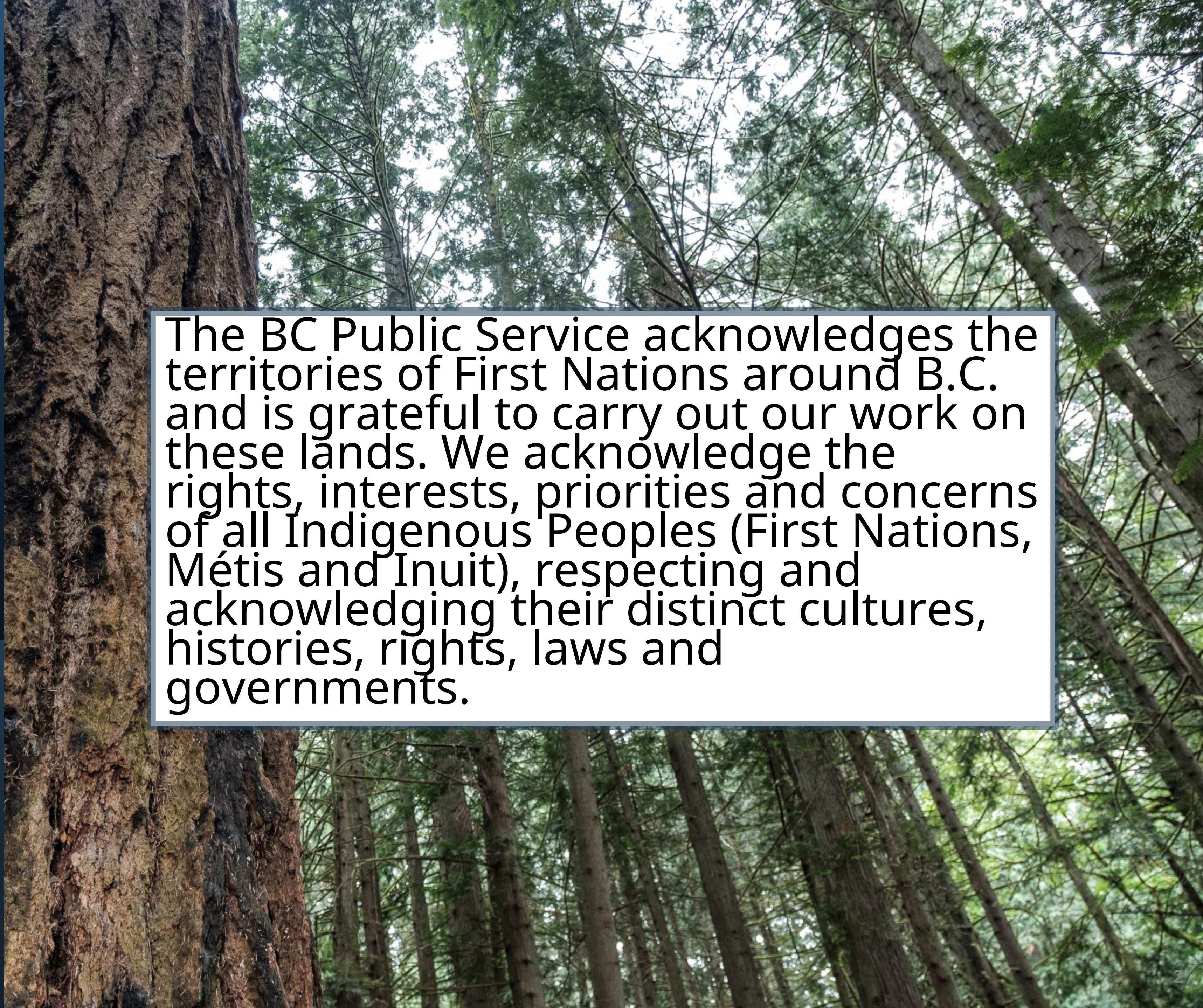
OCIO | Office of the Chief Information Officer

Security Threat and Risk Assessment 101

BRITISH COLUMBIA | Ministry of Citizens' Services

Territorial Acknowledgement



The BC Public Service acknowledges the territories of First Nations around B.C. and is grateful to carry out our work on these lands. We acknowledge the rights, interests, priorities and concerns of all Indigenous Peoples (First Nations, Métis and Inuit), respecting and acknowledging their distinct cultures, histories, rights, laws and governments.

Risk definition

Why should we care about risk?

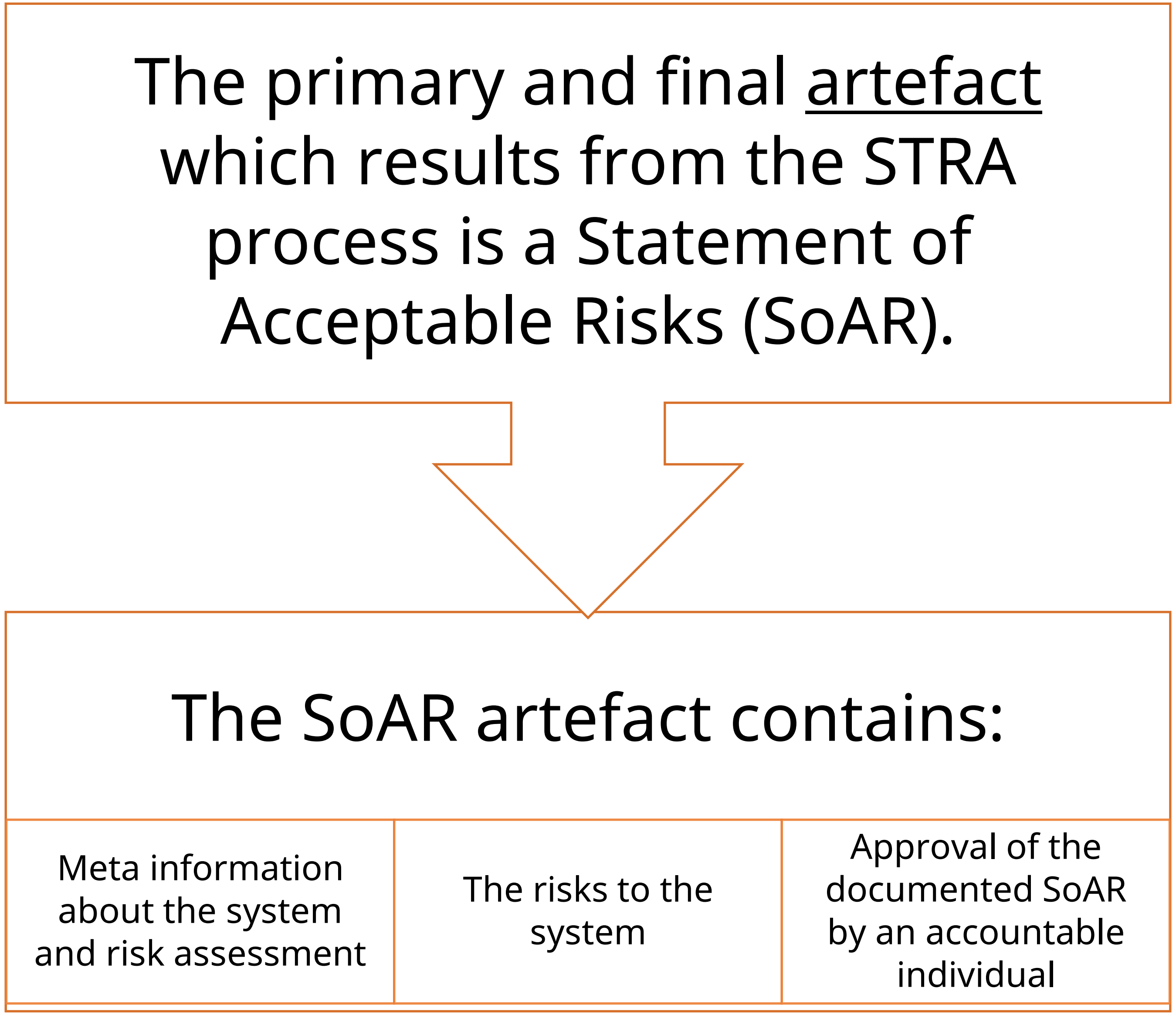
What is a Security Threat and Risk Assessment (STRA)?

~

The process of assessing information security risk to a system at a point in time.

~

What results from the STRA process?



The primary and final artefact which results from the STRA process is a Statement of Acceptable Risks (SoAR).

The SoAR artefact contains:

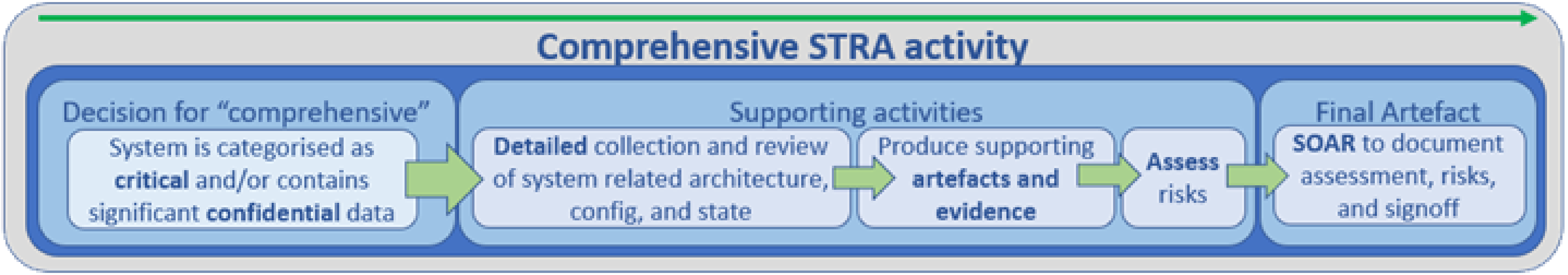
Meta information about the system and risk assessment	The risks to the system	Approval of the documented SoAR by an accountable individual

Do I ever need additional documentation to support an STRA?

The primary risk evaluator may decide to produce other supporting documents, and/or collect evidence in certain circumstances.

This is often in cases where:

- a system is classified as “Critical”, and/or
- where there is a level of complexity to a system, and/or
- where a significant amount of confidential information is involved.



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**

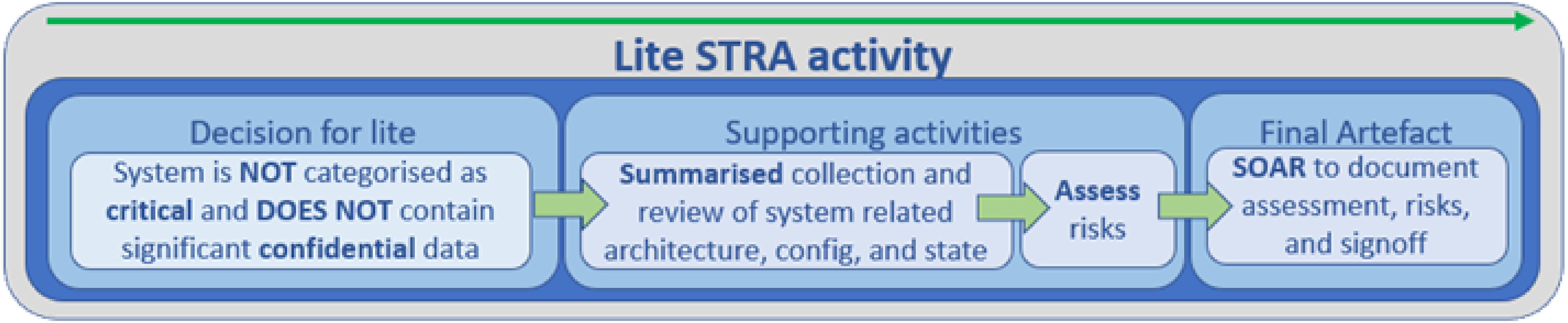
Assess risks

Final Artefact

SOAR to document assessment, risks, and signoff

What is a comprehensive STRA?

- Any STRA where additional supporting artefacts are also supplied beyond just the SoAR.
- The SoAR is always the final artefact and is used to document the risks and handle approvals.



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

What is a lite (fast tracked) STRA?

- This is any STRA where the SoAR is the only artefact resulting from the STRA process.

Is there any example / reference STRA process, more detailed, to help guide us through implementation?

Yes, there is a reference STRA process available which can help provide you with this guidance.

See: https://www2.gov.bc.ca/gov/content?id=31BECBD755944429B194E5780A3097DF

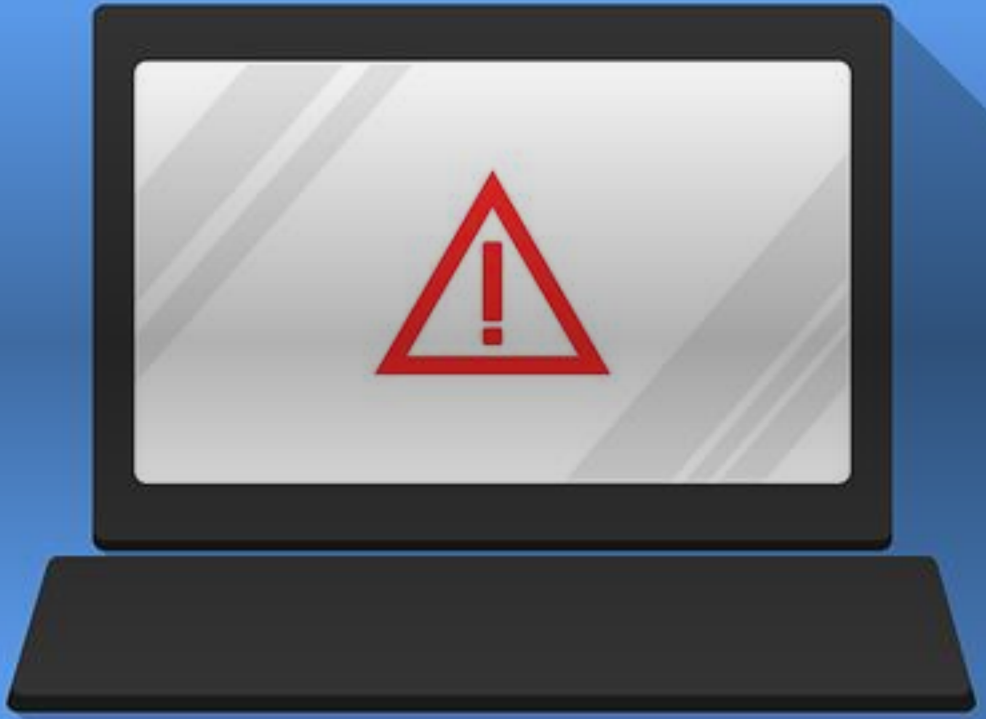
Difference between compliance and risk management?

Compliance

Risk Management

Does a risk assessment ever use controls?

What is a “vulnerability”?



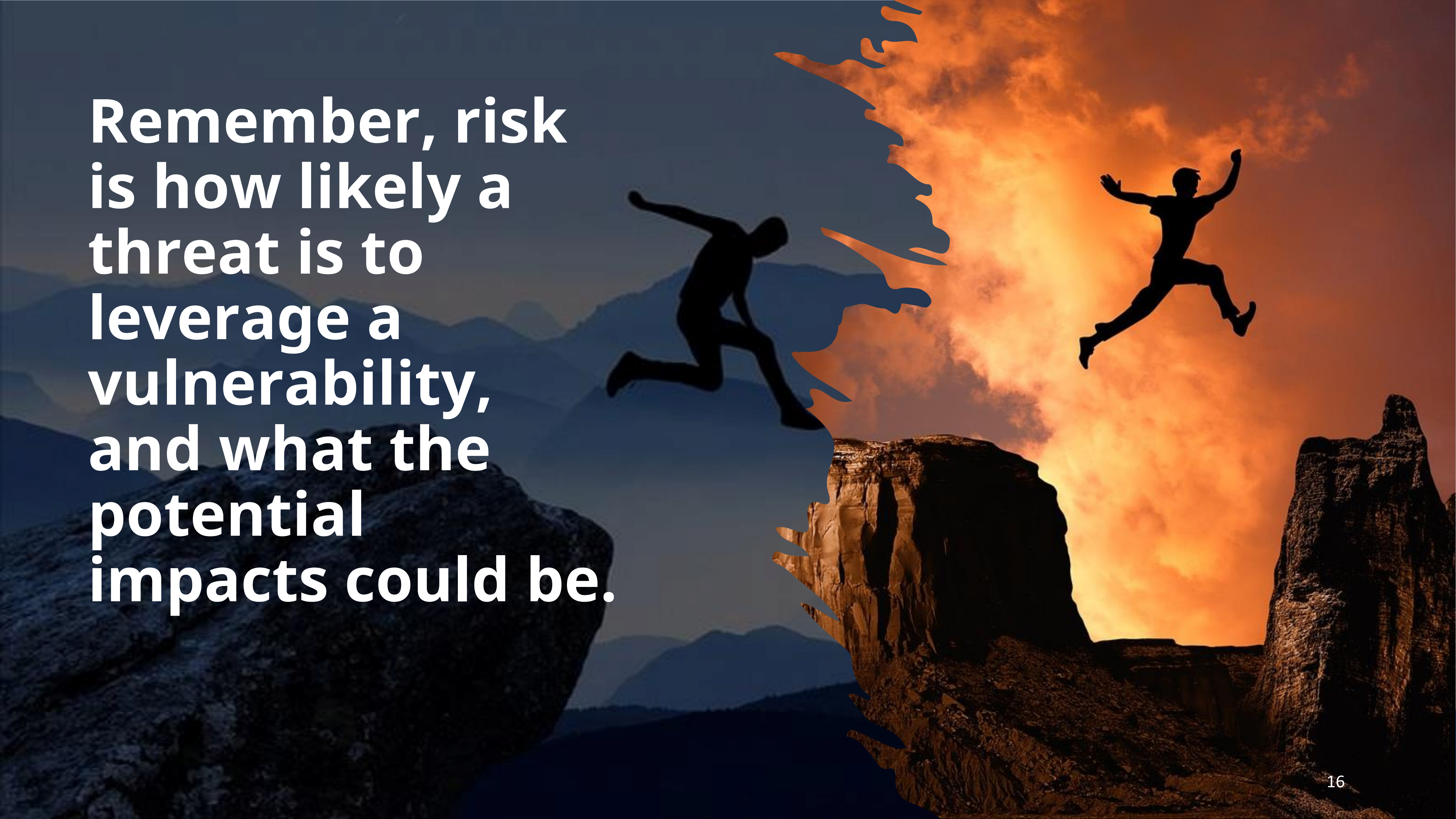
Do I need to perform a vulnerability scan or penetration test every time I complete an STRA?

The short answer is NO.

In special circumstances, if a system is critical, or highly complex, the primary risk evaluator may deem it appropriate and worthwhile to conduct a vulnerability scan or penetration test to help inform an STRA.

It is advisable that the primary risk evaluator of an STRA be empowered to make this decision where possible.

What is a “threat”?



Remember, risk is how likely a threat is to leverage a vulnerability, and what the potential impacts could be.

How is a risk rating determined?

LIKELIHOOD X POTENTIAL IMPACT = RISK RATING

Critical
Rating: 17 to 25

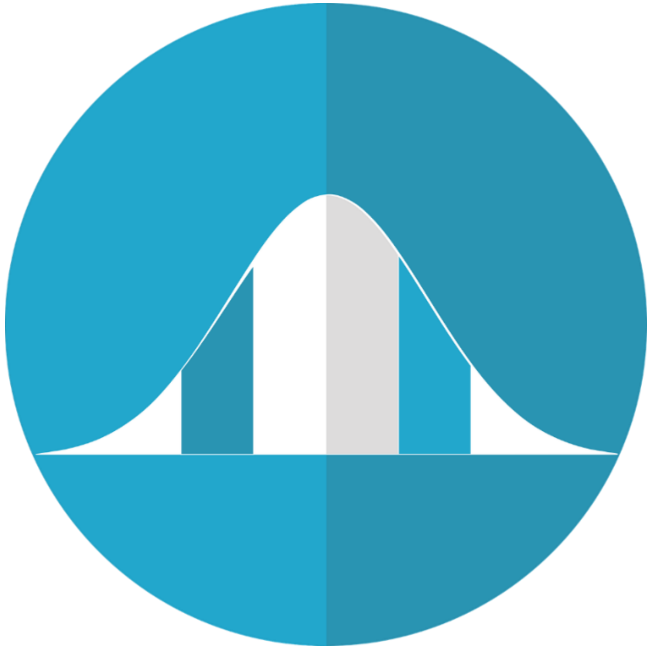
High
Score: 15 to 16

Medium
Score: 8 to 14

Low
Score: 2 to 7

Very Low
Score: 1

How can I determine likelihood for a risk?



Almost certain (>90-100%)
Score: 5

Likely (>50-90%)
Score: 4

Possible (>25-50%)
Score: 3

Unlikely (>10-25%)
Score: 2

Rare (0-10%)
Score: 1

How can I determine impact for a risk?

Catastrophic
Score: 5

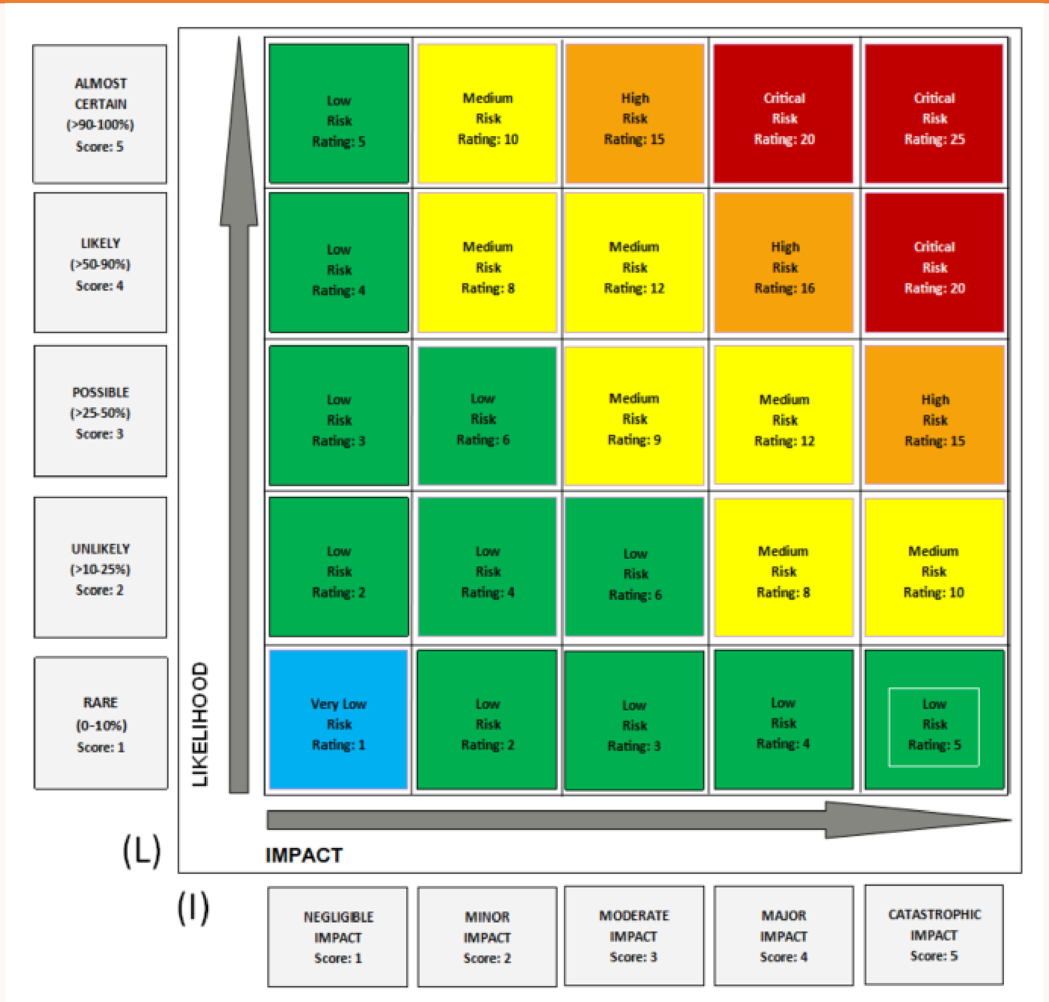
Major Impact
Score: 4

Moderate Impact
Score: 3

Minor Impact
Score: 2

Negligible Impact
Score: 1

Make rating risk easy. Use a matrix.



ALMOST CERTAIN (>90-100%) Score: 5	Low Risk Rating: 5	Medium Risk Rating: 10	High Risk Rating: 15	Critical Risk Rating: 20	Critical Risk Rating: 25
LIKELY (>50-90%) Score: 4	Low Risk Rating: 4	Medium Risk Rating: 8	Medium Risk Rating: 12	High Risk Rating: 16	Critical Risk Rating: 20
POSSIBLE (>25-50%) Score: 3	Low Risk Rating: 3	Low Risk Rating: 6	Medium Risk Rating: 9	Medium Risk Rating: 12	High Risk Rating: 15
UNLIKELY (>10-25%) Score: 2	Low Risk Rating: 2	Low Risk Rating: 4	Low Risk Rating: 6	Medium Risk Rating: 8	Medium Risk Rating: 10
RARE (0-10%) Score: 1	Very Low Risk Rating: 1	Low Risk Rating: 2	Low Risk Rating: 3	Low Risk Rating: 4	Low Risk Rating: 5
(L)	IMPACT				
(I)	NEGLIGIBLE IMPACT Score: 1	MINOR IMPACT Score: 2	MODERATE IMPACT Score: 3	MAJOR IMPACT Score: 4	CATASTROPHIC IMPACT Score: 5

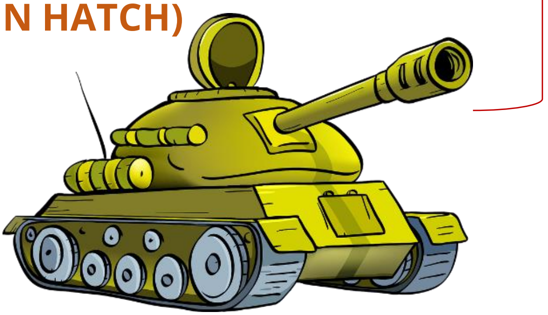
See:

https://www2.gov.bc.ca/gov/content?id=BA0689FE831E4C719D4BA54690D6C5DF

Let’s bring it all together

Likelihood that a
Harm / impact will
occur =
Almost Certain
(MUNITION IS FALLING
DIRECTLY ABOVE TANK)

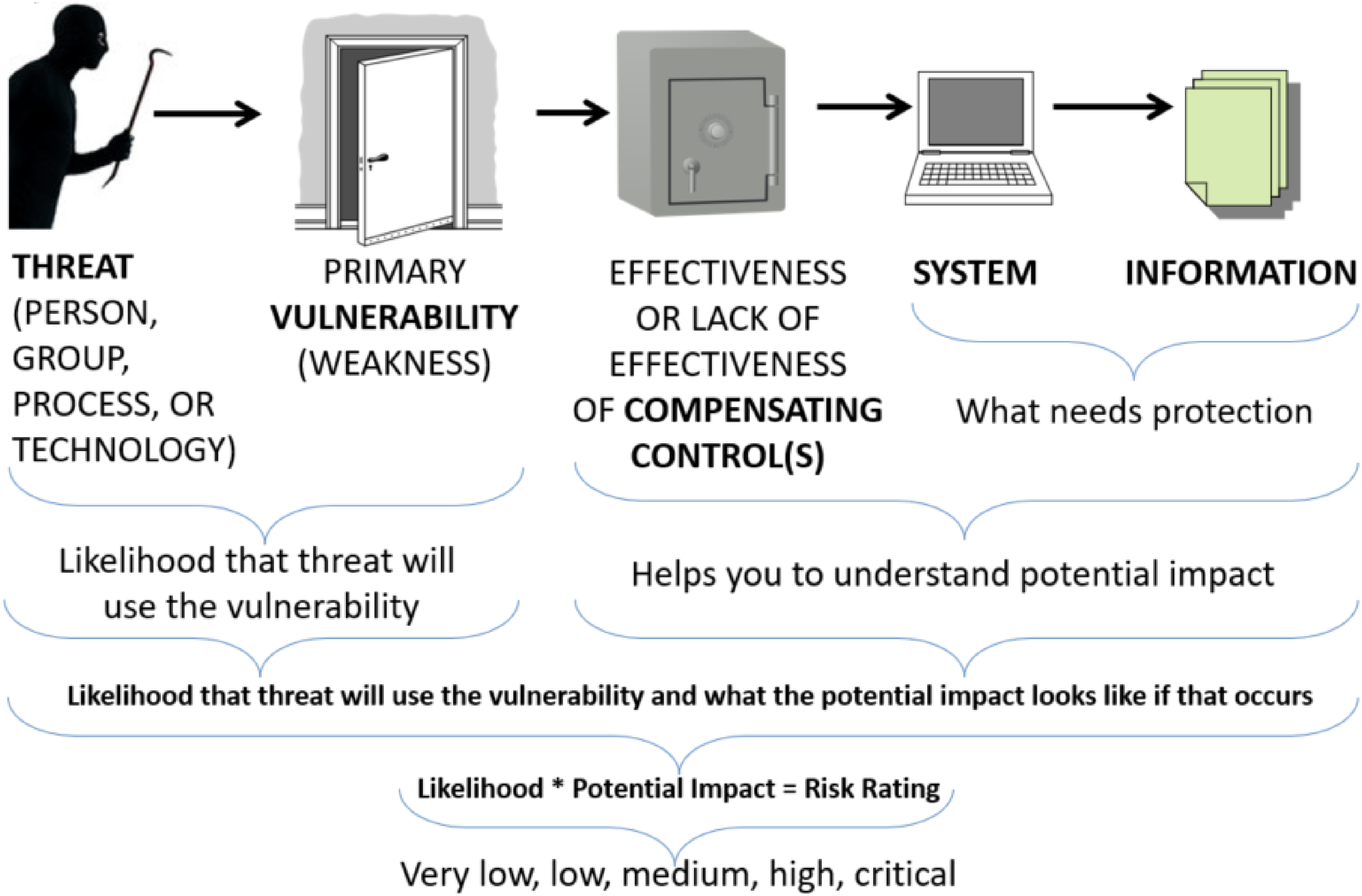
Vulnerability
(Exposed Weakness)
(OPEN HATCH)



Potential impact =
Catastrophic
(TANK IS NO MORE)

What does it mean to the organization?
(Loss of life, loss of equipment, and loss of battle.)

Let’s bring it all together



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

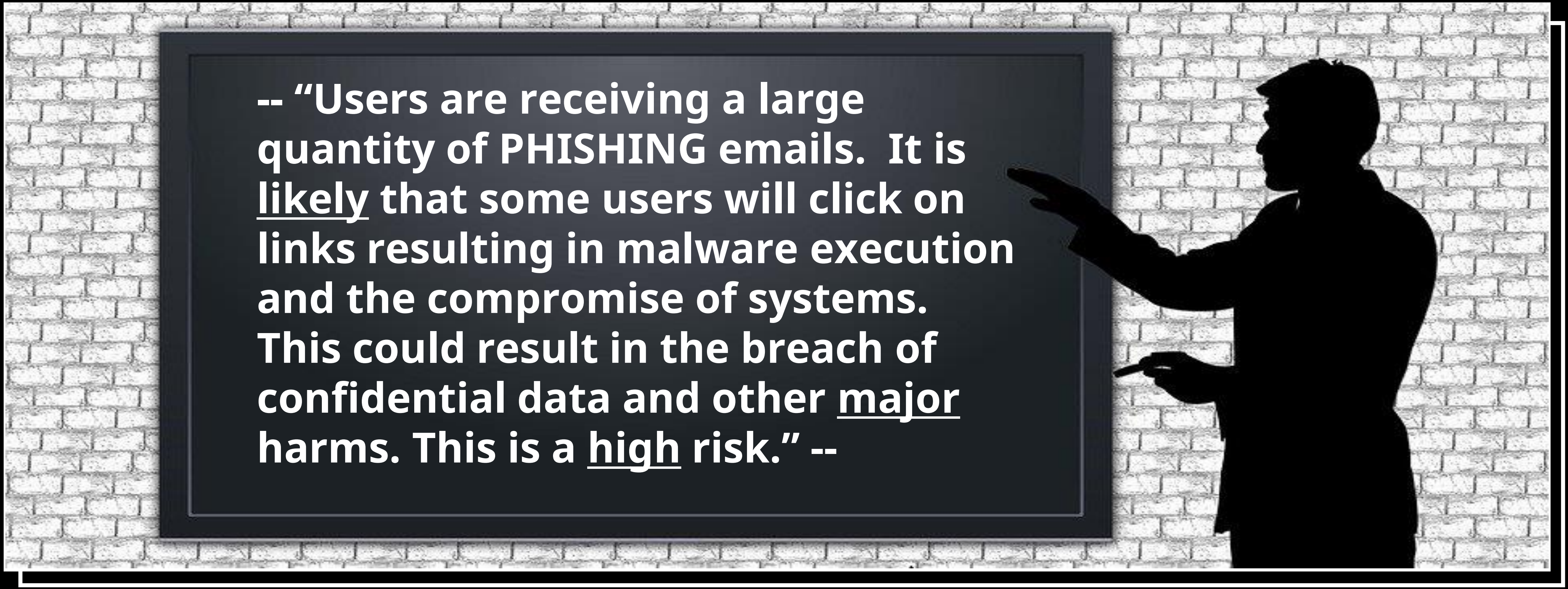
Likelihood that threat will use the vulnerability and what the potential impact looks like if that occurs

Likelihood * Potential Impact = Risk Rating

Very low, low, medium, high, critical

Writing a risk statement / description

EXAMPLE



-- "Users are receiving a large quantity of PHISHING emails. It is likely that some users will click on links resulting in malware execution and the compromise of systems. This could result in the breach of confidential data and other major harms. This is a high risk." --

Responsible VS Accountable

1

Responsible means you have an obligation to perform a task.

2

Accountable means you must answer for the overall outcome.

What do you do once you know you have a risk?

Treat it **or** **Consciously Accept it** **Don’t ignore it**

Treating risk

Avoid

Mitigate
(Reduce
Risk)

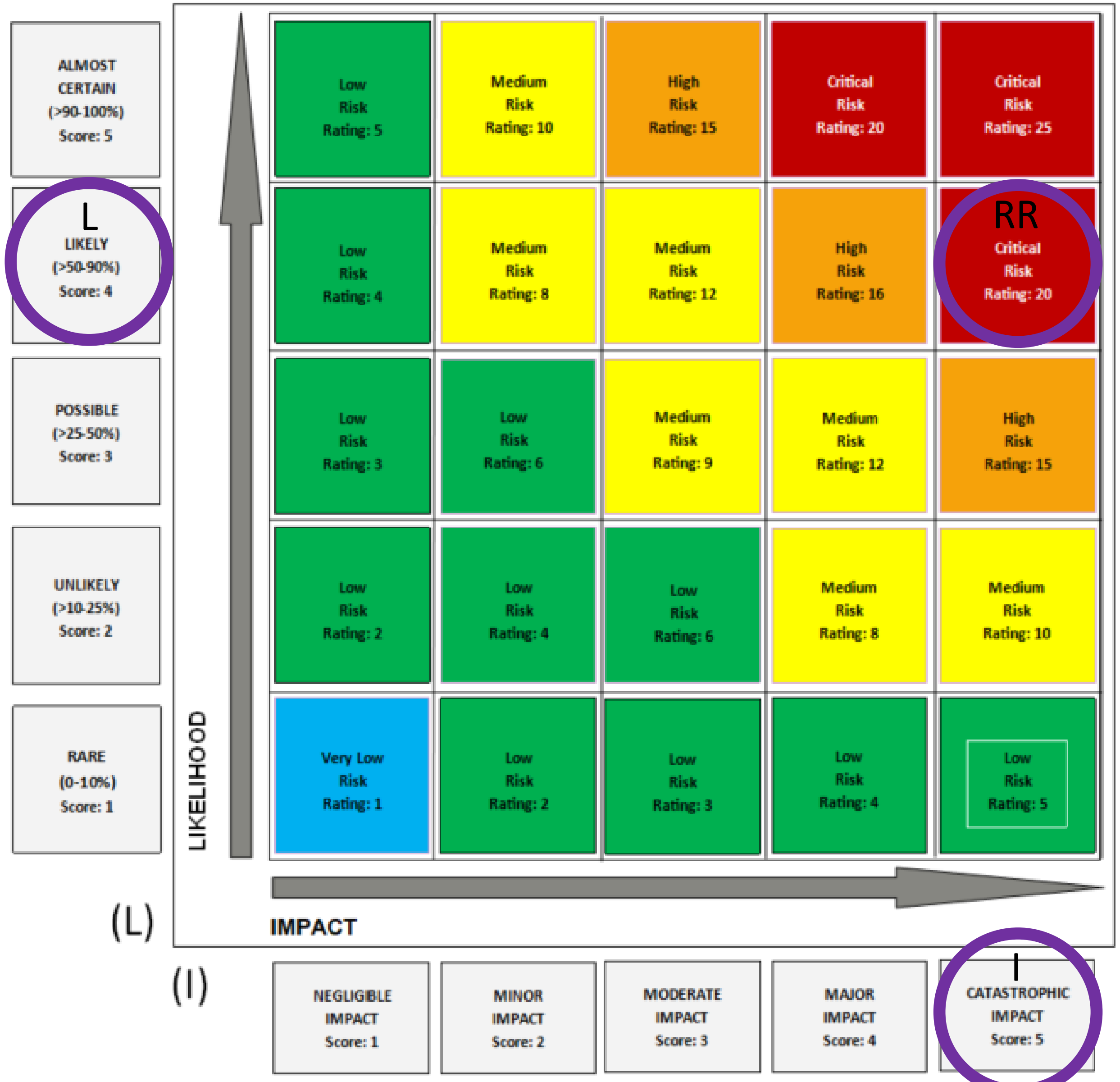
Transfer

Remediate
(Fix)

Accept

Example Risk:

Risk to house by tree



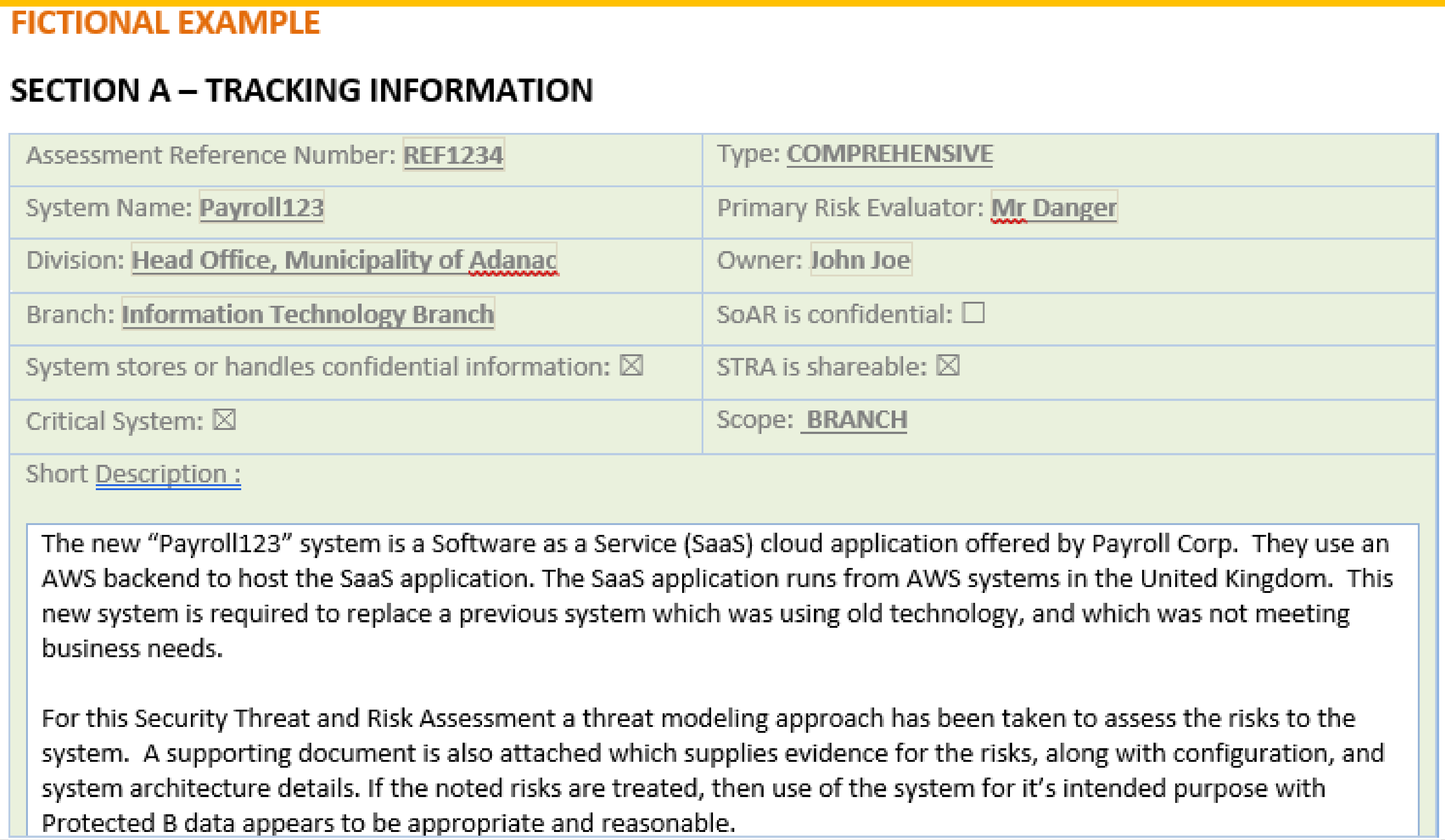
	NEGLIGIBLE IMPACT Score: 1	MINOR IMPACT Score: 2	MODERATE IMPACT Score: 3	MAJOR IMPACT Score: 4	I CATASTROPHIC IMPACT Score: 5
ALMOST CERTAIN (>90-100%) Score: 5	Low Risk Rating: 5	Medium Risk Rating: 10	High Risk Rating: 15	Critical Risk Rating: 20	Critical Risk Rating: 25
L LIKELY (>50-90%) Score: 4	Low Risk Rating: 4	Medium Risk Rating: 8	Medium Risk Rating: 12	High Risk Rating: 16	RR Critical Risk Rating: 20
POSSIBLE (>25-50%) Score: 3	Low Risk Rating: 3	Low Risk Rating: 6	Medium Risk Rating: 9	Medium Risk Rating: 12	High Risk Rating: 15
UNLIKELY (>10-25%) Score: 2	Low Risk Rating: 2	Low Risk Rating: 4	Low Risk Rating: 6	Medium Risk Rating: 8	Medium Risk Rating: 10
RARE (0-10%) Score: 1	Very Low Risk Rating: 1	Low Risk Rating: 2	Low Risk Rating: 3	Low Risk Rating: 4	Low Risk Rating: 5

Likelihood (L) * Impact (I) = Risk Rating (RR)

How do I know when an STRA is needed?

Example of how to complete a SoAR for an STRA

Example of how to complete a SoAR for an STRA



FICTIONAL EXAMPLE

SECTION A – TRACKING INFORMATION

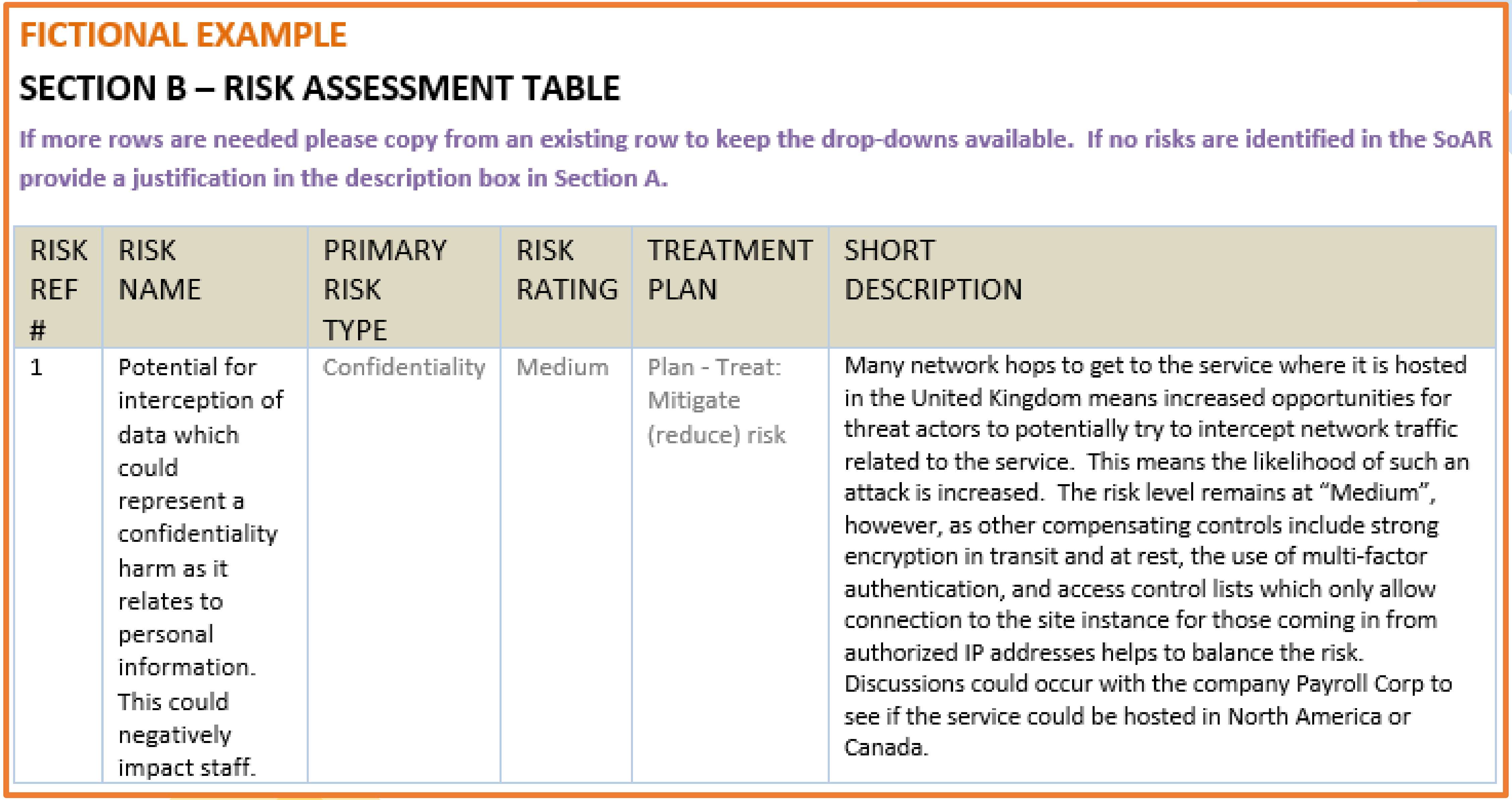
Assessment Reference Number: REF1234	Type: COMPREHENSIVE
System Name: Payroll123	Primary Risk Evaluator: Mr Danger
Division: Head Office, Municipality of Adanac	Owner: John Joe
Branch: Information Technology Branch	SoAR is confidential: ☐
System stores or handles confidential information: ☒	STRA is shareable: ☒
Critical System: ☒	Scope: BRANCH

Short Description :

The new "Payroll123" system is a Software as a Service (SaaS) cloud application offered by Payroll Corp. They use an AWS backend to host the SaaS application. The SaaS application runs from AWS systems in the United Kingdom. This new system is required to replace a previous system which was using old technology, and which was not meeting business needs.

For this Security Threat and Risk Assessment a threat modeling approach has been taken to assess the risks to the system. A supporting document is also attached which supplies evidence for the risks, along with configuration, and system architecture details. If the noted risks are treated, then use of the system for it's intended purpose with Protected B data appears to be appropriate and reasonable.

Example of how to complete a SoAR for an STRA



FICTIONAL EXAMPLE

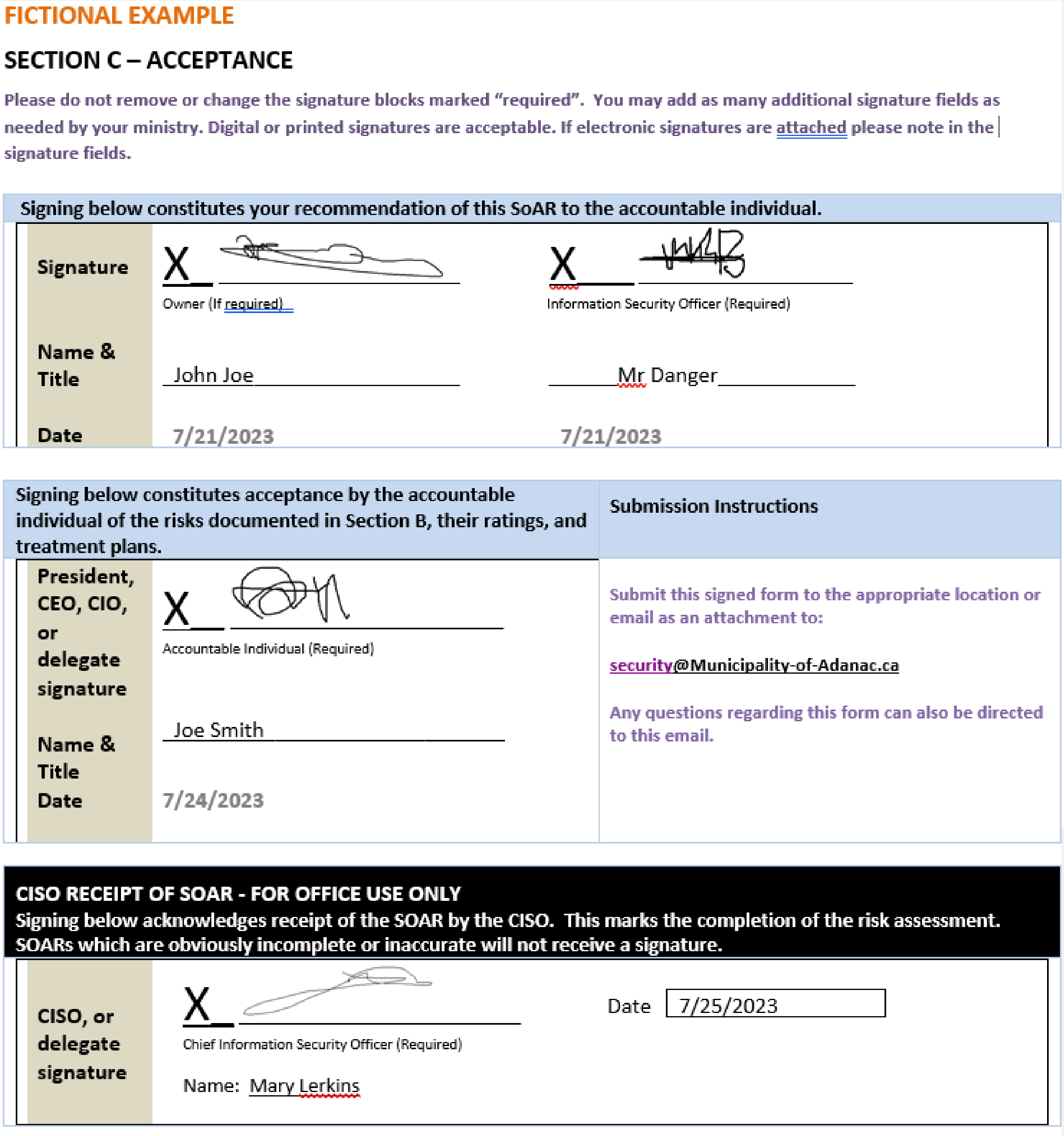
SECTION B – RISK ASSESSMENT TABLE

If more rows are needed please copy from an existing row to keep the drop-downs available. If no risks are identified in the SoAR provide a justification in the description box in Section A.

RISK REF #	RISK NAME	PRIMARY RISK TYPE	RISK RATING	TREATMENT PLAN	SHORT DESCRIPTION
1	Potential for interception of data which could represent a confidentiality harm as it relates to personal information. This could negatively impact staff.	Confidentiality	Medium	Plan - Treat: Mitigate (reduce) risk	Many network hops to get to the service where it is hosted in the United Kingdom means increased opportunities for threat actors to potentially try to intercept network traffic related to the service. This means the likelihood of such an attack is increased. The risk level remains at "Medium", however, as other compensating controls include strong encryption in transit and at rest, the use of multi-factor authentication, and access control lists which only allow connection to the site instance for those coming in from authorized IP addresses helps to balance the risk. Discussions could occur with the company Payroll Corp to see if the service could be hosted in North America or Canada.

And more risks…

Example of how to complete a SoAR for an STRA



FICTIONAL EXAMPLE

SECTION C – ACCEPTANCE

Please do not remove or change the signature blocks marked “required”. You may add as many additional signature fields as needed by your ministry. Digital or printed signatures are acceptable. If electronic signatures are attached please note in the signature fields.

Signing below constitutes your recommendation of this SoAR to the accountable individual.

Signature	X Owner (If required)	X Information Security Officer (Required)
Name & Title	John Joe	Mr Danger
Date	7/21/2023	7/21/2023

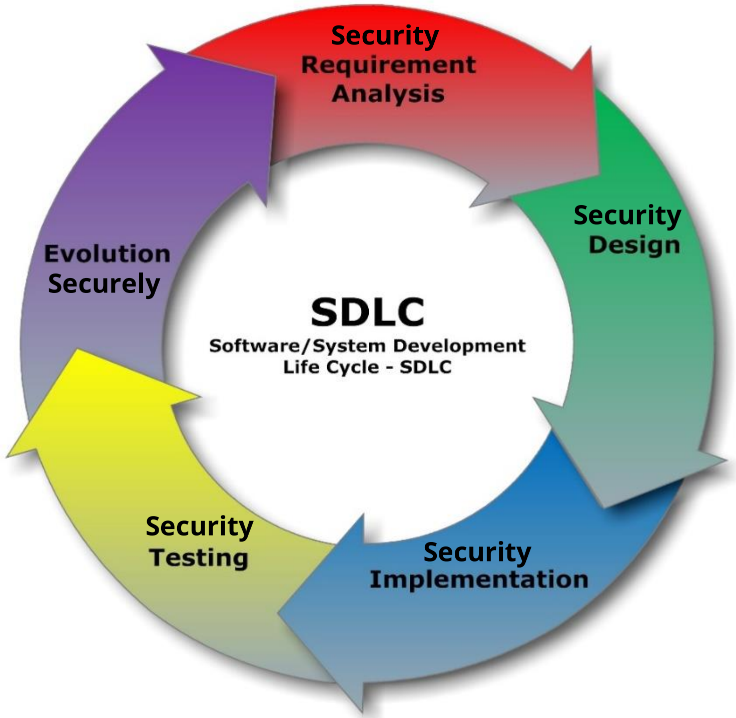
Signing below constitutes acceptance by the accountable individual of the risks documented in Section B, their ratings, and treatment plans.		**Submission Instructions**
President, CEO, CIO, or delegate signature	X Accountable Individual (Required)	Submit this signed form to the appropriate location or email as an attachment to: security@Municipality-of-Adanac.ca Any questions regarding this form can also be directed to this email.
Name & Title	Joe Smith	
Date	7/24/2023	

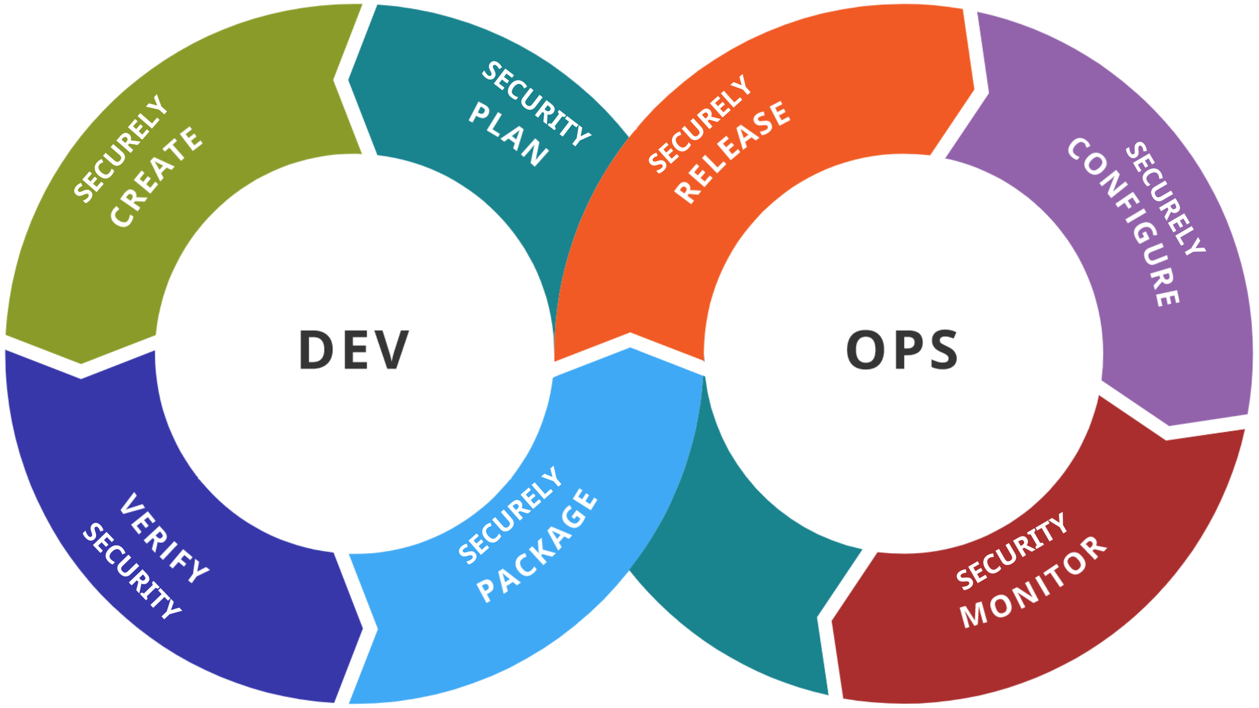
CISO RECEIPT OF SOAR - FOR OFFICE USE ONLY

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

CISO, or delegate signature	X Chief Information Security Officer (Required) Name: Mary Lerkins	Date 7/25/2023

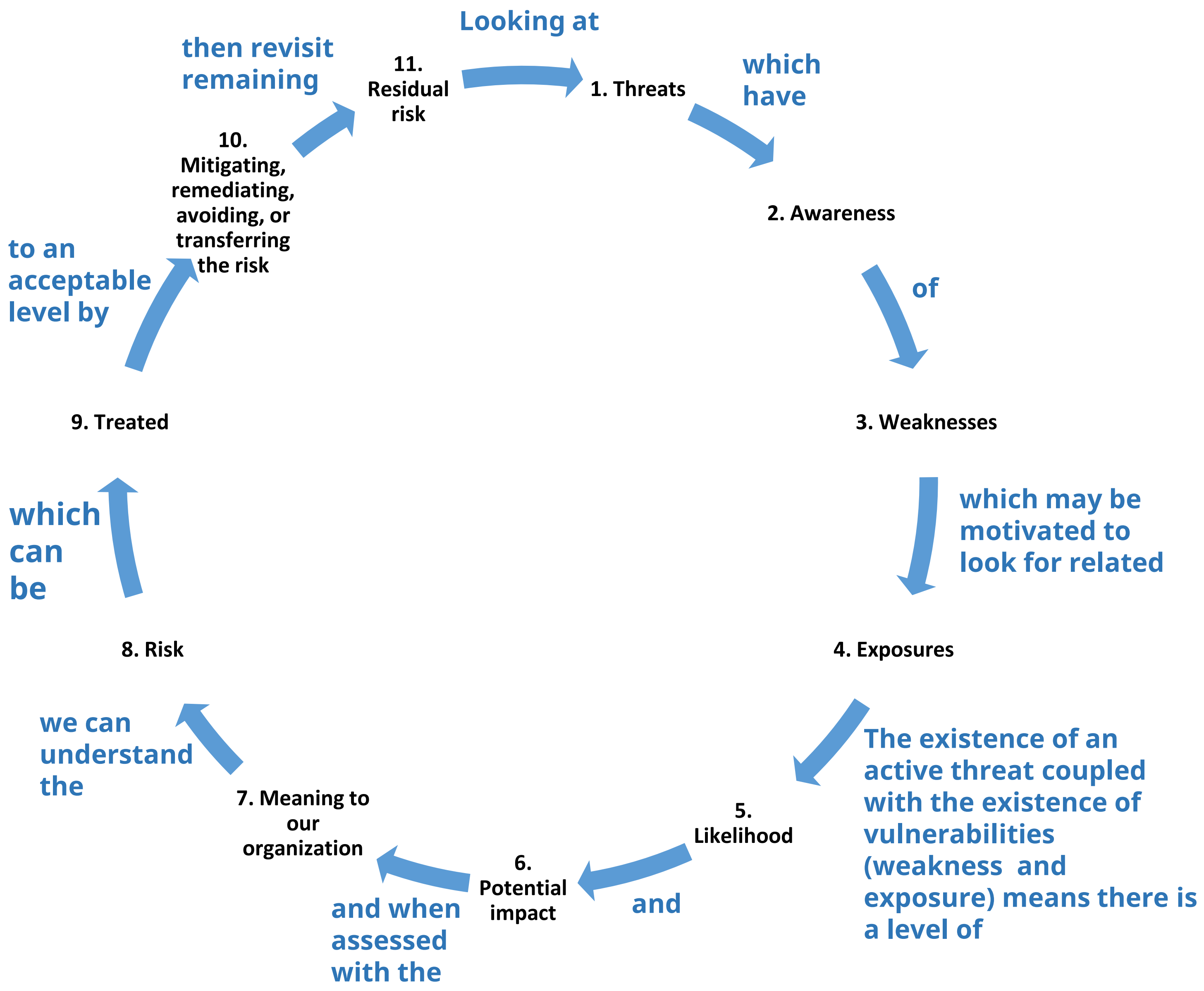
Software / System Development Life Cycle (SDLC) and DevOps





Why considering security risks at every stage is advisable

The information security risk lifecycle



Looking at

1. Threats

which have

2. Awareness

of

3. Weaknesses

which may be motivated to look for related

4. Exposures

The existence of an active threat coupled with the existence of vulnerabilities (weakness and exposure) means there is a level of

5. Likelihood

and

6. Potential impact

and when assessed with the

7. Meaning to our organization

we can understand the

8. Risk

which can be

9. Treated

to an acceptable level by

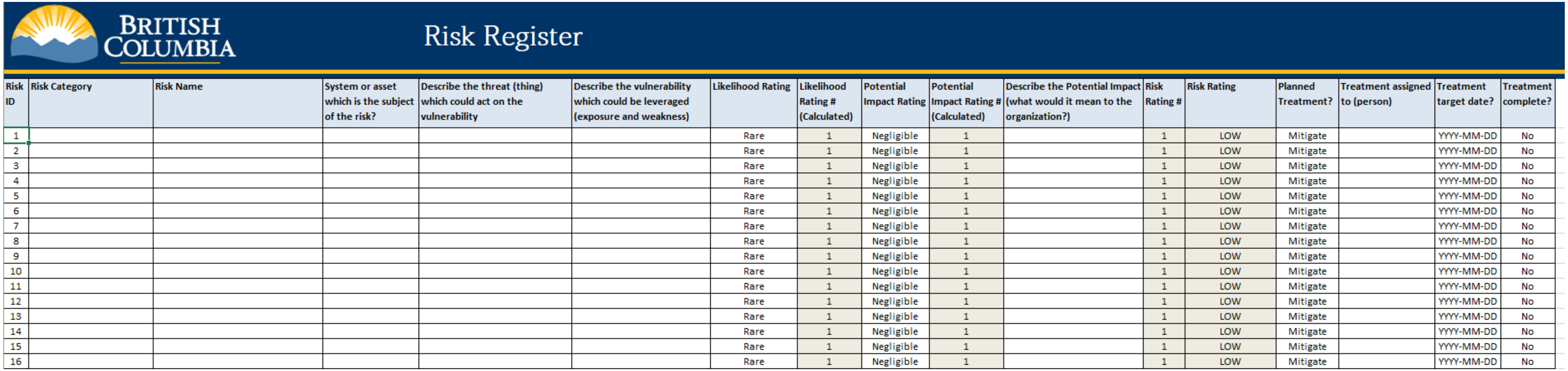
10. Mitigating, remediating, avoiding, or transferring the risk

then revisit remaining

11. Residual risk

The STRA is complete.
What do I do with the risk now?

What can a risk register look like?



BRITISH COLUMBIA

Risk Register

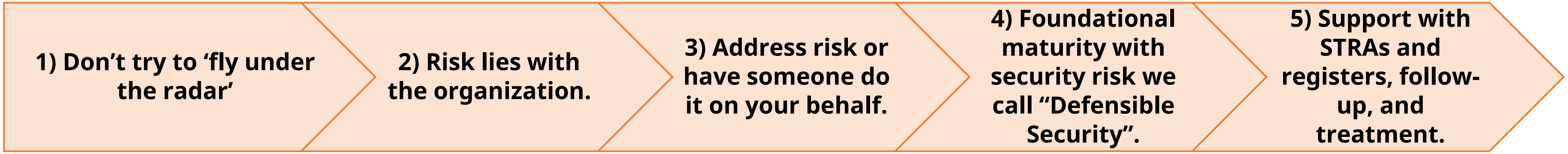
Risk ID	Risk Category	Risk Name	System or asset which is the subject of the risk?	Describe the threat (thing) which could act on the vulnerability	Describe the vulnerability which could be leveraged (exposure and weakness)	Likelihood Rating	Likelihood Rating # (Calculated)	Potential Impact Rating	Potential Impact Rating # (Calculated)	Describe the Potential Impact (what would it mean to the organization?)	Risk Rating #	Risk Rating	Planned Treatment?	Treatment assigned to (person)	Treatment target date?	Treatment complete?
1						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
2						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
3						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
4						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
5						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
6						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
7						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
8						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
9						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
10						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
11						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
12						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
13						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
14						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
15						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No
16						Rare	1	Negligible	1		1	LOW	Mitigate		YYYY-MM-DD	No

https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/vulnerability-risk-management/risk_register_template.xlsx

EXAMPLE

Risk ID	Risk Category	Risk Name	System or asset which is the subject of the risk?	Describe the threat (thing) which could act on the vulnerability	Describe the vulnerability which could be leveraged (exposure and weakness)	Likelihood Rating	Likelihood Rating # (Calculated)	Potential Impact Rating	Potential Impact Rating # (Calculated)	Describe the Potential Impact (what would it mean to the organization?)	Risk Rating #	Risk Rating	Planned Treatment?	Treatment assigned to (person)	Treatment target date?	Treatment complete?
1	Network and Device Security	Users are receiving a large quantity of PHISHING emails which are likely to result in harms to systems.	Workstations and other connected systems	Malicious actor using a phishing email to infect system with malware.	Users who are not adequately trained or aware of how to handle Phishing emails. Systems which are not sufficiently hardened with anti-malware software.	Likely	4	Major	4	Systems infected by a successful Phishing attack could result in a ransom situation or further lateral attacks by malware to other network devices. This could cause harms to confidentiality, availability, or integrity. Downstream this could cause reputational and financial harm.	16	HIGH	Mitigate	JOHN DOE	2122-01-01	No

Key take aways



1) Don’t try to ‘fly under the radar’

2) Risk lies with the organization.

3) Address risk or have someone do it on your behalf.

4) Foundational maturity with security risk we call “Defensible Security”.

5) Support with STRAs and registers, follow-up, and treatment.

Where can I find more on how to complete an STRA?

Government of B.C.

STRA site

https://www2.gov.bc.ca/gov/content?id=7175C19B66564EA3A343AB8B668BEFC2

Where can I find more on Information Security Risk Management?

Government of B.C.

Professional Development site

https://www2.gov.bc.ca/gov/content?id=56FE9F38FC2749B286B59C6D04D30A22

Thank you.

Any Questions?

Image Sources

Pixabay License

(https://pixabay.com/service/license-summary/)
Free for commercial use. No attribution required.

- https://pixabay.com/photos/cliff-leap-high-rock-boy-2699812/
- https://pixabay.com/photos/teds-couple-love-together-cute-1808323/
- https://pixabay.com/illustrations/rule-hook-check-mark-custom-1752622/
- https://pixabay.com/vectors/falling-hazard-warning-caution-24031/
- https://pixabay.com/vectors/man-doll-puppet-controlled-master-6853954/
- https://pixabay.com/illustrations/cyber-security-internet-security-1923446/
- https://pixabay.com/photos/scam-hacker-security-virus-fraud-4126798/
- https://pixabay.com/photos/cliff-leap-high-rock-boy-2699812/
- https://pixabay.com/photos/mountain-leap-high-rock-boy-2699809/
- https://pixabay.com/illustrations/rating-star-five-application-4068907/
- https://pixabay.com/vectors/bayesian-statistics-bell-curve-2889576/
- https://pixabay.com/photos/asteroid-comet-meteorite-3628185/
- https://pixabay.com/vectors/air-raid-bombing-raid-bomber-bomb-148909/
- https://pixabay.com/vectors/tank-cannon-weapons-t-34-war-6898680/
- https://pixabay.com/vectors/explosion-detonation-blast-burst-147909/
- https://pixabay.com/illustrations/smartboard-monitor-training-school-1523538/
- https://pixabay.com/photos/auto-repair-oil-change-oil-auto-3691962/
- https://pixabay.com/illustrations/thumbs-up-good-great-like-thumb-4423320/
- https://pixabay.com/photos/man-head-scared-cover-emotion-314481/
- https://pixabay.com/vectors/worker-craft-tools-craftsmen-6351121/
- https://pixabay.com/vectors/woman-business-point-hand-up-1453935/
- https://pixabay.com/illustrations/man-manager-employer-office-banker-5583395/
- https://pixabay.com/vectors/africa-african-comic-characters-2027628/
- https://pixabay.com/vectors/woman-engineer-work-worker-lady-1455991/
- https://pixabay.com/photos/house-architecture-front-yard-1836070/
- https://pixabay.com/vectors/tree-grenn-fruits-trunk-falling-158522/
- https://pixabay.com/photos/hacker-question-mark-hoodie-attack-2883630/
- https://pixabay.com/photos/poses-female-education-posing-1367416/

Creative Commons Attribution-Share Alike 3.0 Unported license.

(https://creativecommons.org/licenses/by-sa/3.0/)
Free to: Share — copy and redistribute the material in any medium or format. Adapt — remix, transform, and build upon the material for any purpose, even commercially.

- https://commons.wikimedia.org/wiki/File:SDLC_-_Software_Development_Life_Cycle.jpg

Creative Commons Attribution-Share Alike 4.0 International license.

(https://creativecommons.org/licenses/by-sa/4.0/)
Free to: Share — copy and redistribute the material in any medium or format. Adapt — remix, transform, and build upon the material for any purpose, even commercially.

- https://commons.wikimedia.org/wiki/File:Devops-toolchain.svg

Creative Commons Attribution-NonCommercial-ShareAlike (CC BY-NC-SA 2.0).

(https://creativecommons.org/licenses/by-nc-sa/2.0) Attribution: Judy Baxter
Free to: Share — copy and redistribute the material in any medium or format. Adapt — remix, transform, and build upon the material.

- https://www.flickr.com/photos/judybaxter/281024071
- https://live.staticflickr.com/87/281024071_d4fec7a1ec_o_d.jpg