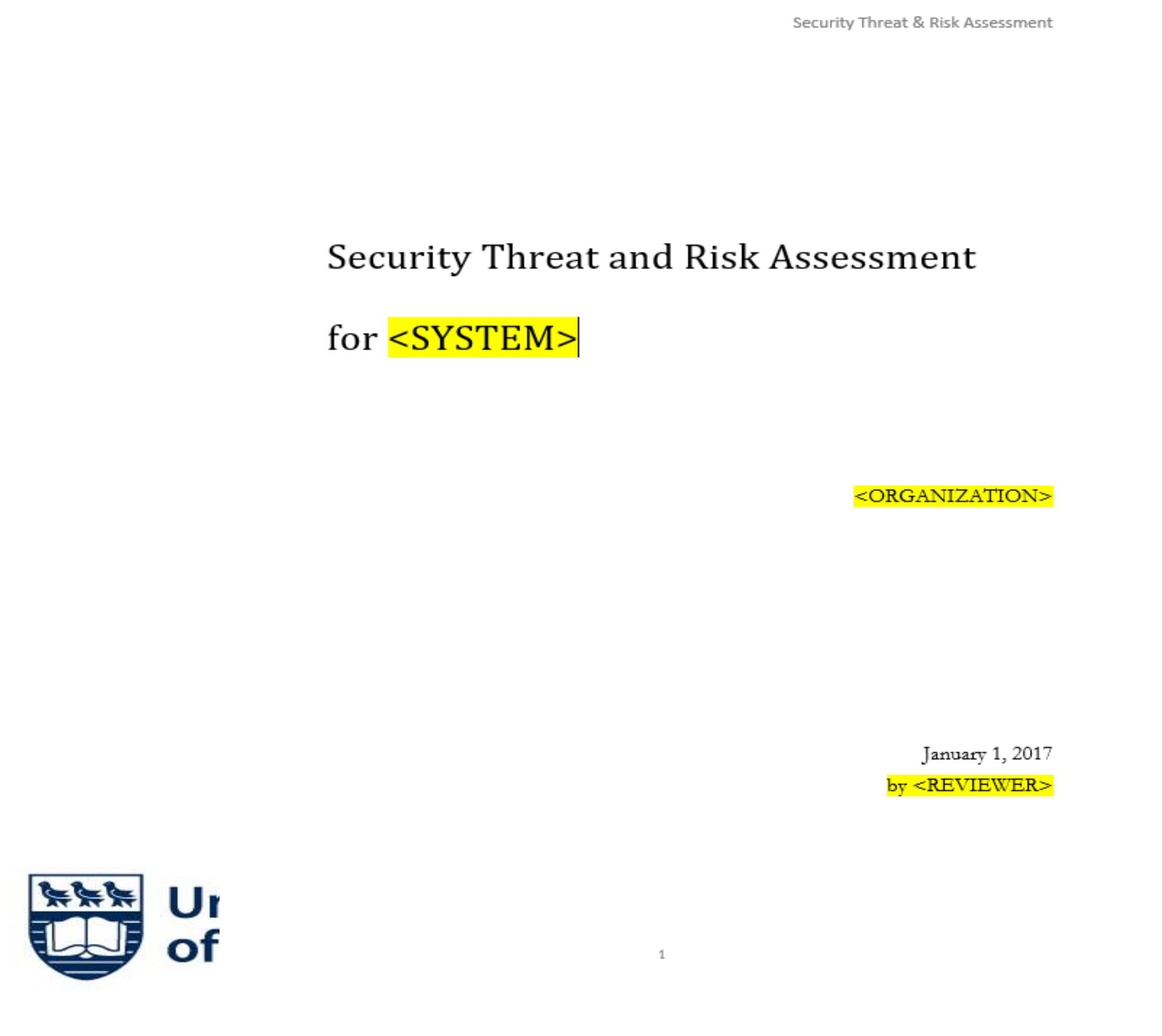
Supporting activities: **Detailed** collection and review of system related architecture, config, and state → Produce supporting **artefacts and evidence** → **Assess** risks

Final Artefact: **SOAR** to document assessment, risks, and signoff

University of Victoria

Risk Assessments

- Security Threat and Risk Assessment (STRA)



Security Threat & Risk Assessment

Security Threat and Risk Assessment

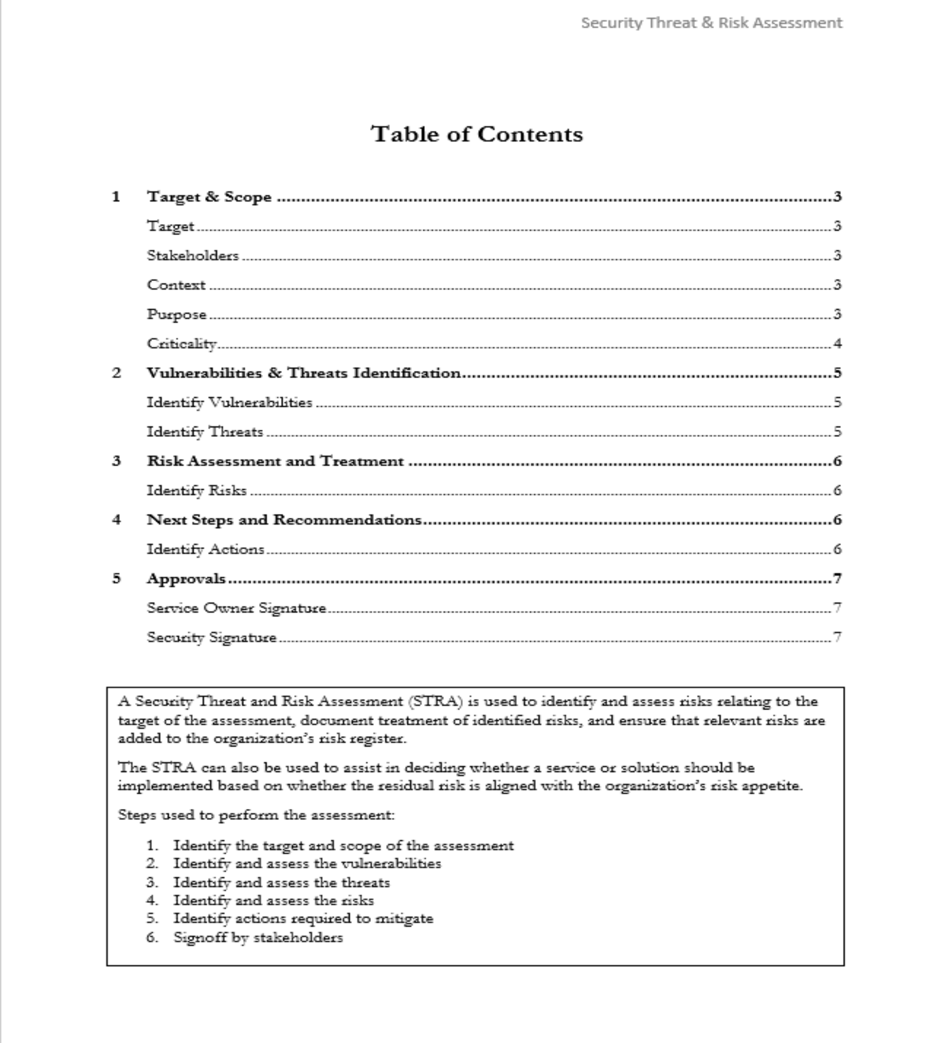
for <SYSTEM>

<ORGANIZATION>

January 1, 2017

by <REVIEWER>

1



Security Threat & Risk Assessment

Table of Contents

A Security Threat and Risk Assessment (STRA) is used to identify and assess risks relating to the target of the assessment, document treatment of identified risks, and ensure that relevant risks are added to the organization's risk register.

The STRA can also be used to assist in deciding whether a service or solution should be implemented based on whether the residual risk is aligned with the organization's risk appetite.

Steps used to perform the assessment:

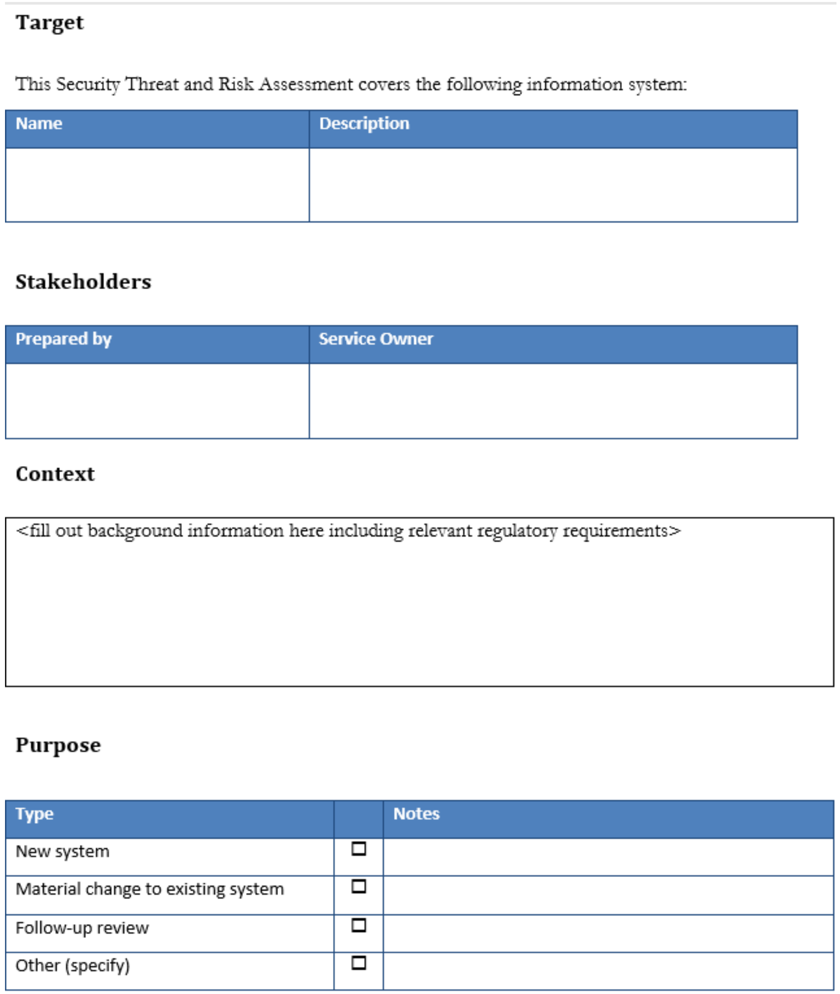
1. Identify the target and scope of the assessment
2. Identify and assess the vulnerabilities
3. Identify and assess the threats
4. Identify and assess the risks
5. Identify actions required to mitigate
6. Signoff by stakeholders

Risk Assessment Sections (Sample)

- Target & Scope
  - Stakeholders, Context
  - Purpose, Criticality
- Vulnerabilities & Threat Identification
  - Identify Vulnerabilities
  - Identify Threats
- Risk Assessment and Treatment
  - Identify Risks
- Next Steps and Recommendations
  - Identify Actions
- Approvals
  - Business Owner Signature
  - Security Signature

Risk Assessment Sections (Sample)

- Target & Scope
  - Stakeholders, Context, Purpose, Criticality



Target

This Security Threat and Risk Assessment covers the following information system:

Name	Description

Stakeholders

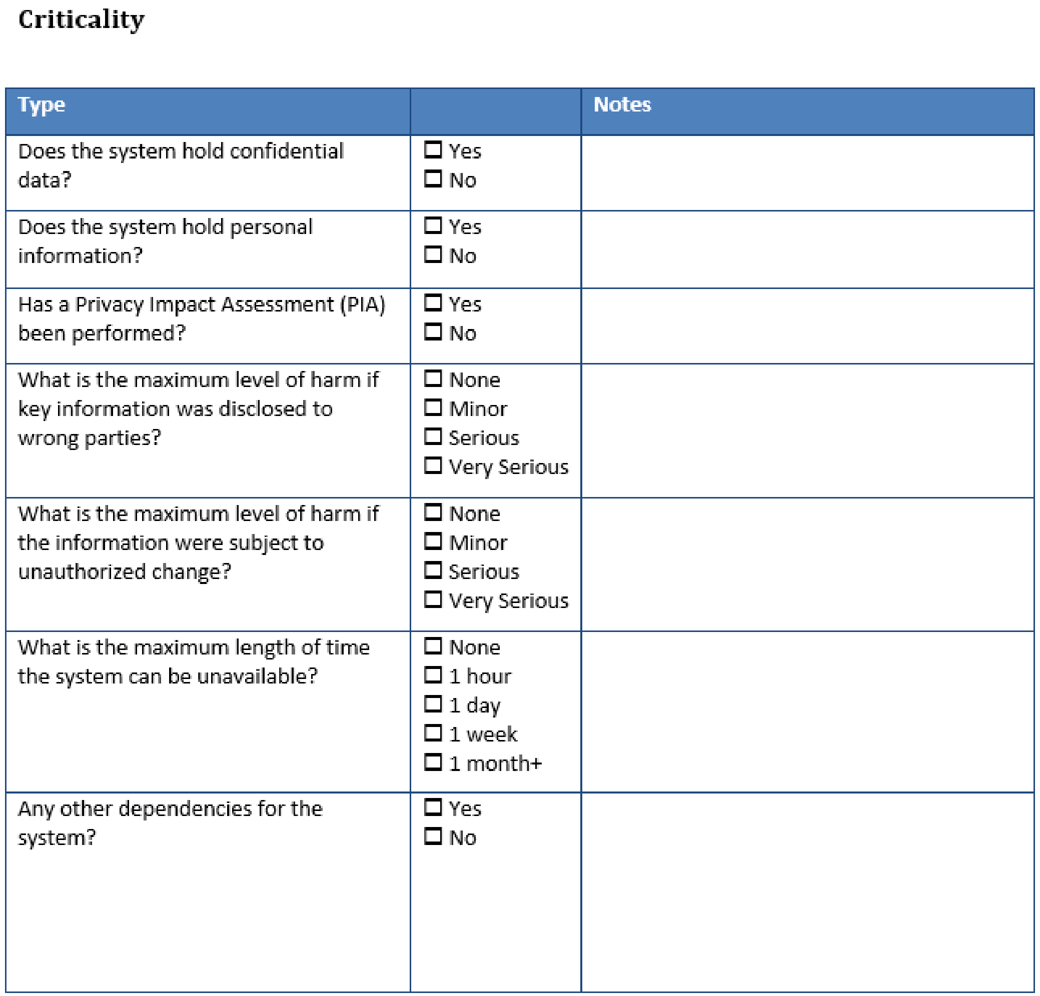
Prepared by	Service Owner

Context

<fill out background information here including relevant regulatory requirements>

Purpose

Type		Notes
New system	□	
Material change to existing system	□	
Follow-up review	□	
Other (specify)	□	

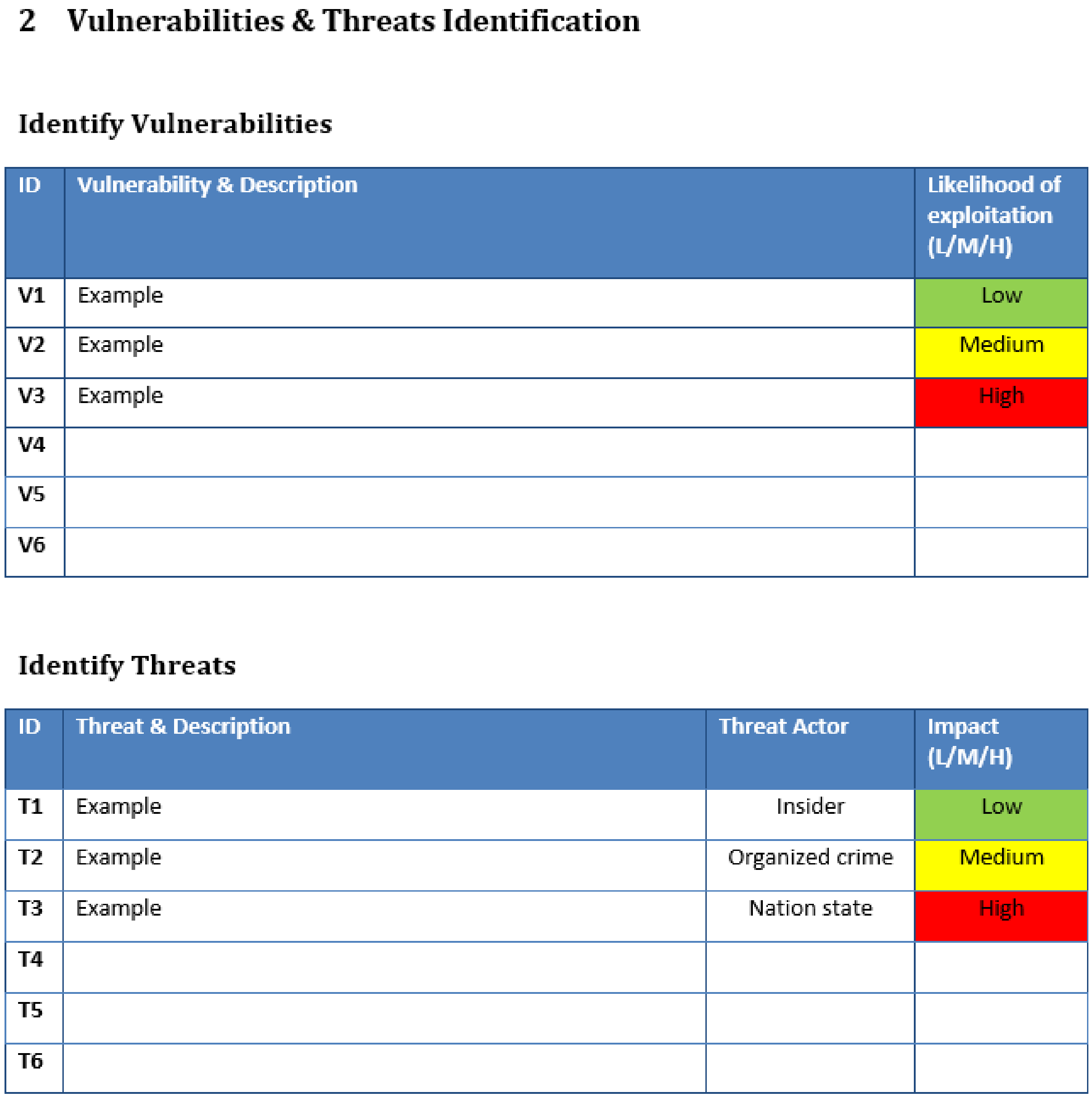


Criticality

Type		Notes
Does the system hold confidential data?	□ Yes □ No	
Does the system hold personal information?	□ Yes □ No	
Has a Privacy Impact Assessment (PIA) been performed?	□ Yes □ No	
What is the maximum level of harm if key information was disclosed to wrong parties?	□ None □ Minor □ Serious □ Very Serious	
What is the maximum level of harm if the information were subject to unauthorized change?	□ None □ Minor □ Serious □ Very Serious	
What is the maximum length of time the system can be unavailable?	□ None □ 1 hour □ 1 day □ 1 week □ 1 month+	
Any other dependencies for the system?	□ Yes □ No	

Risk Assessment Sections (Sample)

- Vulnerabilities & Threat Identification
  - Identify Vulnerabilities
  - Identify Threats



2 Vulnerabilities & Threats Identification

Identify Vulnerabilities

ID	Vulnerability & Description	Likelihood of exploitation (L/M/H)
V1	Example	Low
V2	Example	Medium
V3	Example	High
V4		
V5		
V6		

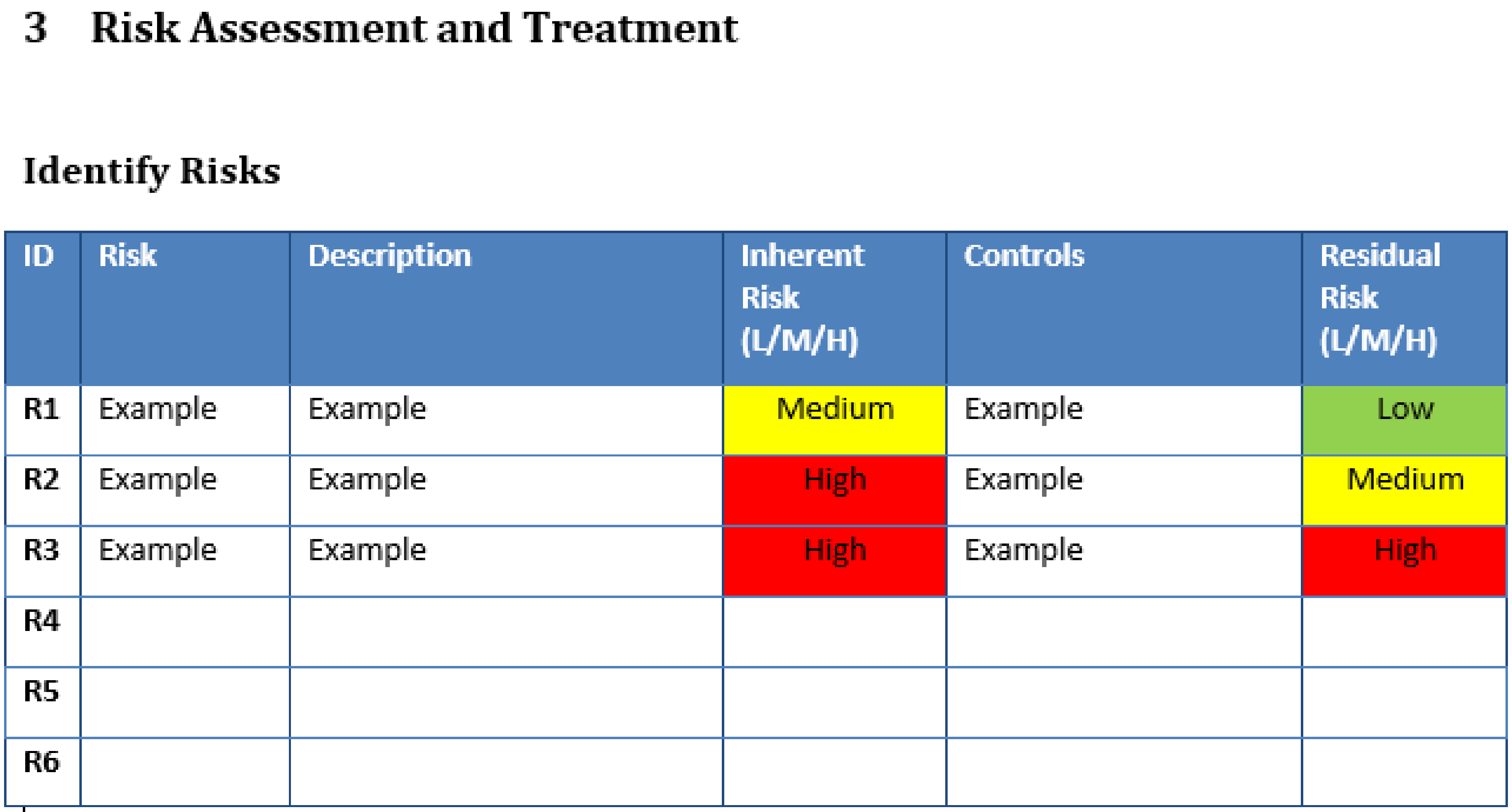
Identify Threats

ID	Threat & Description	Threat Actor	Impact (L/M/H)
T1	Example	Insider	Low
T2	Example	Organized crime	Medium
T3	Example	Nation state	High
T4			
T5			
T6			

University of Victoria

Risk Assessment Sections (Sample)

- Risk Assessment and Treatment
  - Identify Risks



3 Risk Assessment and Treatment

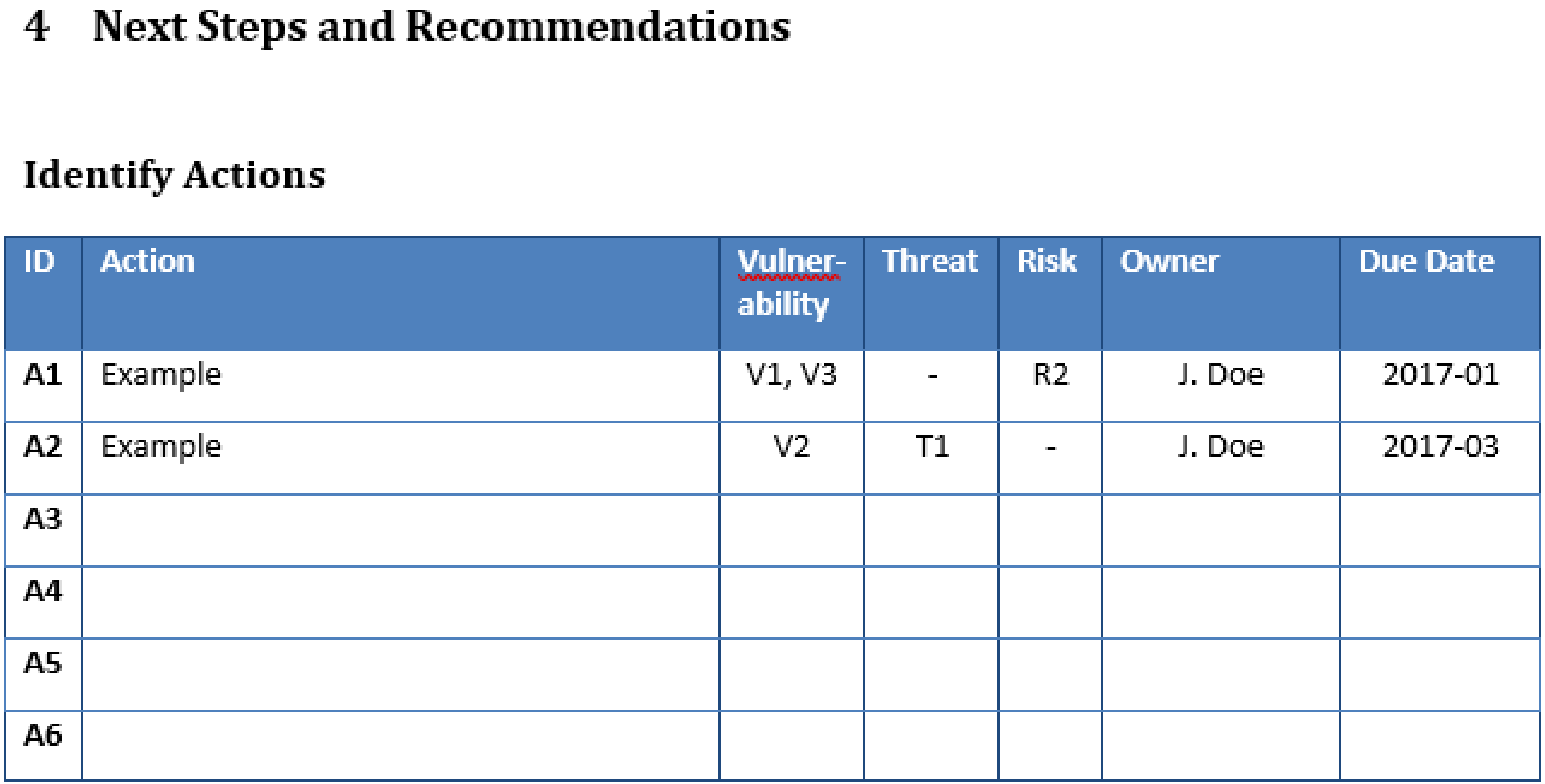
Identify Risks

ID	Risk	Description	Inherent Risk (L/M/H)	Controls	Residual Risk (L/M/H)
R1	Example	Example	Medium	Example	Low
R2	Example	Example	High	Example	Medium
R3	Example	Example	High	Example	High
R4					
R5					
R6					

University of Victoria

Risk Assessment Sections (Sample)

- Next Steps and Recommendations
  - Identify Actions



4 Next Steps and Recommendations

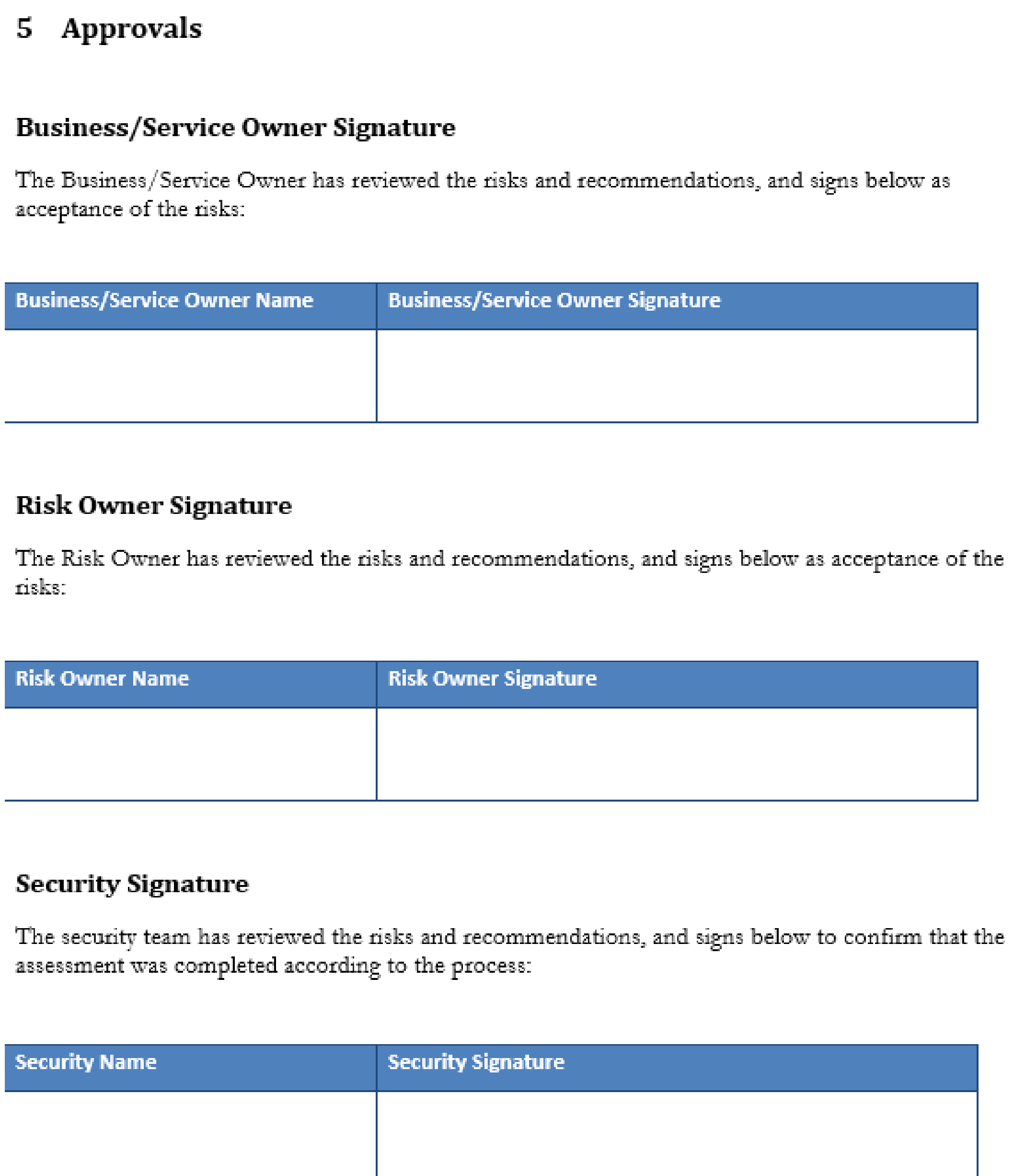
Identify Actions

ID	Action	Vulner-ability	Threat	Risk	Owner	Due Date
A1	Example	V1, V3	-	R2	J. Doe	2017-01
A2	Example	V2	T1	-	J. Doe	2017-03
A3						
A4						
A5						
A6						

Risk Assessment Sections (Sample)

- Approvals
  - Business/Service Owner Signature
  - Risk Owner Signature
  - Security Signature
- this is a good example of “conscious acceptance of risk”
- the responsible individuals are aware of the risks and decide what to do with them
- business does not transfer risk to security

University of Victoria



5 Approvals

Business/Service Owner Signature

The Business/Service Owner has reviewed the risks and recommendations, and signs below as acceptance of the risks:

Business/Service Owner Name	Business/Service Owner Signature

Risk Owner Signature

The Risk Owner has reviewed the risks and recommendations, and signs below as acceptance of the risks:

Risk Owner Name	Risk Owner Signature

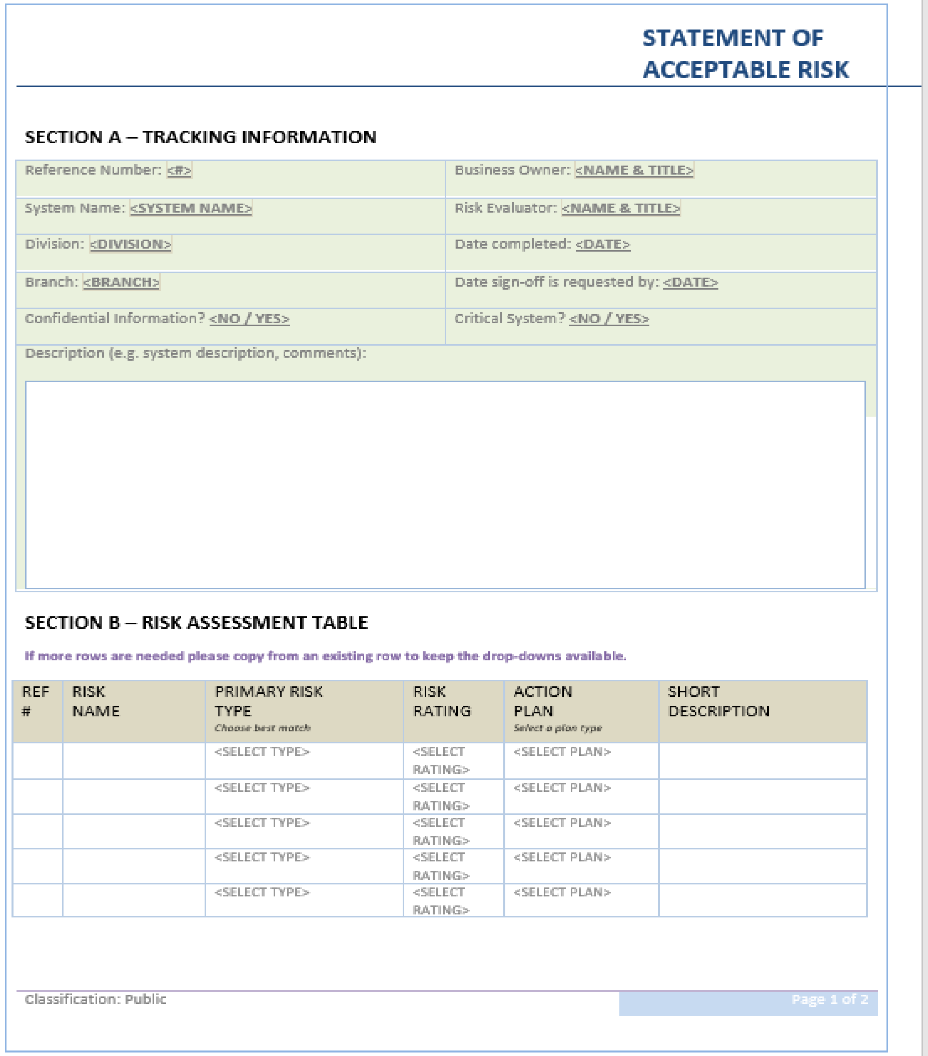
Security Signature

The security team has reviewed the risks and recommendations, and signs below to confirm that the assessment was completed according to the process:

Security Name	Security Signature

Risk Assessments

- Statement of Acceptable Risk (SoAR)



STATEMENT OF ACCEPTABLE RISK

SECTION A – TRACKING INFORMATION

Reference Number: <#>	Business Owner: <NAME & TITLE>
System Name: <SYSTEM NAME>	Risk Evaluator: <NAME & TITLE>
Division: <DIVISION>	Date completed: <DATE>
Branch: <BRANCH>	Date sign-off is requested by: <DATE>
Confidential Information? <NO / YES>	Critical System? <NO / YES>
Description (e.g. system description, comments):	

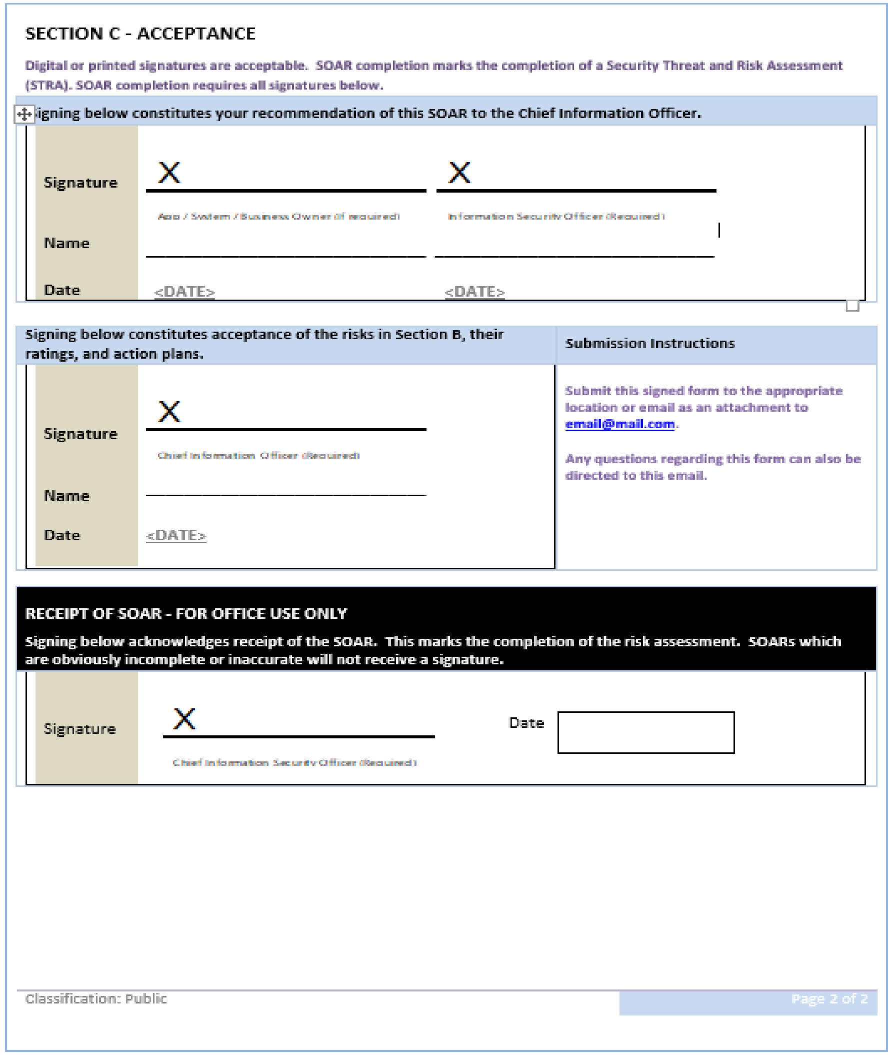
SECTION B – RISK ASSESSMENT TABLE

If more rows are needed please copy from an existing row to keep the drop-downs available.

REF #	RISK NAME	PRIMARY RISK TYPE *Choose best match*	RISK RATING	ACTION PLAN *Select a plan type*	SHORT DESCRIPTION
		<SELECT TYPE>	<SELECT RATING>	<SELECT PLAN>	
		<SELECT TYPE>	<SELECT RATING>	<SELECT PLAN>	
		<SELECT TYPE>	<SELECT RATING>	<SELECT PLAN>	
		<SELECT TYPE>	<SELECT RATING>	<SELECT PLAN>	
		<SELECT TYPE>	<SELECT RATING>	<SELECT PLAN>	

Classification: Public

Page 1 of 2



SECTION C - ACCEPTANCE

Digital or printed signatures are acceptable. SOAR completion marks the completion of a Security Threat and Risk Assessment (STRA). SOAR completion requires all signatures below.

Signing below constitutes your recommendation of this SOAR to the Chief Information Officer.

Signature	X ______________________ App / System / Business Owner (if required)	X ______________________ Information Security Officer (Required)
Name	______________________	______________________
Date	<DATE>	<DATE>

Signing below constitutes acceptance of the risks in Section B, their ratings, and action plans.		Submission Instructions
Signature	X ______________________ Chief Information Officer (Required)	Submit this signed form to the appropriate location or email as an attachment to email@mail.com. Any questions regarding this form can also be directed to this email.
Name	______________________	
Date	<DATE>	

RECEIPT OF SOAR - FOR OFFICE USE ONLY

Signing below acknowledges receipt of the SOAR. This marks the completion of the risk assessment. SOARs which are obviously incomplete or inaccurate will not receive a signature.

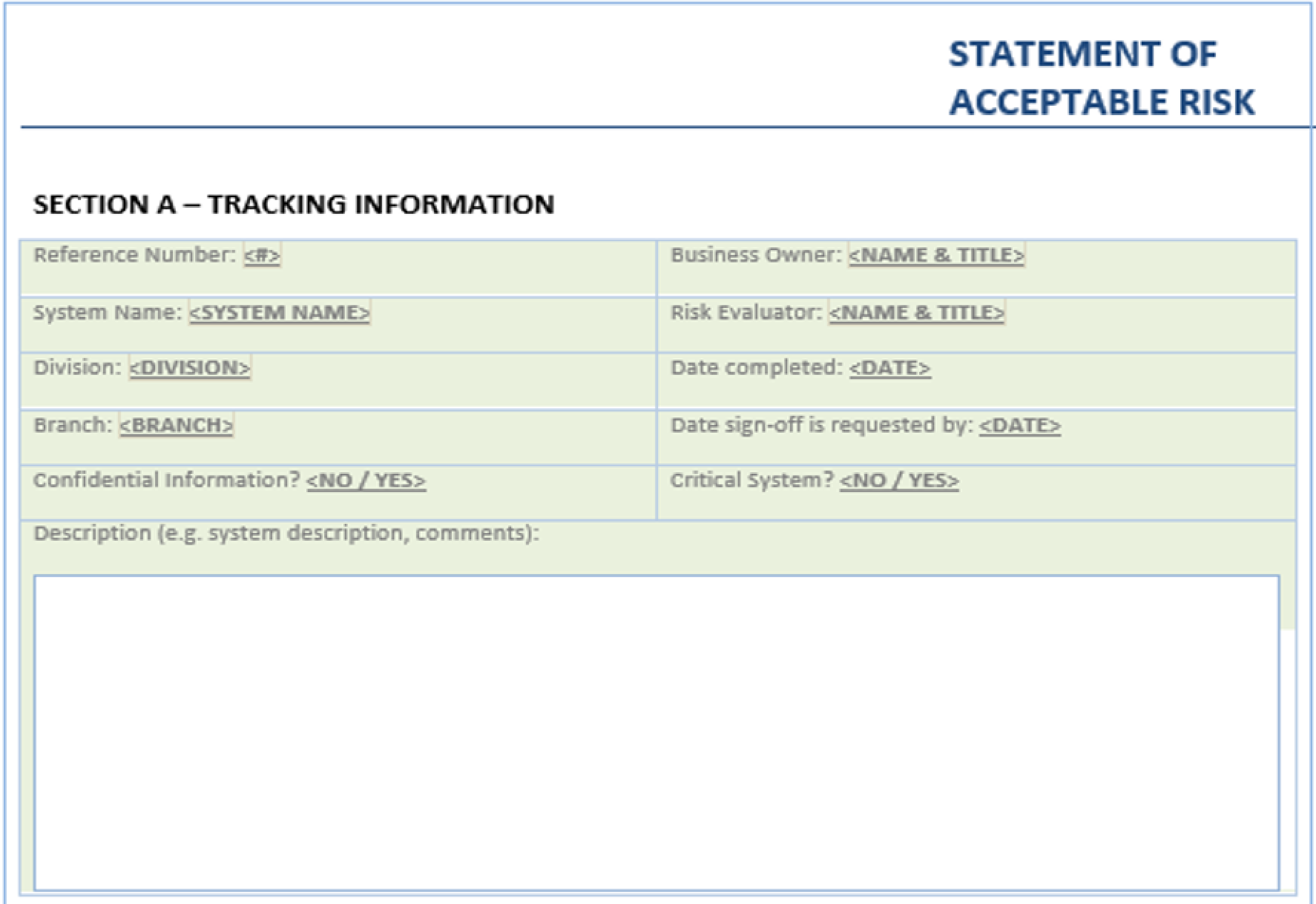
Signature	X ______________________ Chief Information Security Officer (Required)	Date	

Classification: Public

Page 2 of 2

Risk Assessments

- Statement of Acceptable Risk (SoAR)



STATEMENT OF ACCEPTABLE RISK

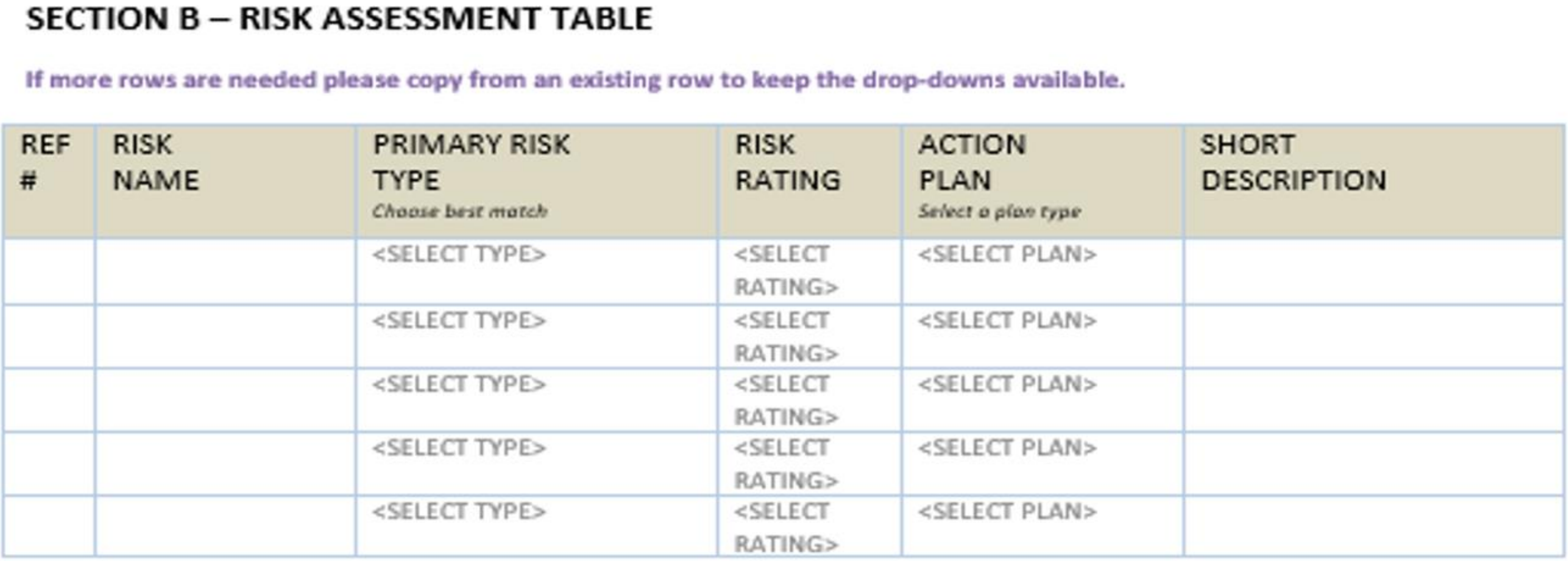
SECTION A – TRACKING INFORMATION

Reference Number: <#>	Business Owner: <NAME & TITLE>
System Name: <SYSTEM NAME>	Risk Evaluator: <NAME & TITLE>
Division: <DIVISION>	Date completed: <DATE>
Branch: <BRANCH>	Date sign-off is requested by: <DATE>
Confidential Information? <NO / YES>	Critical System? <NO / YES>
Description (e.g. system description, comments):	

University of Victoria

Risk Assessments

- Statement of Acceptable Risk (SoAR)



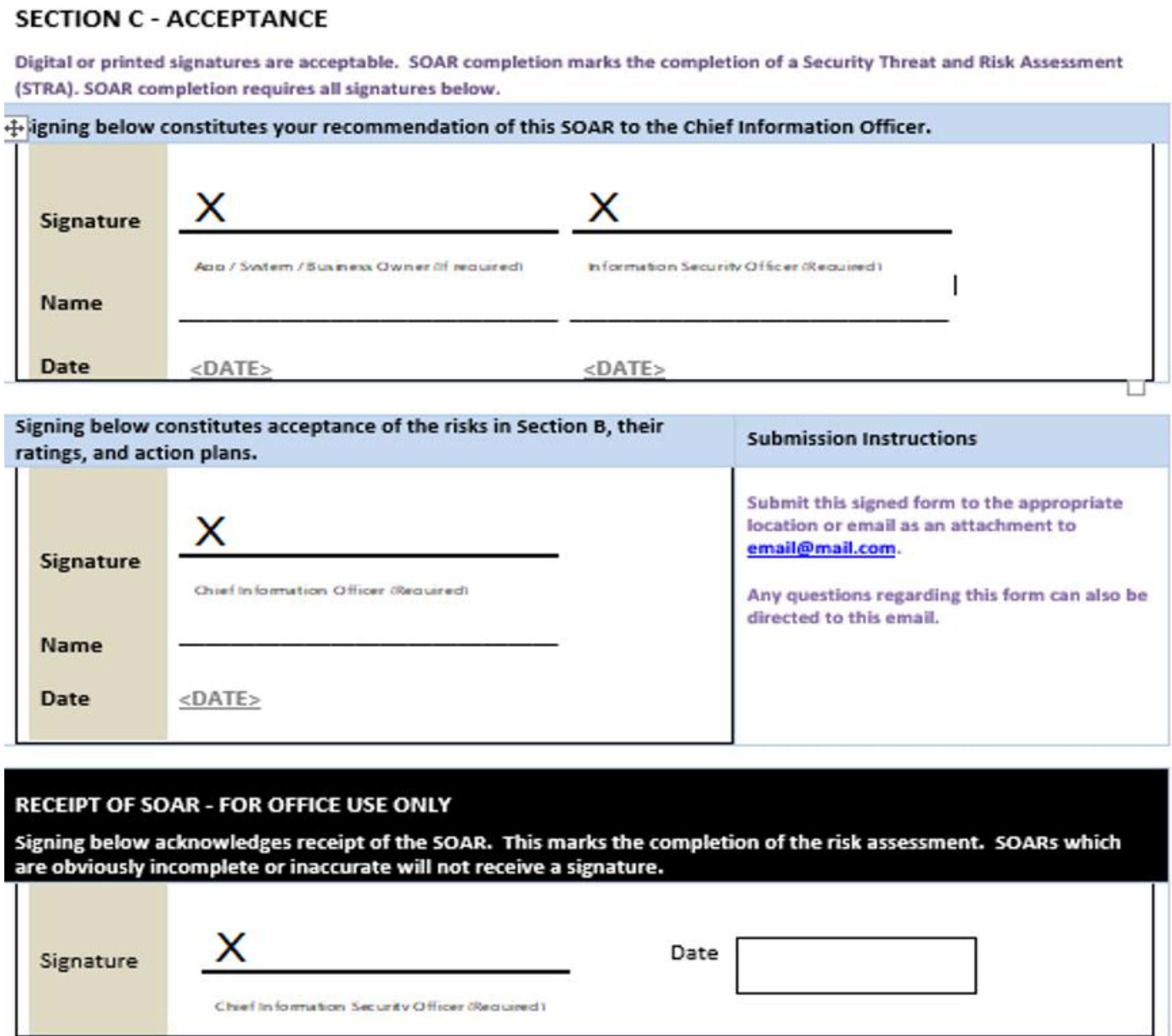
SECTION B – RISK ASSESSMENT TABLE

If more rows are needed please copy from an existing row to keep the drop-downs available.

REF #	RISK NAME	PRIMARY RISK TYPE *Choose best match*	RISK RATING	ACTION PLAN *Select a plan type*	SHORT DESCRIPTION
		<SELECT TYPE>	<SELECT RATING>	<SELECT PLAN>	
		<SELECT TYPE>	<SELECT RATING>	<SELECT PLAN>	
		<SELECT TYPE>	<SELECT RATING>	<SELECT PLAN>	
		<SELECT TYPE>	<SELECT RATING>	<SELECT PLAN>	
		<SELECT TYPE>	<SELECT RATING>	<SELECT PLAN>	

Risk Assessments

- Statement of Acceptable Risk (SoAR)



SECTION C - ACCEPTANCE

Digital or printed signatures are acceptable. SOAR completion marks the completion of a Security Threat and Risk Assessment (STRA). SOAR completion requires all signatures below.

Signing below constitutes your recommendation of this SOAR to the Chief Information Officer.

Signature	X ______________________ App / System / Business Owner (If required)	X ______________________ Information Security Officer (Required)
Name	______________________	______________________
Date	<DATE>	<DATE>

Signing below constitutes acceptance of the risks in Section B, their ratings, and action plans.

Signature	X ______________________ Chief Information Officer (Required)
Name	______________________
Date	<DATE>

Submission Instructions

Submit this signed form to the appropriate location or email as an attachment to email@mail.com.

Any questions regarding this form can also be directed to this email.

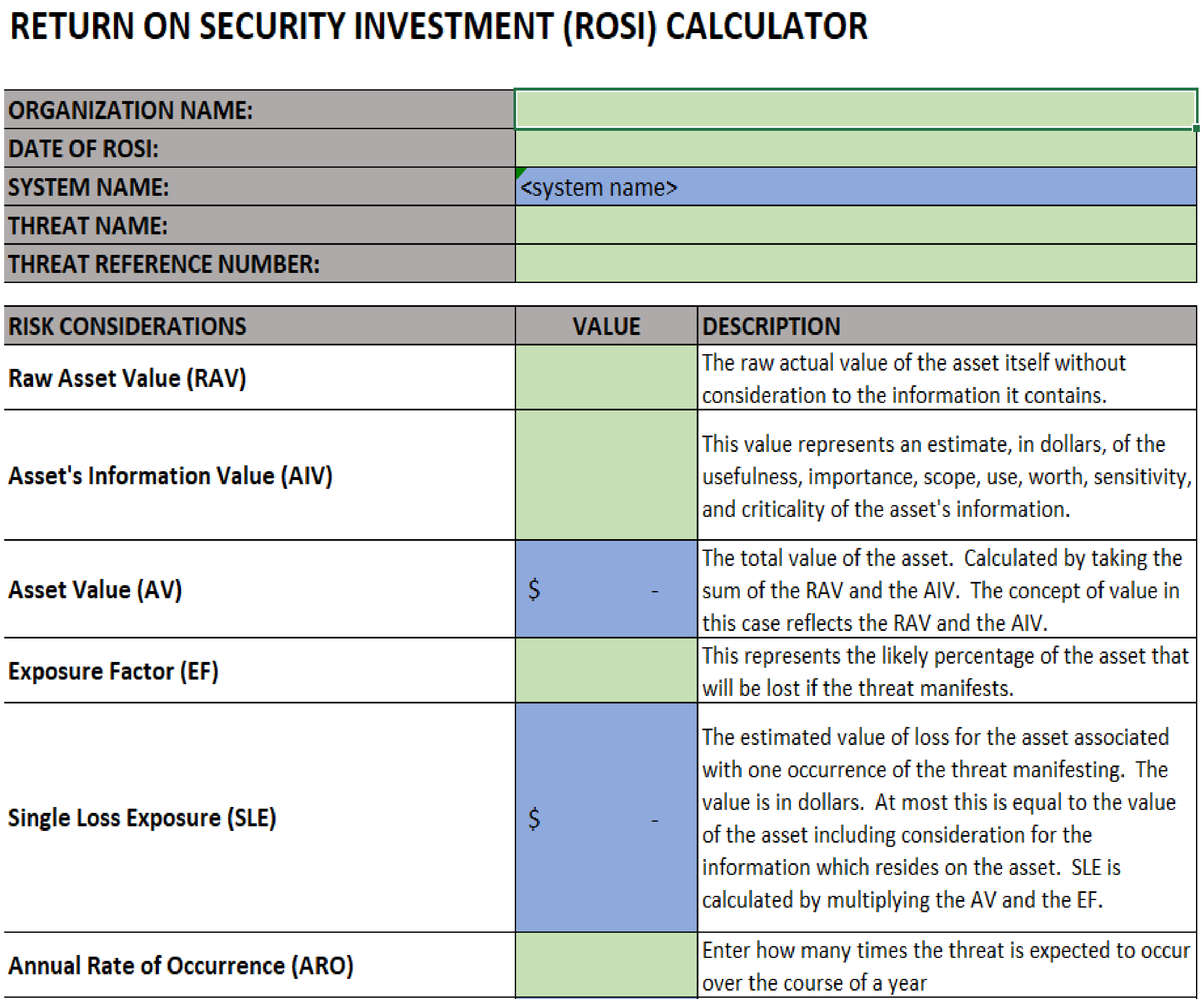
RECEIPT OF SOAR - FOR OFFICE USE ONLY

Signing below acknowledges receipt of the SOAR. This marks the completion of the risk assessment. SOARs which are obviously incomplete or inaccurate will not receive a signature.

Signature	X ______________________ Chief Information Security Officer (Required)	Date	

University of Victoria

Return on Security Investment (ROSI)



RETURN ON SECURITY INVESTMENT (ROSI) CALCULATOR

ORGANIZATION NAME:	
DATE OF ROSI:	
SYSTEM NAME:	<system name>
THREAT NAME:	
THREAT REFERENCE NUMBER:	

RISK CONSIDERATIONS	VALUE	DESCRIPTION
Raw Asset Value (RAV)		The raw actual value of the asset itself without consideration to the information it contains.
Asset's Information Value (AIV)		This value represents an estimate, in dollars, of the usefulness, importance, scope, use, worth, sensitivity, and criticality of the asset's information.
Asset Value (AV)	$ -	The total value of the asset. Calculated by taking the sum of the RAV and the AIV. The concept of value in this case reflects the RAV and the AIV.
Exposure Factor (EF)		This represents the likely percentage of the asset that will be lost if the threat manifests.
Single Loss Exposure (SLE)	$ -	The estimated value of loss for the asset associated with one occurrence of the threat manifesting. The value is in dollars. At most this is equal to the value of the asset including consideration for the information which resides on the asset. SLE is calculated by multiplying the AV and the EF.
Annual Rate of Occurrence (ARO)		Enter how many times the threat is expected to occur over the course of a year

This statement addresses the DDoS (12345) threat. Annually UBC sustains approximately 4 incidents resulting in a 50 percent loss of the website asset's value on each occurrence. Considering the raw asset and the information it contains, we estimate that each incident costs approximately $505000 in losses. Therefor, the predicted cost for all losses annually related to this threat is $2020000. We expect to be able to mitigate 25 percent of the risk this year at a cost of $50000 to treat. This will reduce the value of the risk exposure by $505000. The value of the remaining residual risk will be $1515000. This represents a Return on Security Investment of 658 percent. Considering the treatment solution cost, this is a good investment. The selected treatment is likely appropriate.

Threat Modelling

- way to identify threats, visualize, understand security

1) defining security requirements/security objectives
2) identify assets and dependencies

   - visualize/diagram

3) identify trust zones
4) identify threats/vulnerabilities
5) document threat model

what are the threats
who is orchestrating them
why are they doing it
what can you do to prevent

is that sufficient to mitigate
risk to an acceptable level

STRIDE model of threats

NOT TESTED

Threat	Property	Mitigation
Spoofing Identity (impersonating someone or something else)	Authentication	passwords, MFA, digital signatures
Tampering with Data (changing information)	Integrity	access controls/permissions, digital signatures
Repudiation (claiming to have not done something)	Non-repudiation	logging, auditing, digital signatures
Information Disclosure (unauthorized exposure of info)	Confidentiality	encryption, information classification
Denial of Service (deny or degrade service)	Availability	patching, WAF, IPS
Elevation of Privilege (user increases their access without authorization)	Authorization	access control/permissions, logging, alerting

Vulnerabilities

- common vulnerabilities:
    - weak encryption, buffer overflows, lack of input validation, SQL injections, Cross Site Scripting (XSS), broken authentication or session management, misconfiguration…

Supply Chain,
Third Parties

Vendor Security

- not enough for your organization to have adequate security
- if you rely on other organizations they may pose a risk to yours
- important to ensure the organization is good to do business with
- they may not be capable of protecting your organization
- important to ensure have a contract in place
  - with acceptable contract terms
  - with ‘teeth’ – penalties if they are violated
- consider whether you can afford to audit/check for compliance
  - third party assessment and monitoring
- applying risk-based management concepts to the supply chain

University of Victoria

Vendor Security Requirements

1. **<u>Access control</u>**

The vendor **must / should:**

(a) implement an access control policy and associated access control procedures that address, without limitation, onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges and inactivity timeouts;

(b) document, follow, review, and update the vendor’s access control policies and procedures at least every three years;

(c) ensure that all access to information and system functions is based on principles of “least privilege” and “need to know”, and that employees, contractors or vendors are provided only with the access they are authorized to have in accordance with such principles;

(d) identify and segregate conflicting duties and areas of responsibility to reduce incidents of fraud and other abuse (e.g. separation of duties);

(e) review and update the current access control policy at least every three years;

(f) review and update the current access control procedures at least annually;

University of Victoria

Vendor Security Requirements

SECURITY SCHEDULE
February 2020
If a provision of the main body of the Agreement conflicts with a provision of this Schedule, then unless expressly stated otherwise within the Agreement, the provision of this Schedule will prevail to the extent of such conflict.

1 Definitions

In this Schedule,

(a) “**Cloud Services**” means services made available to users on demand via the Internet that are characterised by resource pooling, rapid elasticity and measured services with broad network access. Cloud Services include Software as a Service, Platform as a Service and Infrastructure as a Service, as such terms are understood pursuant to definitions provided by the National Institute of Standards and Technology (NIST).

(b) “**Industry Best Practice**” means best practices commonly recognized in the IT industry from time to time and applicable to the protection and security of sensitive information of a nature similar to Protected Information against unauthorised access, disclosure or use, or any unauthorized attempts to access, disclose or use such information.

(c) “**Protected Information**” means any and all of:

i. “personal information” as defined in the *Freedom of Information and Protection of Privacy Act,* British Columbia;
ii. information and records of information the Contractor is required to treat as confidential under the Agreement; and
iii. records, the integrity or availability of which are to be preserved by the Contractor under this Agreement, which in the case of records not falling within (i) or (ii), are marked by the Province as “Protected Information” or
the Province otherwise instructs the Contractor that the record is “Protected Information” under the Agreement.

(d) “Province Information” means information of the Province, including without limitation any Protected Information, that is disclosed to the Contractor, accessed by the Contractor or collected by the Contractor in relation to the Services and includes any information derived therefrom.

(e) “Services” means the services provided by the Contractor to the Province under the Agreement and includes, if applicable, any Cloud Services.

(f) “Systems” means any systems, subsystems, equipment, devices, infrastructure, networks, hardware and software used in connection with the Services, including for managing, operating or providing the Services.

University of Victoria

Vendor Security Requirements

2 Applicability
For greater clarity, unless otherwise specified in the Agreement, the terms and conditions of this Schedule apply to the provision of all Services by the Contractor, its subcontractors and their respective personnel. Any reference to Contractor herein will include all subcontractors, Contractor personnel and subcontractor personnel, as applicable.

3 Industry Best Practice
The Contractor must have in place and maintain security controls to protect Protected Information that conform to commonly accepted industry norms that a prudent operator providing similar services would have implemented. Without limitation, the Contractor will perform its obligations under this Schedule in a manner that best conforms to Industry Best Practice.

4 Compliance and Certifications
Compliance and certification requirements will depend on the type of service provided by the Contractor.
(a) For Cloud Services, the Contractor must at all times satisfy at least one of the following security standards:
i. compliance requirements identified for a Cloud Service Provider, in the Government of Canada Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM); or
ii. compliance requirements identified for a Cloud Service Provider, in the US Federal Risk and Authorization Management Program (FedRAMP) for moderate impact information systems; or
iii. certification with ISO/IEC 27001 based on requirements for a Cloud Service Provider controls in ISO/IEC 27017:2015; or
iv. certification with Cloud Security Alliance (CSA) – Level 2 CSA STAR;
(b) For all other Services that are not cloud services, the Contractor must satisfy:
i. certification with ISO/IEC 27001 based on requirements for Information Technology controls in ISO/IEC 27002:2013; or
ii. applicable Province IM/IT standards accessible at
https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards

University
of Victoria

Vendor Security Requirements

5 Attestation of Compliance and Certification of Services

To verify compliance with, as applicable, section 4(a) (with respect to Cloud Services) or 4(b) (with respect to non-Cloud Services), the Contractor must provide the Province with satisfactory evidence, by way of independent third-party attestation from a reputable information systems auditor, that any Services provided by the Contractor or used by the Contractor in connection with the Services satisfy and comply with at least one of the security standards set forth in, as applicable, section 4(a) (with respect to Cloud Services) or 4(b) (with respect to non-Cloud Services).

6 Access Control

With respect to the access, by any Contractor personnel, to any part of the Contractor's Systems that may contain Province Information, the Contractor must:

(a) implement access control policies and procedures that address onboarding, off-boarding, transition between roles, regular access reviews, limitations and usage control of administrator privileges, and inactivity timeouts;

(b) identify and segregate conflicting duties and areas of responsibility, such as separation of duties;

(c) maintain a current and accurate inventory of computer accounts;

(d) review the inventory of computer accounts on a regular basis to identify dormant, fictitious or unused accounts;

(e) enforce principles of "least privilege" and "need to know";

(f) review user access rights on a regular basis to identify excessive privileges;

(g) enforce a limit of logon attempts and concurrent sessions.

Vendor Security Requirements

8 Security Awareness

(a) The Contractor must ensure that all persons employed or retained to perform the Services receive security awareness training, annually and supervision at a level and in substance that is appropriate to that person’s position and the Contractor’s obligations under this Schedule.

(b) The Contractor must not permit any person the Contractor hires or uses to access or obtain any Protected Information unless that person is contractually bound to the Contractor in writing to keep Protected Information confidential on terms no less protective than the terms applicable to the Contractor under the Agreement.

9 Log Generation and Retention

The Contractor must:

(a) generate and retain logs that are sufficiently detailed to determine who did what and when for a period of 90 days online;

(b) provide real time access to logs;

(c) provide the technical capability to forward the logs to the Province; and

(d) correlate, monitor, and alert on logs.

10 Investigations Support and Security Investigations

The Contractor must:

(a) retain investigation reports related to a security investigation for a period of 2 years after the investigation is completed or provide to the Province for retention;

(b) provide reasonable investigative support to the Province;

(c) maintain chain of custody for evidence;

(d) support e-discovery; and

(e) maintain legal holds to meet needs of investigations and judicial requests.

Vendor Security Requirements

11 Network Time Protocol
Systems used by the Contractor or any subcontractor in the provision of Services must synchronise time with a stratum-2 (or higher time) reliable source.

12 Vulnerability Scan/Penetration Testing
The Contractor must conduct regular:
(a) vulnerability scans;
(b) web application scans; and
(c) penetration tests.

13 Configuration and Patch Management
The Contractor must:
(a) have an information security policy based on recognized industry standards;
(b) apply system hardening methods in securing Contractor Systems;
(c) logically isolate and encrypt Province Information;
(d) ensure workstations and servers used in management and provisioning of the Services are patched and secured with anti-malware protection;
(e) remedy vulnerabilities in a timely manner according to criticality;
(f) patch all systems and software regularly according to industry best practices; and
(g) use secure coding practices when developing applications and application programming interfaces.

Vendor Security Requirements

14 Business Continuity, Disaster Recovery, and Backup Plans

The Contractor must:

(a) have a business continuity plan and a disaster recovery plan;
(b) conduct backups of critical data; and
(c) review and test business continuity, disaster recovery, and backup plans and procedures regularly.

15 Incident Response and Management

The Contractor must:

(a) have an incident management plan and an incident response plan; and
(b) review and test both incident management and incident response plans annually.

16 Notifications of Breaches

The Contractor must notify the Province within 24 hours of the Contractor’s identification of a breach or incident that has affected, or may affect, Province Information.

17 Notifications of Changes

The Contractor must notify the Province of any changes to the Contractor’s security policies, procedures or agreements that may materially lower the security of Province Information.

18 Asset Management and Disposal

The Contractor must

(a) maintain an inventory of Province Information assets;
(b) use secure methods when disposing of Province Information Assets, and
(c) maintain records of Province Information asset disposals.

Vendor Security Requirements

19 Physical Security

The Contractor must:

(a) develop, document, and disseminate a physical and environmental protection policy;

(b) regularly review and update its current physical and environmental protection policy and procedures; and

(c) review physical access logs at least once monthly.

20 Threat and Risk Assessments

The Contractor must:

(a) conduct threat and risk assessments on any part of the Contractor's Systems that is new, or has been materially changed since the last threat and risk assessment was conducted; and

(b) support the Province in completing Security Threat and Risk Assessments.

21 Security Screening

The Contractor must:

(a) screen all Contractor personnel prior to Contractor authorizing access to Province or Contractor Systems;

(b) conduct criminal record checks on all Contractor personnel who have access to any Province or Contractor Systems;

(c) make a reasonable determination of whether the individual constitutes an unreasonable security risk taking into consideration the duties of the individual, the type and sensitivity of information to which the individual may be exposed, and all applicable laws; and

(d) require all Contractor personnel to proactively disclose criminal offences to the Contractor unless prohibited by applicable law.

Vendor Security Requirements

22 Supply Chain

The Contractor must ensure that its suppliers and subcontractors involved in the provision of Services meet or exceed the standards set forth in this Schedule.

23 Encryption

The Contractor must:

(a) implement and maintain encryption of Province Information while at rest and in transit;

(b) offer the Province the technical capability of cryptographic key management to allow the Province to manage encryption keys in relation to Province Information at rest and in transit;

(c) not hold or have access to encryption keys if such encryption keys are managed by the Province to encrypt Province information at rest or in transit; and

(d) not provide encryption keys used to secure Province Information to a third party or the ability to break such encryption.

24 Isolation Controls and Logical Isolation of Data

The Contractor must:

(a) implement and maintain the logical isolation of Province Information, even in the case of equipment or technology failure;

(b) implement, where supported by available technology, the logical isolation of audit records related to Province Information and activities, even in the case of equipment or technology failure; segregate tenancy traffic from management network traffic; and

(c) not use Protected Information for test or development purposes without the written approval of the Province.

Vendor Security Requirements

25 Technical Controls

The Contractor must:

(a) implement firewalls, web application firewalls, distributed denial of service, and intrusion prevention systems to control traffic flow to and from the Contractor's Systems; and

(b) secure remote access to the Contractor's Systems by Contractor personnel and contractors.

26 Use of Province Systems

Use of Province Systems by the Contractor or its personnel (including subcontractors) must be restricted to activities necessary for provision of the Services. The Province reserves the right to not make any particular Province facility, system, network or device available to the Contractor unless the Contractor or its individual personnel (as applicable) agree to any additional terms and conditions acceptable to the Province.

27 Security Contact

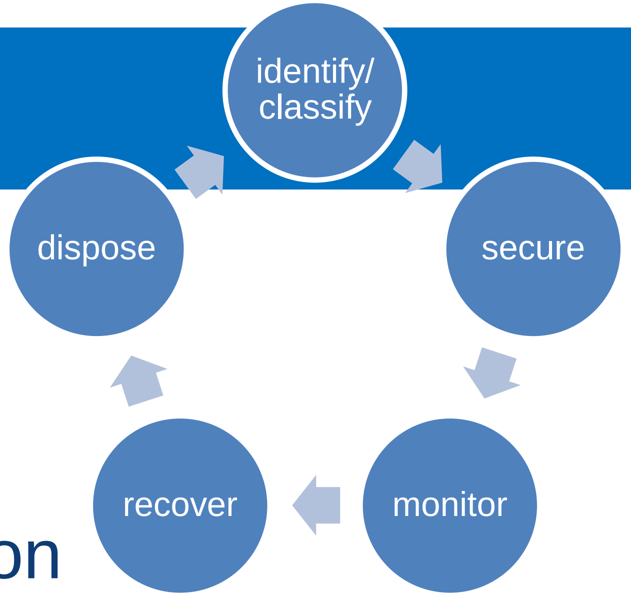
If not set out elsewhere in the Agreement, the Contractor must provide the contact information for the individual who will coordinate compliance by the Contractor on matters relating to this Schedule.

Vendor Security Requirements Summary

Standards: vendor must ensure that they are compliant with a widely adopted, acceptable security standard.
Compliance: (a)vendor must ensure it can demonstrate compliance with a security standard by way of an annual SOC 2 Type II audit conducted by an independent third-party auditor. (b)vendor must demonstrate compliance with security obligations if they are not covered anywhere else.
Access Control: (a)vendor must implement an access control policy and procedures that address onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges and inactivity timeouts. (b)vendor must identify and segregate conflicting duties and areas of responsibility (e.g.. separation of duties). (c)vendor must maintain a current and accurate inventory of computer accounts and (d)review the inventory on a regular basis to identify dormant, fictitious or unused accounts. (e)vendor must enforce a limit of logon attempts and (f)concurrent sessions as well as (g)multi-factor authentication for privileged access.
Passwords: (a)vendor must enforce password length, complexity, and history for password-based authentication. (b)vendor must support multi-factor authentication. (c)vendor must support single sign-on technologies for authentication.
Awareness: vendor must ensure that it conducts security awareness and training for employees.
Logging: (a)vendor must retain logs that are sufficiently detailed to determine who did what when for a period of 90 days online. (b)vendor must provide online access to logs. (c)vendor must provide the technical capability to forward the logs. (d) vendor must correlate, monitor, and alert on logs.
Investigations: (a)vendor must retain investigation reports related to a security investigation for a period of 2 years after the investigation is completed. (b)vendor must provide adequate investigative support. (c)vendor must support e-discovery and legal holds to meet needs of investigations and judicial requests.
Time: vendor must ensure that infrastructure is synchronized with Stratum 1 time servers.
Change Control: (a)vendor must implement change controls in accordance with reasonable industry practices. (b)vendor must test changes to the environment as part of the change management process. (c)vendor must not utilize production data in test environments.
Configuration/Patch Management/Best Practices: (a)vendor must have an information security policy based on industry best practices. (b)vendor must harden systems and servers using appropriate industry standards. (c)vendor must secure databases using appropriate industry standards and logically isolate and encrypt information. (d)vendor must ensure workstations used in management and provisioning are patched and (e)secured with antivirus. (f)vendor must implement physical security according to industry best practices. (g)vendor must remedy vulnerabilities and patches according to criticality. (h)vendor must ensure that applications and programming interfaces are developed according to industry standards.
BCP/DRP: (a)vendor must have a business continuity plan and a disaster recovery plan that are reviewed and tested annually. (b)vendor must conduct backups using appropriate industry standards.(c)vendor must have incident management and incident response plans that are reviewed and tested annually.
Asset Disposal: vendor must dispose of assets according to industry best practices.
Threat/Risk Assessments: (a)vendor must conduct threat and risk assessments on new systems or material changes to existing ones. (b)vendor must support in completing Security Threat and Risk Assessments (STRAs).
Security Testing: (a)vendor must conduct vulnerability scans for new systems and material changes to existing ones. (b)vendor must conduct web app vulnerability scans for new systems and material changes to existing ones. (c)vendor must conduct penetration tests at least annually.
Security Screening: (a)vendor must screen individuals prior to authorizing access to information systems. (b)vendor must conduct criminal record checks on employees.
Supply Chain: vendor must ensure suppliers and contractors meet or exceed vendor's own security policies.
Encryption: (a)vendor must implement encryption of data in transit and at rest for information and(b) provide the technical capability to manage encryption keys.
Logical Separation: (a)vendor must logically isolate information and segregate traffic from other tenants and management traffic. (b)vendor must implement security devices between zones.
Technical Controls: (a)vendor must implement firewalls and intrusion prevention. (b) vendor must implement application layer firewalls.(c) vendor must enable/configure security controls in the tenancy such as firewall, intrusion prevention, antivirus, and encryption (IaaS). (d)vendor must secure remote access according to industry best practices. (e)vendor must implement distributed denial of service attack protection.
Breach Notification:(a) vendor must notify within 24 hours of a potential or actual breach or incident that may affect the information.(b) vendor must notify of any changes to security policies, procedures or agreements.

Asset Management & Information Security Classification

Asset Management



- asset lifecycle

1) identify/classify	info created or collected
2) secure	secured based on value/classification
3) monitor	monitor asset for changes that impact protection
4) recover	be able to recover from changes (e.g. backups)
5) dispose	
- archive	store it
- defensible destruction	destroy the right things in right way

Asset Management

- asset commissioning
  - have a definition of asset, asset classification
  - have policies that say what you track, asset inventory, asset ownership, asset retention
- asset decommissioning
  - have policies that say what you do with assets when it’s time to get rid of
- reverse logistics
  - process to harvest value out of products or final disposal

Asset Management

NIST Cybersecurity Framework

Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried
	ID.AM-2: Software platforms and applications within the organization are inventoried
	ID.AM-3: Organizational communication and data flows are mapped
	ID.AM-4: External information systems are catalogued
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

University of Victoria

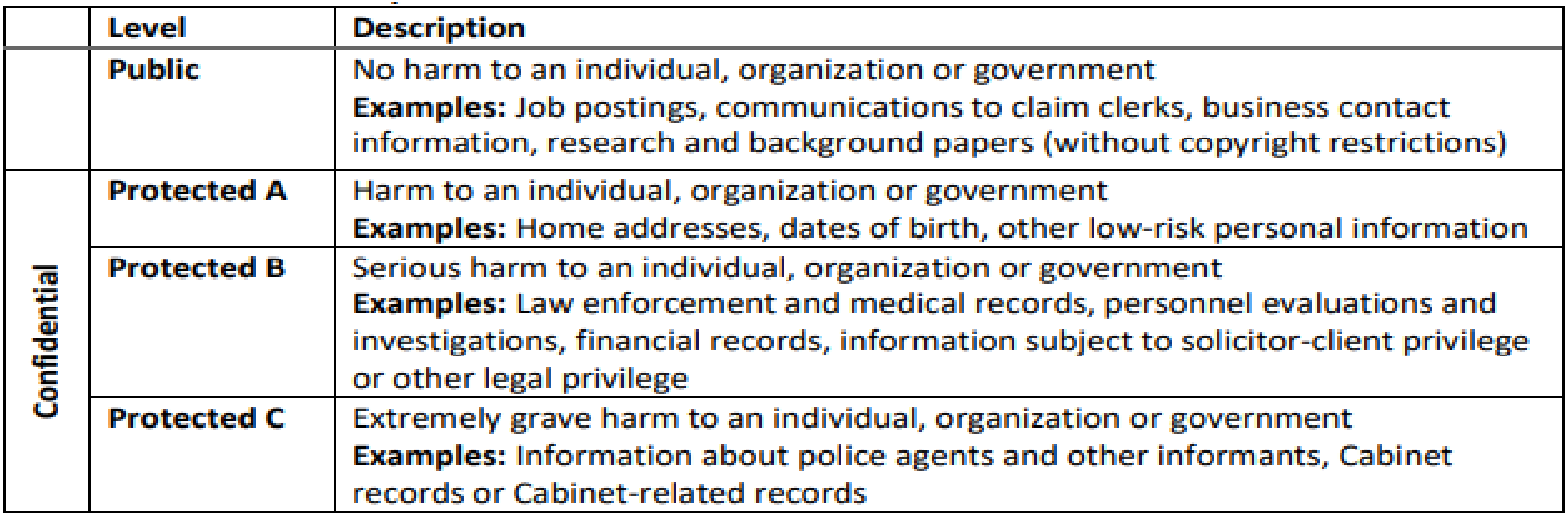
Asset Management

- fields in asset management system (basic)
  - asset name/hostname, serial #, location, IP address, owner, criticality, what does it do

Host	IP address	Serial #	Make/Model	Location	Owner	Criticality	Purpose

Information Classification

- different labels and effectiveness
  - low/med/high, 1/2/3, a/b/c
  - private, confidential, top secret, sensitive



	Level	Description
	Public	No harm to an individual, organization or government **Examples:** Job postings, communications to claim clerks, business contact information, research and background papers (without copyright restrictions)
Confidential	**Protected A**	Harm to an individual, organization or government **Examples:** Home addresses, dates of birth, other low-risk personal information
	Protected B	Serious harm to an individual, organization or government **Examples:** Law enforcement and medical records, personnel evaluations and investigations, financial records, information subject to solicitor-client privilege or other legal privilege
	Protected C	Extremely grave harm to an individual, organization or government **Examples:** Information about police agents and other informants, Cabinet records or Cabinet-related records

Information Classification

- information classification determines required privacy and security controls
  - data ownership: have legal rights over the data, authority to make decisions
  - data stewardship: responsible for quality of the data
  - data custodians: taking care of data, preventing issues

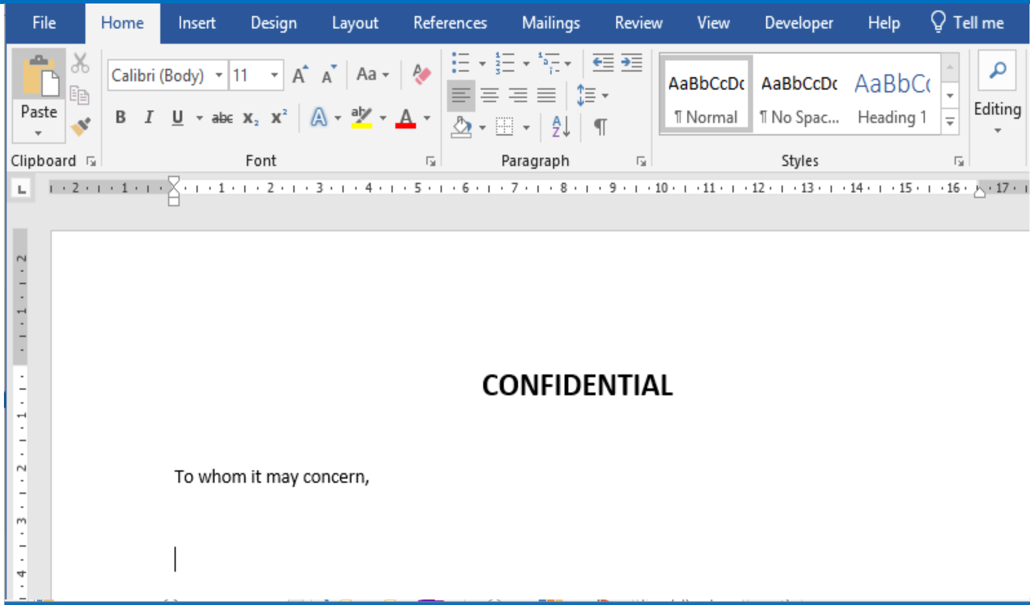
other names:

  - data controller dictates how and why data will be used by the organization
  - data processor processes any data given by data controller

…need to protect sensitive data at rest and data in transit… often but not always through encryption…

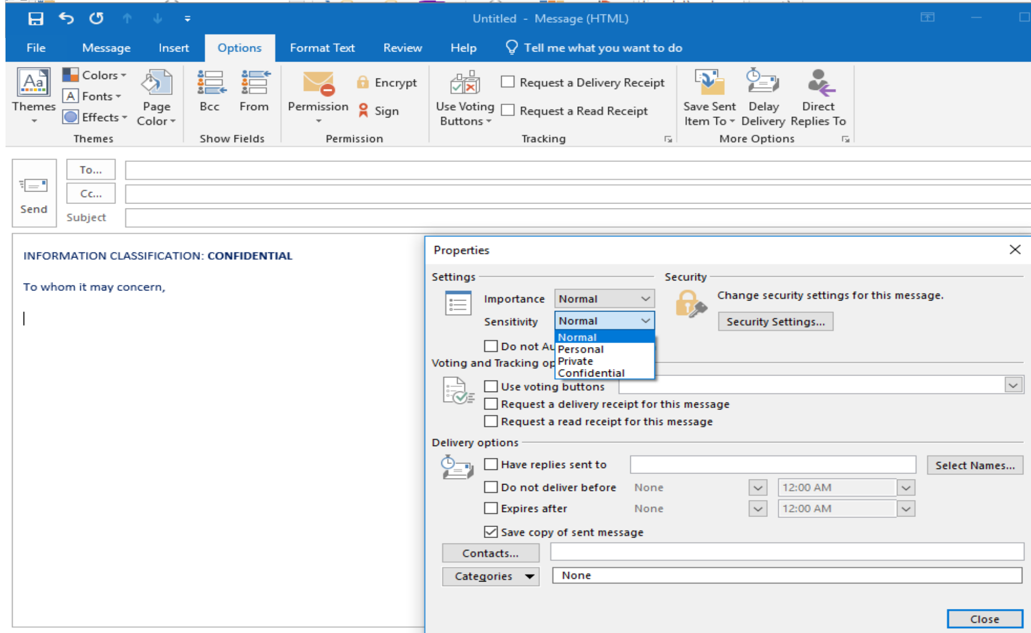
Information Classification

- labelling
  - manual or automatic
- office productivity
- email
- virtualization
  - remote views into data
- digital rights management



CONFIDENTIAL

To whom it may concern,



INFORMATION CLASSIFICATION: CONFIDENTIAL

To whom it may concern,

Properties

Settings

Importance: Normal

Sensitivity: Normal

Normal
Personal
Private
Confidential

□ Do not Au

Security

Change security settings for this message.

Security Settings...

Voting and Tracking op

□ Use voting buttons

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Delivery options

□ Have replies sent to — Select Names...

□ Do not deliver before: None — 12:00 AM

□ Expires after: None — 12:00 AM

☑ Save copy of sent message

Contacts...

Categories: None

Close

University of Victoria

Protection/tracking of Information

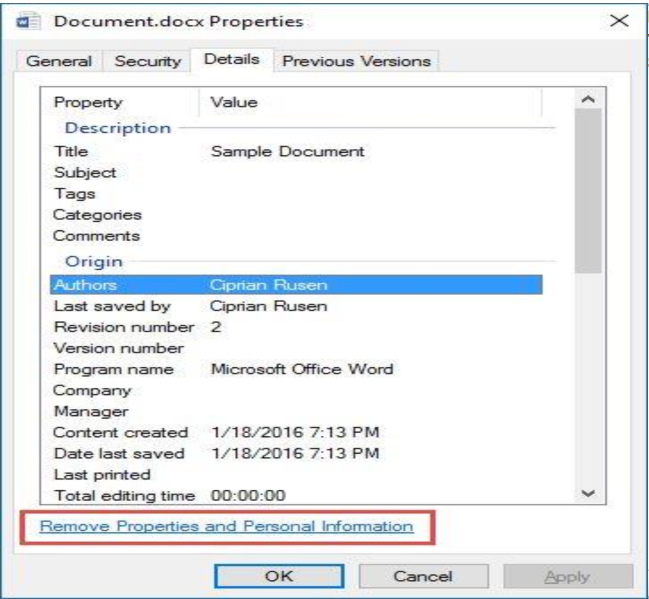
- identify your crown jewels, ensure they benefit from adequate protection otherwise end up as a headline

- techniques to mark files:

meta-tagging

beaconing, email pixel tracking

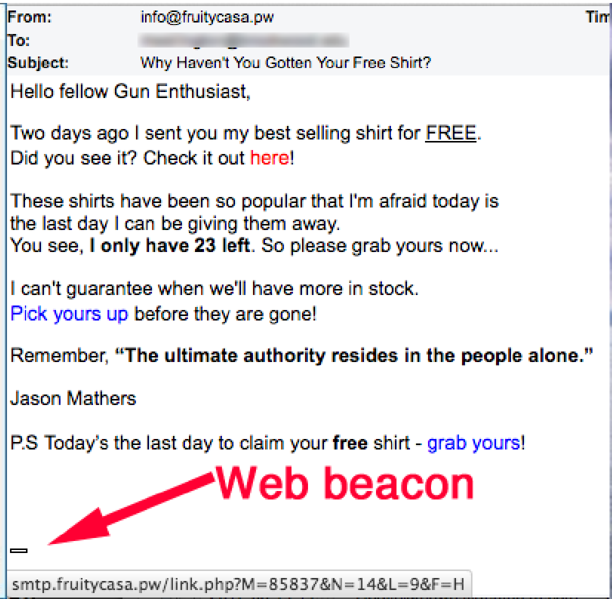
watermarking



Document.docx Properties

Property	Value
Description	
Title	Sample Document
Subject	
Tags	
Categories	
Comments	
Origin	
Authors	Ciprian Rusen
Last saved by	Ciprian Rusen
Revision number	2
Version number	
Program name	Microsoft Office Word
Company	
Manager	
Content created	1/18/2016 7:13 PM
Date last saved	1/18/2016 7:13 PM
Last printed	
Total editing time	00:00:00

Remove Properties and Personal Information



From: info@fruitycasa.pw
To: [redacted]
Subject: Why Haven't You Gotten Your Free Shirt?

Hello fellow Gun Enthusiast,

Two days ago I sent you my best selling shirt for FREE.
Did you see it? Check it out here!

These shirts have been so popular that I'm afraid today is
the last day I can be giving them away.
You see, **I only have 23 left**. So please grab yours now...

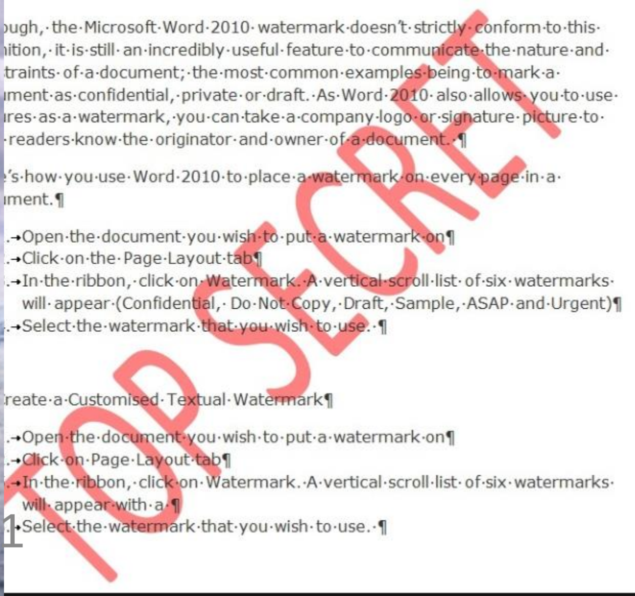
I can't guarantee when we'll have more in stock.
Pick yours up before they are gone!

Remember, **“The ultimate authority resides in the people alone.”**

Jason Mathers

P.S Today's the last day to claim your **free** shirt - grab yours!

smtp.fruitycasa.pw/link.php?M=85837&N=14&L=9&F=H



ugh,·the·Microsoft·Word·2010·watermark·doesn't·strictly·conform·to·this·
ition,·it·is·still·an·incredibly·useful·feature·to·communicate·the·nature·and·
traints·of·a·document;·the·most·common·examples·being·to·mark·a·
ment·as·confidential,·private·or·draft.·As·Word·2010·also·allows·you·to·use·
res·as·a·watermark,·you·can·take·a·company·logo·or·signature·picture·to·
·readers·know·the·originator·and·owner·of·a·document.·¶

's·how·you·use·Word·2010·to·place·a·watermark·on·every·page·in·a·
ment.¶

.→Open·the·document·you·wish·to·put·a·watermark·on¶
.→Click·on·the·Page·Layout·tab¶
.→In·the·ribbon,·click·on·Watermark.·A·vertical·scroll·list·of·six·watermarks·
will·appear·(Confidential,·Do·Not·Copy,·Draft,·Sample,·ASAP·and·Urgent)¶
.→Select·the·watermark·that·you·wish·to·use.·¶

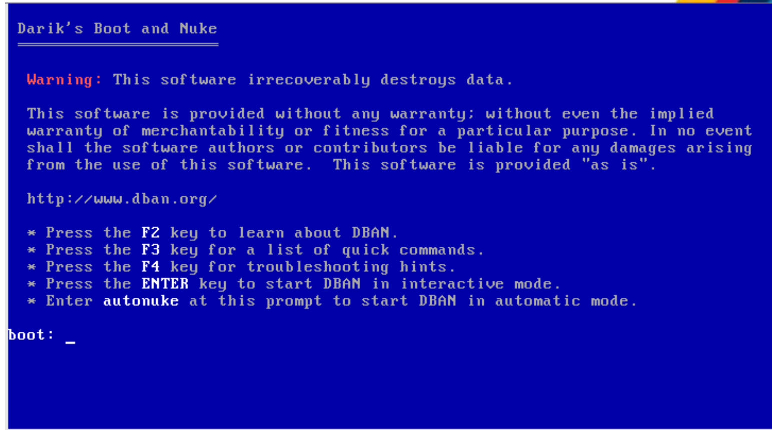
reate·a·Customised·Textual·Watermark¶

.→Open·the·document·you·wish·to·put·a·watermark·on¶
.→Click·on·Page·Layout·tab¶
.→In·the·ribbon,·click·on·Watermark.·A·vertical·scroll·list·of·six·watermarks·
will·appear·with·a·¶
.→Select·the·watermark·that·you·wish·to·use.·¶

Secure Disposal of Information

- physical destruction
  - e.g. hard drive, tape, USB
  - drill, shred, burn, degauss
- logical destruction
  - write over
    - e.g. DBAN - Darik's Boot and Nuke (problem doesn't erase hidden/bad sectors)
    - DoD – 7 passes, DoD short – 3 passes
  - throw away encryption keys

disrupts/eliminates
magnetic field removing data



```
Darik's Boot and Nuke

 Warning: This software irrecoverably destroys data.

 This software is provided without any warranty; without even the implied
 warranty of merchantability or fitness for a particular purpose. In no event
 shall the software authors or contributors be liable for any damages arising
 from the use of this software.  This software is provided "as is".

 http://www.dban.org/

 * Press the F2 key to learn about DBAN.
 * Press the F3 key for a list of quick commands.
 * Press the F4 key for troubleshooting hints.
 * Press the ENTER key to start DBAN in interactive mode.
 * Enter autonuke at this prompt to start DBAN in automatic mode.

boot: _
```

Secure Disposal of Information

- hard drive shredding
- EDDIE (Evil Destroyer of Delicate Internal Electronics)
  - erasing or sanitizing electronic media does not guarantee that all private information is non-retrievable. British Columbia is a leader in protecting electronic data and its industrial shredder, ‘EDDIE’ (Evil Destroyer of Delicate Internal Electronics), breaks down electronic media, such as hard drives, handheld devices and flexible media, to a particulate size of ¾”.
  - All shredded material is sent off for 100% recycling and will be used for energy processes or turned back into raw materials to create new items such as cement, metal products, park benches, etc.
  - similar device (https://youtu.be/qB13fMO9UC4)
  - another video https://youtu.be/p1eLF4b68dE
- what is the sensitivity of the information?
- what is the assurance level you require?
- what is the confidence, comfort level?

University of Victoria

Clearance

- pre-employment screening
- background/reference checks
- criminal record check eg. backcheck
- credit check eg. Equifax/Transunion
- security clearance eg. federal government 330-60-nf-eng form
    - Level I (Confidential)
    - Level II (Secret)
    - Level III (Top Secret)

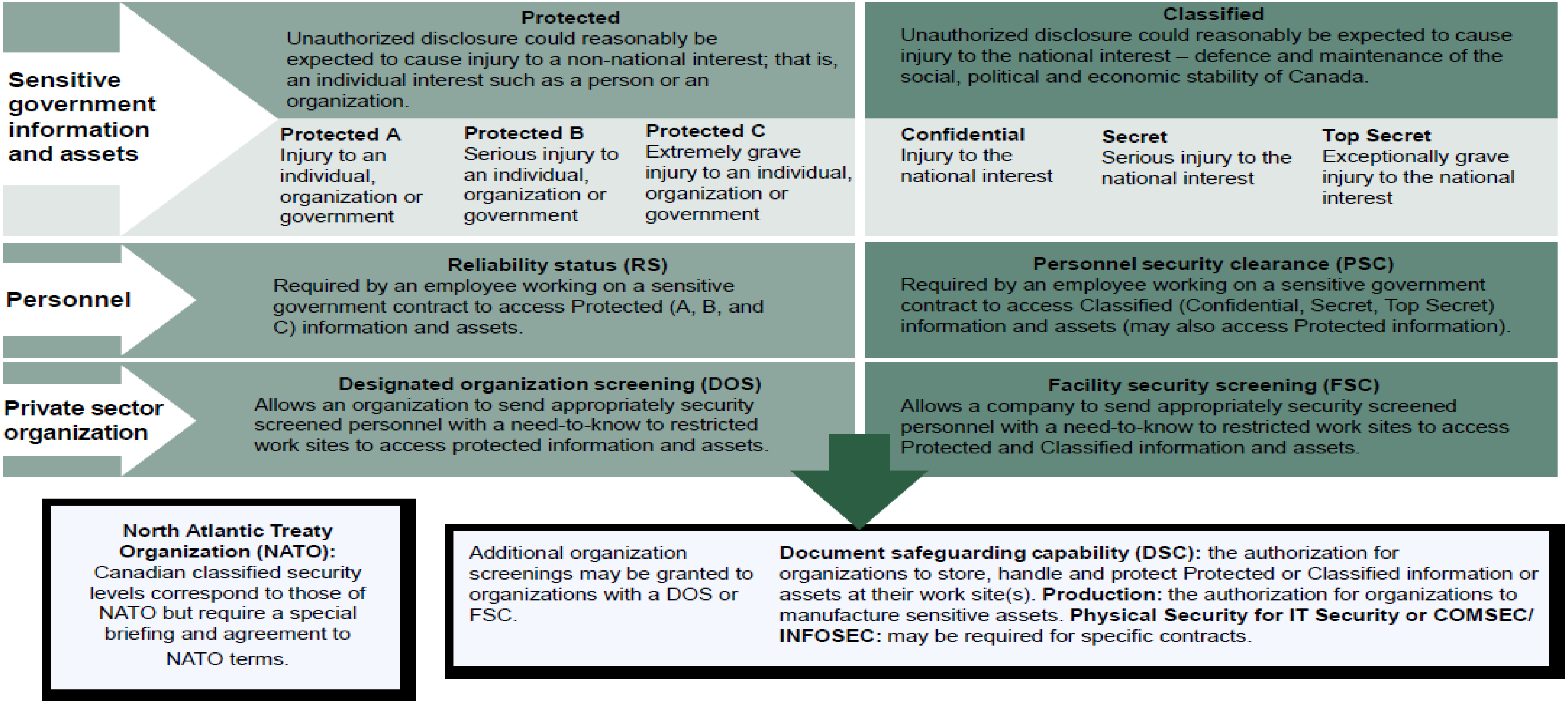
Clearance

- employee screening
- indicators of future performance
- interviews
- job descriptions
- background checks
- reference checks
- education, licensing, certification verification
- … more in onboarding, offboarding

job rotation
job description
- need to know
- least privilege

mandatory vacations

Clearance



Sensitive government information and assets

Protected
Unauthorized disclosure could reasonably be expected to cause injury to a non-national interest; that is, an individual interest such as a person or an organization.

Protected A
Injury to an individual, organization or government

Protected B
Serious injury to an individual, organization or government

Protected C
Extremely grave injury to an individual, organization or government

Classified
Unauthorized disclosure could reasonably be expected to cause injury to the national interest – defence and maintenance of the social, political and economic stability of Canada.

Confidential
Injury to the national interest

Secret
Serious injury to the national interest

Top Secret
Exceptionally grave injury to the national interest

Personnel

Reliability status (RS)
Required by an employee working on a sensitive government contract to access Protected (A, B, and C) information and assets.

Personnel security clearance (PSC)
Required by an employee working on a sensitive government contract to access Classified (Confidential, Secret, Top Secret) information and assets (may also access Protected information).

Private sector organization

Designated organization screening (DOS)
Allows an organization to send appropriately security screened personnel with a need-to-know to restricted work sites to access protected information and assets.

Facility security screening (FSC)
Allows a company to send appropriately security screened personnel with a need-to-know to restricted work sites to access Protected and Classified information and assets.

North Atlantic Treaty Organization (NATO):
Canadian classified security levels correspond to those of NATO but require a special briefing and agreement to NATO terms.

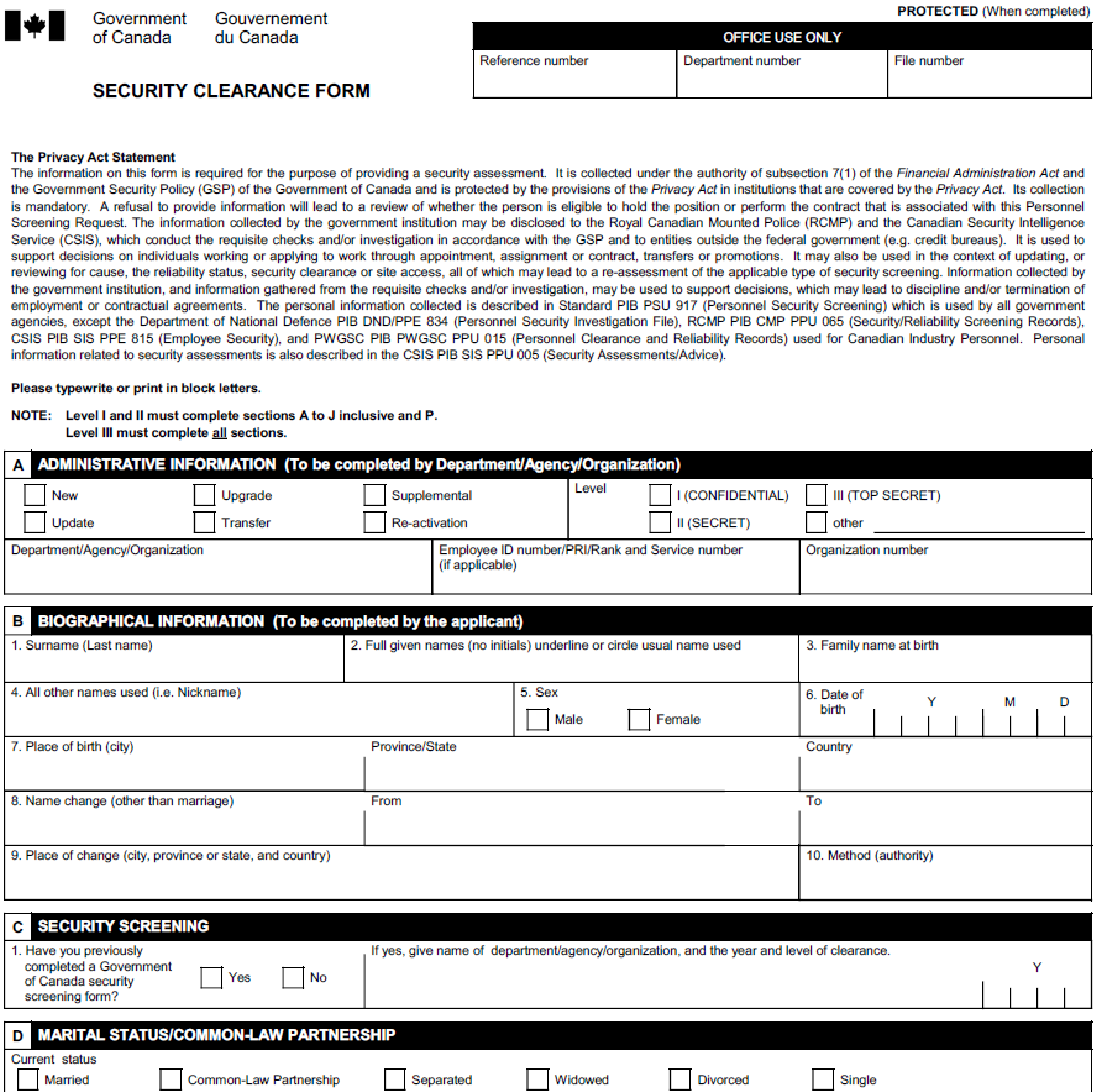
Additional organization screenings may be granted to organizations with a DOS or FSC.

Document safeguarding capability (DSC): the authorization for organizations to store, handle and protect Protected or Classified information or assets at their work site(s). **Production:** the authorization for organizations to manufacture sensitive assets. **Physical Security for IT Security or COMSEC/ INFOSEC:** may be required for specific contracts.

Clearance

- note classification

- Level I (confidential)
- Level II (secret)
- Level III (top secret)



Government of Canada Gouvernement du Canada

PROTECTED (When completed)

OFFICE USE ONLY		
Reference number	Department number	File number

SECURITY CLEARANCE FORM

The Privacy Act Statement

The information on this form is required for the purpose of providing a security assessment. It is collected under the authority of subsection 7(1) of the *Financial Administration Act* and the Government Security Policy (GSP) of the Government of Canada and is protected by the provisions of the *Privacy Act* in institutions that are covered by the *Privacy Act*. Its collection is mandatory. A refusal to provide information will lead to a review of whether the person is eligible to hold the position or perform the contract that is associated with this Personnel Screening Request. The information collected by the government institution may be disclosed to the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS), which conduct the requisite checks and/or investigation in accordance with the GSP and to entities outside the federal government (e.g. credit bureaus). It is used to support decisions on individuals working or applying to work through appointment, assignment or contract, transfers or promotions. It may also be used in the context of updating, or reviewing for cause, the reliability status, security clearance or site access, all of which may lead to a re-assessment of the applicable type of security screening. Information collected by the government institution, and information gathered from the requisite checks and/or investigation, may be used to support decisions, which may lead to discipline and/or termination of employment or contractual agreements. The personal information collected is described in Standard PIB PSU 917 (Personnel Security Screening) which is used by all government agencies, except the Department of National Defence PIB DND/PPE 834 (Personnel Security Investigation File), RCMP PIB CMP PPU 065 (Security/Reliability Screening Records), CSIS PIB SIS PPE 815 (Employee Security), and PWGSC PIB PWGSC PPU 015 (Personnel Clearance and Reliability Records) used for Canadian Industry Personnel. Personal information related to security assessments is also described in the CSIS PIB SIS PPU 005 (Security Assessments/Advice).

Please typewrite or print in block letters.

NOTE: Level I and II must complete sections A to J inclusive and P.
Level III must complete all sections.

A ADMINISTRATIVE INFORMATION (To be completed by Department/Agency/Organization)

□ New	□ Upgrade	□ Supplemental	Level	□ I (CONFIDENTIAL)	□ III (TOP SECRET)
□ Update	□ Transfer	□ Re-activation		□ II (SECRET)	□ other ______

Department/Agency/Organization	Employee ID number/PRI/Rank and Service number (if applicable)	Organization number

B BIOGRAPHICAL INFORMATION (To be completed by the applicant)

1. Surname (Last name)	2. Full given names (no initials) underline or circle usual name used	3. Family name at birth
4. All other names used (i.e. Nickname)	5. Sex □ Male □ Female	6. Date of birth Y M D
7. Place of birth (city)	Province/State	Country
8. Name change (other than marriage)	From	To
9. Place of change (city, province or state, and country)		10. Method (authority)

C SECURITY SCREENING

1. Have you previously completed a Government of Canada security screening form? □ Yes □ No	If yes, give name of department/agency/organization, and the year and level of clearance. Y

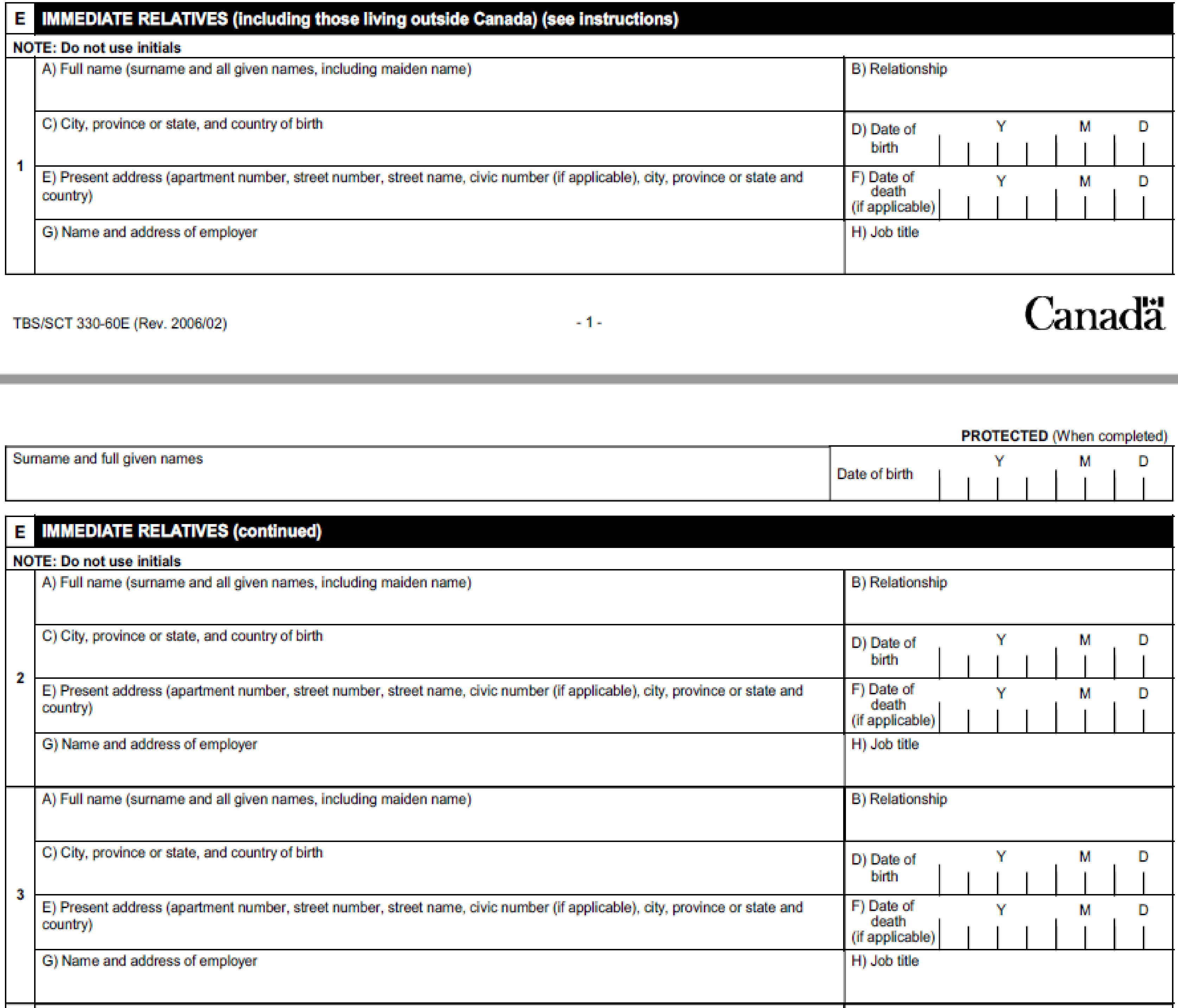
D MARITAL STATUS/COMMON-LAW PARTNERSHIP

Current status

□ Married □ Common-Law Partnership □ Separated □ Widowed □ Divorced □ Single

Clearance

- relatives….*



E	**IMMEDIATE RELATIVES (including those living outside Canada) (see instructions)**	
NOTE: Do not use initials		
1	A) Full name (surname and all given names, including maiden name)	B) Relationship
	C) City, province or state, and country of birth	D) Date of birth Y M D
	E) Present address (apartment number, street number, street name, civic number (if applicable), city, province or state and country)	F) Date of death (if applicable) Y M D
	G) Name and address of employer	H) Job title

PROTECTED (When completed)

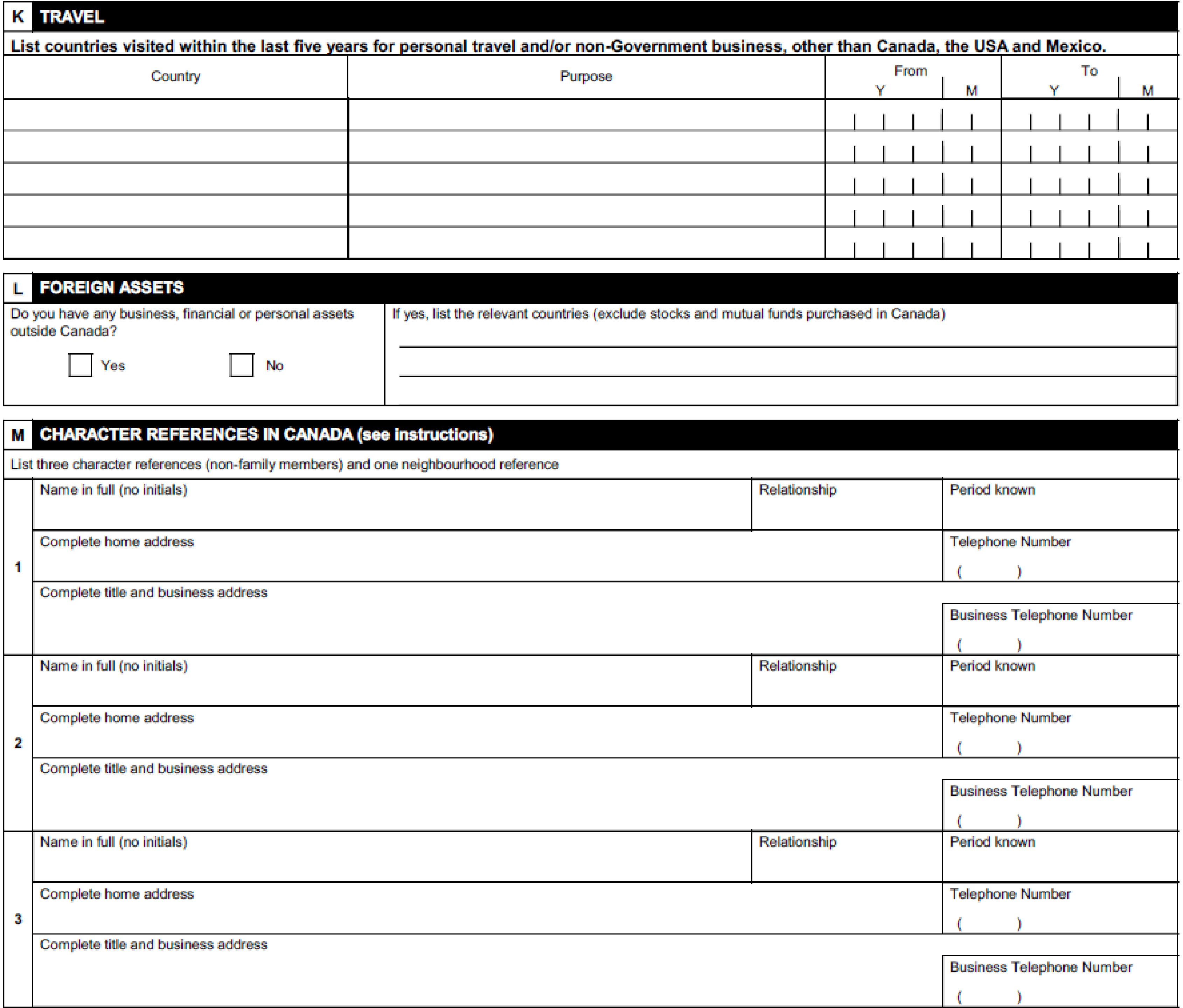
Surname and full given names	Date of birth Y M D

E	**IMMEDIATE RELATIVES (continued)**	
NOTE: Do not use initials		
2	A) Full name (surname and all given names, including maiden name)	B) Relationship
	C) City, province or state, and country of birth	D) Date of birth Y M D
	E) Present address (apartment number, street number, street name, civic number (if applicable), city, province or state and country)	F) Date of death (if applicable) Y M D
	G) Name and address of employer	H) Job title
3	A) Full name (surname and all given names, including maiden name)	B) Relationship
	C) City, province or state, and country of birth	D) Date of birth Y M D
	E) Present address (apartment number, street number, street name, civic number (if applicable), city, province or state and country)	F) Date of death (if applicable) Y M D
	G) Name and address of employer	H) Job title

University of Victoria

Clearance

- neighbours….*



K TRAVEL

List countries visited within the last five years for personal travel and/or non-Government business, other than Canada, the USA and Mexico.

Country	Purpose	From		To	
		Y	M	Y	M

L FOREIGN ASSETS

Do you have any business, financial or personal assets outside Canada?

□ Yes □ No

If yes, list the relevant countries (exclude stocks and mutual funds purchased in Canada)

M CHARACTER REFERENCES IN CANADA (see instructions)

List three character references (non-family members) and one neighbourhood reference

1

Name in full (no initials) | Relationship | Period known

Complete home address | Telephone Number ( )

Complete title and business address | Business Telephone Number ( )

2

Name in full (no initials) | Relationship | Period known

Complete home address | Telephone Number ( )

Complete title and business address | Business Telephone Number ( )

3

Name in full (no initials) | Relationship | Period known

Complete home address | Telephone Number ( )

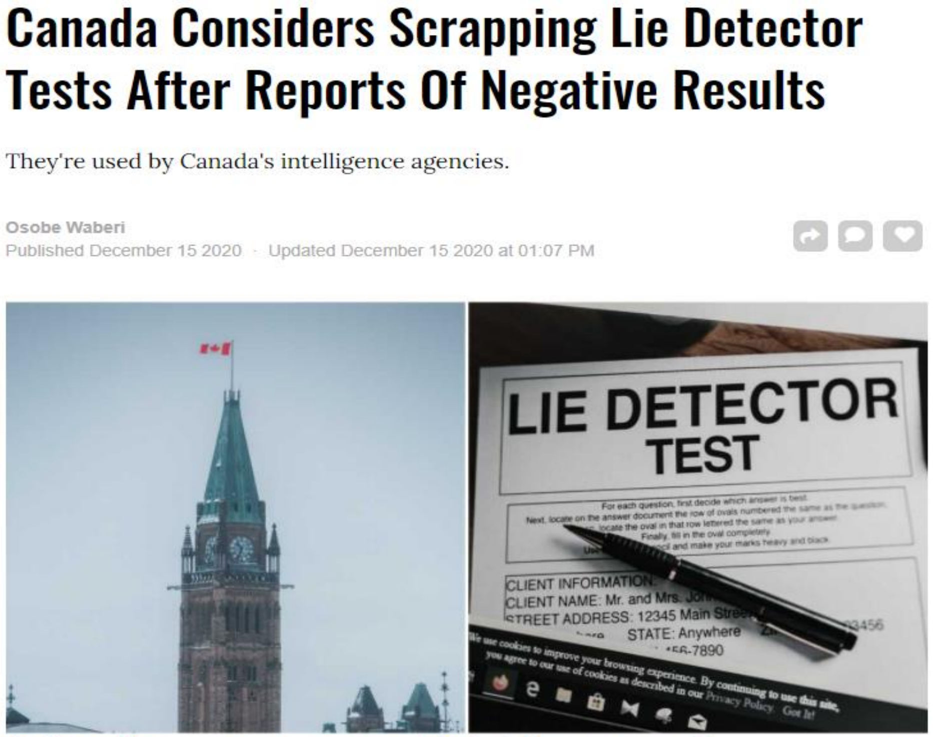
Complete title and business address | Business Telephone Number ( )

University of Victoria

Clearance

- forms
- process
- fingerprints
- polygraph
- what happens if you are part of a group and one person doesn’t have proof of clearance… lowest common denominator

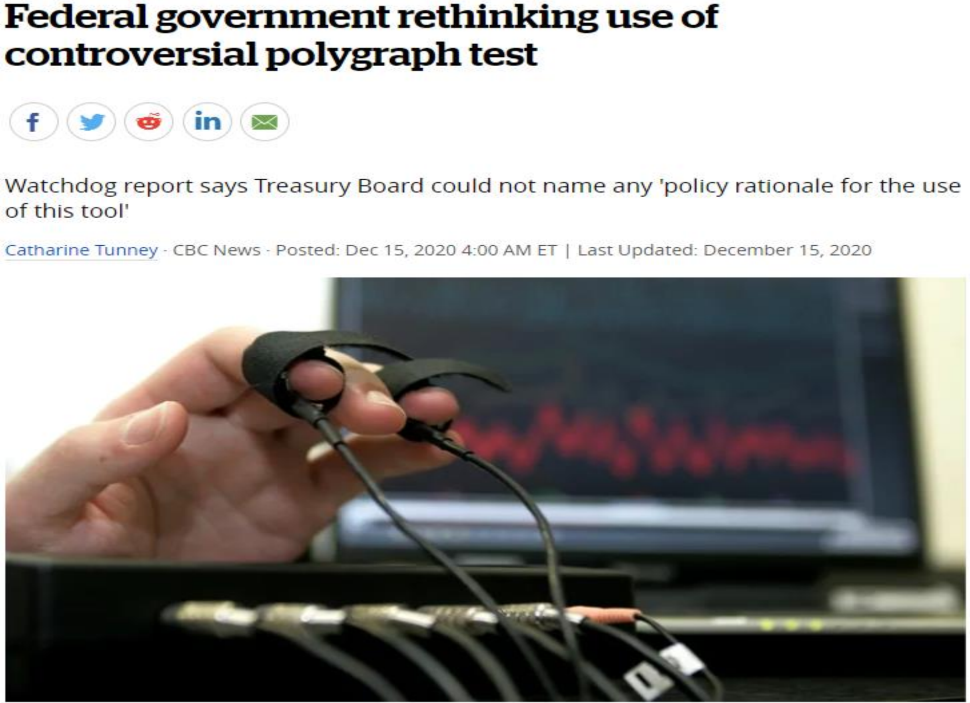
University of Victoria



Canada Considers Scrapping Lie Detector Tests After Reports Of Negative Results

They're used by Canada's intelligence agencies.

Osobe Waberi
Published December 15 2020 · Updated December 15 2020 at 01:07 PM



Federal government rethinking use of controversial polygraph test

Watchdog report says Treasury Board could not name any 'policy rationale for the use of this tool'

Catharine Tunney · CBC News · Posted: Dec 15, 2020 4:00 AM ET | Last Updated: December 15, 2020

Tools & Demos

DISCLAIMER

UNAUTHORIZED USE OF COMPUTER (CRIMINAL CODE OF CANADA)
/ Definitions / "computer program" / "computer service" / "computer system" / "data" / "electro-magnetic, acoustic, mechanical or other device" / "function" / "intercept" .

342.1. [1] Every one who, fraudulently and without colour of right,
[a] obtains, directly or indirectly, any computer service,
[b] by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or
[c] uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph [a] or [b] or an offence under section 430 in relation to data or a computer system
is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.
[2] In this section,
"computer program"
means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;
"computer service"
includes data processing and the storage or retrieval of data;
"computer system"
means a device that, or a group of interconnected or related devices one or more of which,
[a] contains computer programs or other data, and
[b] pursuant to computer programs,
[i] performs logic and control, and
[ii] may perform any other function;

"data“ means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;
"electro-magnetic, acoustic, or other device“ means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;
"function“ includes logic, control, arithmetic, deletion, storage and retrieval and communications or telecommunications to, from or within a computer system;
"intercept“ includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof. [R.S.C. 1985, C.27 [1st Supp.], s.45.]

University of Victoria

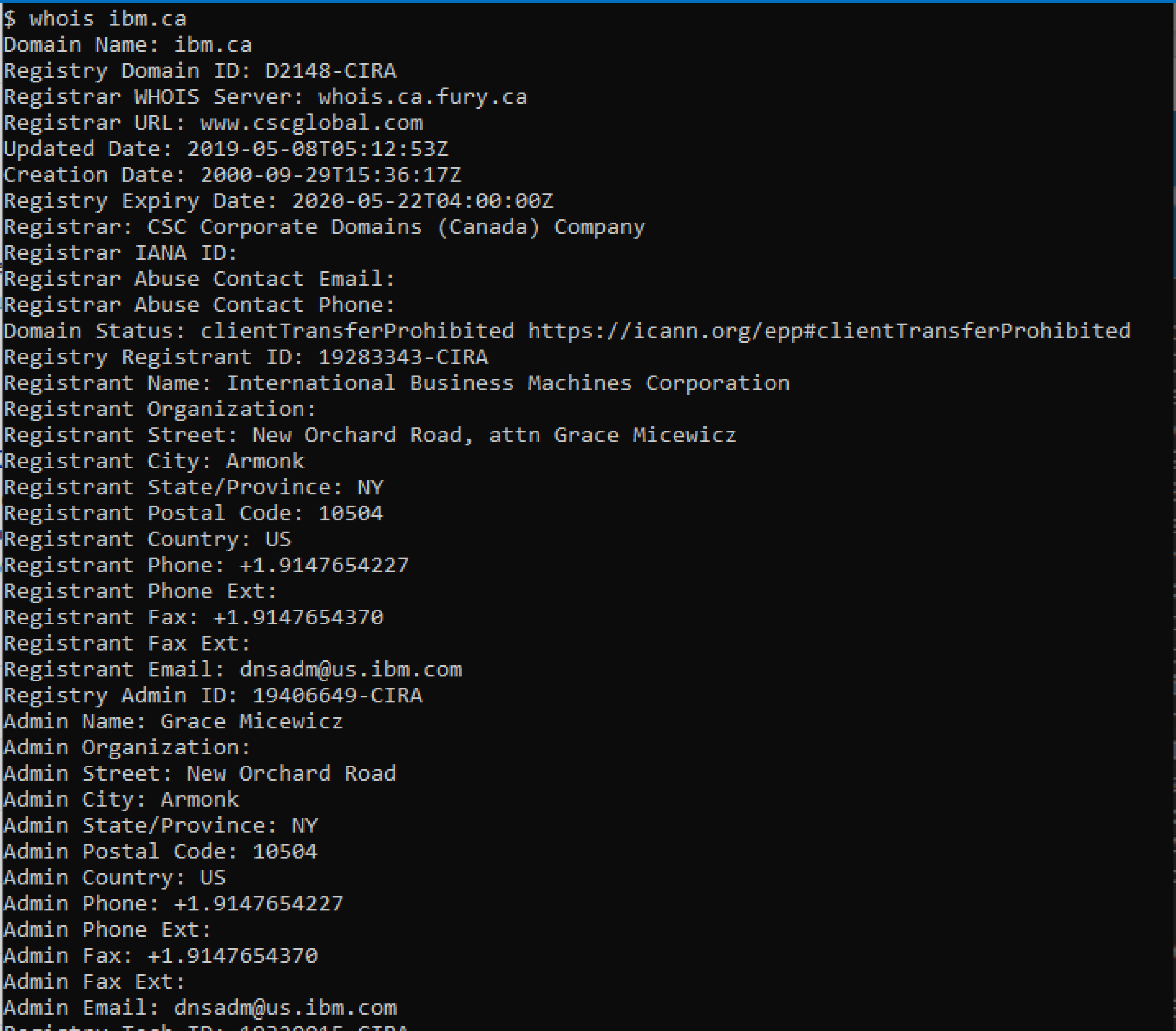
Knowledge check

- what do they do and why are they important?
  - ping, traceroute, netstat
  - nslookup (incl. mx), dig
  - whois
  - nmap, nessus, metasploit
- do not need to be an expert in these things but know they exist
- important to know how attacks are conducted in order to defend against them

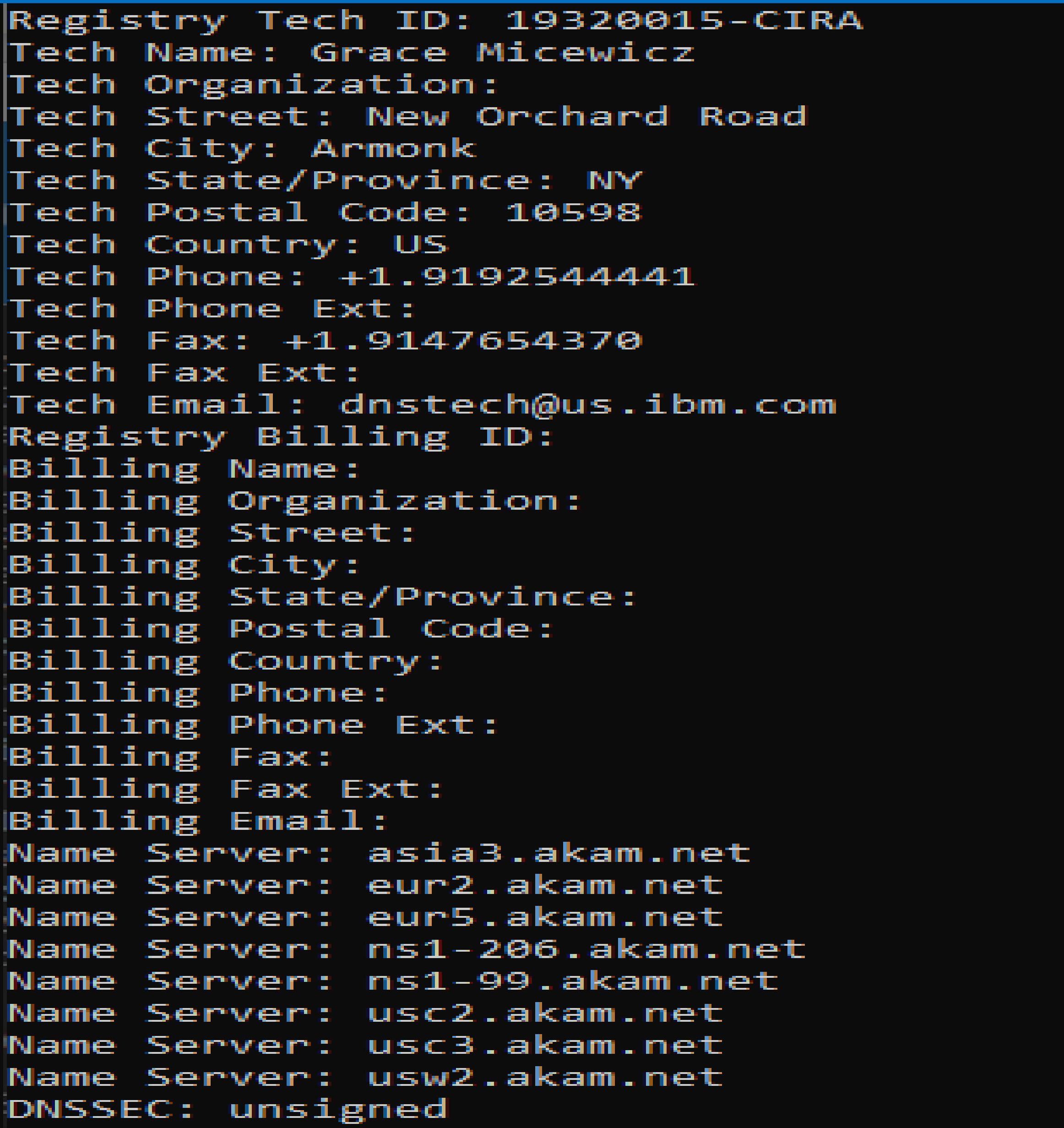
Knowledge check

ping	test connectivity between a source and destination
traceroute	trace the path between a source and destination
netstat	multiple uses including checking what ports are listening on a machine and current connections (netstat –an) or checking the routing table (netstat –rvn)
whois	**find out information regarding a domain**
nmap	often used for port scanning
nessus	often used for network vulnerability scanning
Metasploit	often used to exploit vulnerabilities

WHOIS (provides info about domains)



```
$ whois ibm.ca
Domain Name: ibm.ca
Registry Domain ID: D2148-CIRA
Registrar WHOIS Server: whois.ca.fury.ca
Registrar URL: www.cscglobal.com
Updated Date: 2019-05-08T05:12:53Z
Creation Date: 2000-09-29T15:36:17Z
Registry Expiry Date: 2020-05-22T04:00:00Z
Registrar: CSC Corporate Domains (Canada) Company
Registrar IANA ID:
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: 19283343-CIRA
Registrant Name: International Business Machines Corporation
Registrant Organization:
Registrant Street: New Orchard Road, attn Grace Micewicz
Registrant City: Armonk
Registrant State/Province: NY
Registrant Postal Code: 10504
Registrant Country: US
Registrant Phone: +1.9147654227
Registrant Phone Ext:
Registrant Fax: +1.9147654370
Registrant Fax Ext:
Registrant Email: dnsadm@us.ibm.com
Registry Admin ID: 19406649-CIRA
Admin Name: Grace Micewicz
Admin Organization:
Admin Street: New Orchard Road
Admin City: Armonk
Admin State/Province: NY
Admin Postal Code: 10504
Admin Country: US
Admin Phone: +1.9147654227
Admin Phone Ext:
Admin Fax: +1.9147654370
Admin Fax Ext:
Admin Email: dnsadm@us.ibm.com
Registry Tech ID: 19320015-CIRA
```



```
Registry Tech ID: 19320015-CIRA
Tech Name: Grace Micewicz
Tech Organization:
Tech Street: New Orchard Road
Tech City: Armonk
Tech State/Province: NY
Tech Postal Code: 10598
Tech Country: US
Tech Phone: +1.9192544441
Tech Phone Ext:
Tech Fax: +1.9147654370
Tech Fax Ext:
Tech Email: dnstech@us.ibm.com
Registry Billing ID:
Billing Name:
Billing Organization:
Billing Street:
Billing City:
Billing State/Province:
Billing Postal Code:
Billing Country:
Billing Phone:
Billing Phone Ext:
Billing Fax:
Billing Fax Ext:
Billing Email:
Name Server: asia3.akam.net
Name Server: eur2.akam.net
Name Server: eur5.akam.net
Name Server: ns1-206.akam.net
Name Server: ns1-99.akam.net
Name Server: usc2.akam.net
Name Server: usc3.akam.net
Name Server: usw2.akam.net
DNSSEC: unsigned
```

Steganography DEMO

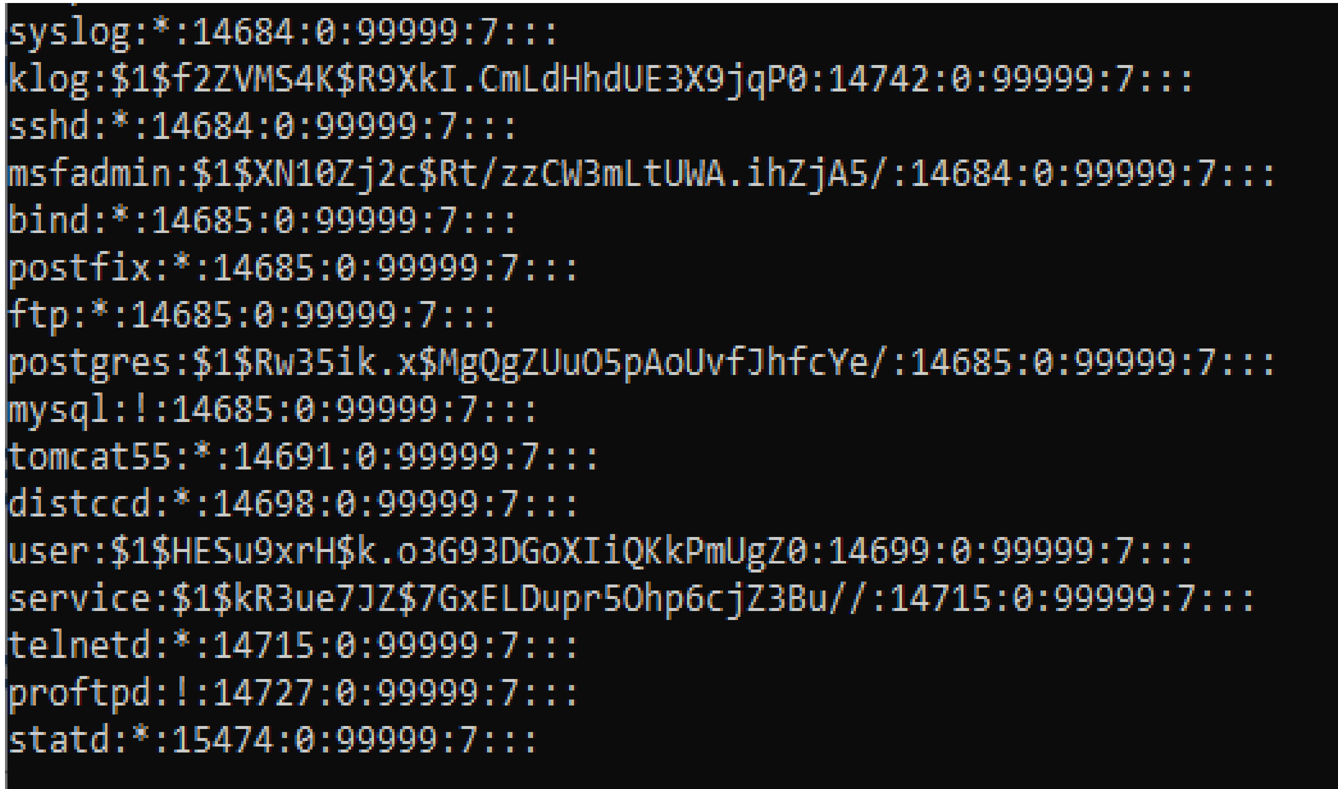
- used to conceal information in a file
- steghide info file.jpg
- steghide embed –cf file.jpg –ef file.txt
- steghide extract –sf file.jpg
- -p for a password

University of Victoria

John the Ripper DEMO

or use hashcat

- password cracker used in pentesting exercises
- takes in encrypted password and encrypts strings and compares output
- can supply a wordlist or brute force
- by default will do single, then default words, then incremental
- can supply parameters
- eg. john –wordlist=words.txt file



```
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```

Assigned Reading

- read Chapters 15, 19-23, 42-46
- consider the lab

University
of Victoria