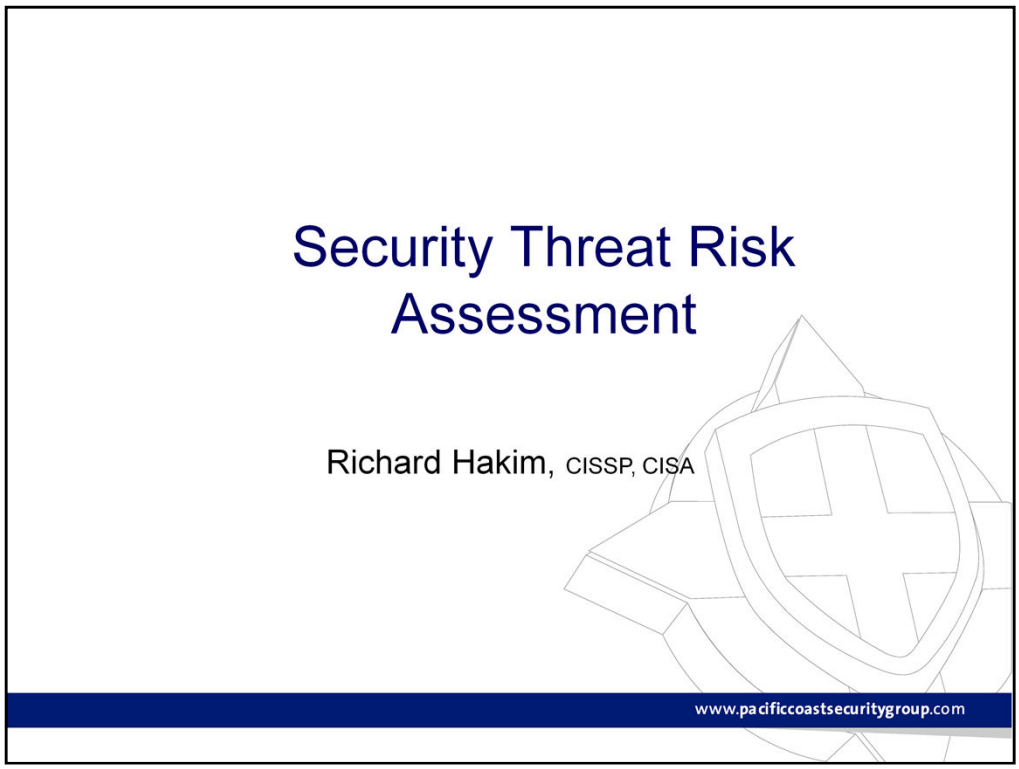
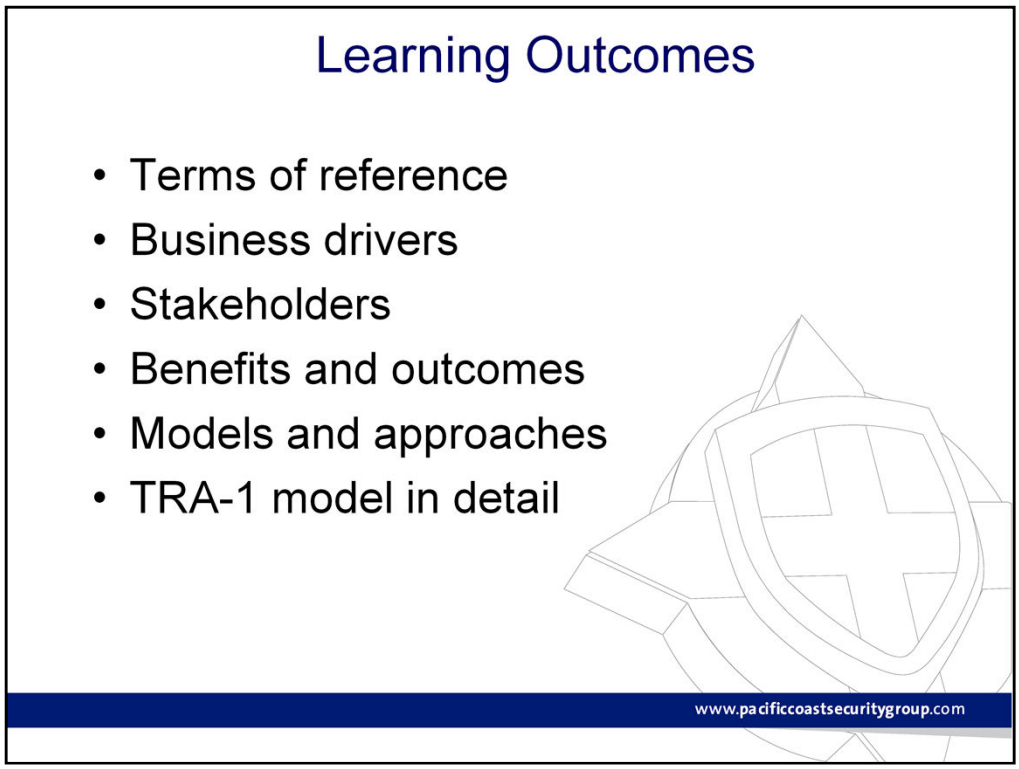


Security Threat and Risk Assessment

Format

The course materials will consist of:

- Two (2) hours of lecture
  - Discussion & white boarding
  - Terms of reference review
  - Slides for reference
- Printed course materials, including sources for further study and reference
- One (1) hour of case study



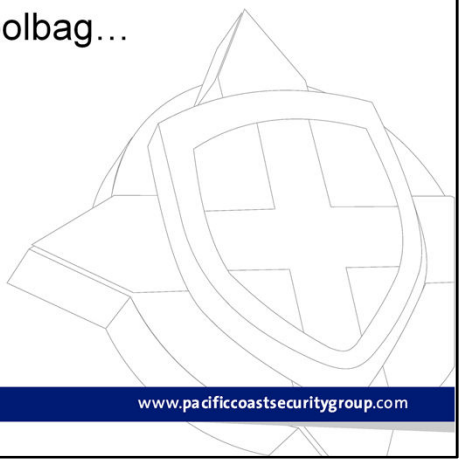
Awareness and understanding …

IT Security


Chinese hackers broke into Canadian government computers in January
February 17, 2011
CBC News reported yesterday that in January, a small group of Chinese hackers were successful in fooling Canadian federal IT staff into providing sensitive information as well as giving them access to government computers, leading to severe Internet restrictions at the Treasury Board and the Finance Department in Ottawa.
The news was also reported by other news outlets. Although the Canadian government has so far offered little information on the security breach, CBC added that the attack cut off Internet access for thousands of public servants, although service has slowly been returning to normal in the past week.
Microsoft Windows Azure™
See How Companies are Saving Money with Windows Azure. Try it For Free
Database Security Guide
Practical Guide to Database Security & Compliance. Free Copy!
SecureTech Canada
Canada's National Security & Public Safety Showcase
1 Hour PayDay Loans
Guaranteed Funding in 1 Hour Don't Pay it Back for 30 Days!
HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS
The New York Times
Asia Pacific
WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION
AFRICA | AMERICAS | ASIA PACIFIC | EUROPE | MIDDLE EAST
TAKE 25%
25% Off with
VANITY FAIR
TRENDING | SECTIONS | PHOTOS | VIDEO | BLOGS | MAGAZINE
Hollywood | Business | Politics | Culture | Society | Style
WE WIN!
IT Security Blog of the Year
nakedsecurity
News. Opinion. Advice. Research
malware | spam | social networks | data loss | law & order | apple | podcast | video
The new Audi A8 is here.
Luxury has progressed.
Disclaimer
Hotmail fights back against hacked email accounts
Widespread site compromise leading to Zeus
'Foreign government' hackers steal secret Pentagon plans
Get naked! Sign-up for our daily newsletter
you@example.com
Hit me!
Don't show me this again
by Graham Cluley on July 15, 2011 | Comments (3)
FILED UNDER: Data loss, Law & order, Malware, Vulnerability
The US Deputy Defense Secretary William Lynn has revealed that a foreign intelligence agency was behind a hack attack that stole classified information about a top secret weapons system.
According to Aviation Week, the weapons system, which is under development, might have to be redesigned after the files were stolen from a military contractor's computer network.
Plans and confidential blueprints were included in the haul of 24,000 files said
WEB EXCLUSIVE
August 2, 2011
Like 522 Tweet 461
ECURITY
ısive: Operation Shady RAT—
ecedented Cyber-espionage Campaign
ntellectual-Property Bonanza
st five years, a high-level hacking campaign—dubbed Operation Shady
infiltrated the computer systems of national governments, global
ons, nonprofits, and other organizations, with more than 70 victims in
ies. Lifted from these highly secure servers, among other sensitive
countless government secrets, e-mail archives, legal contracts, and
hematics. Here, Vanity Fair's Michael Joseph Gross breaks the news of
ı Shady RAT's existence—and speaks to the McAfee cyber-security
ıo discovered it. Related: "Enter the Cyber-dragon".
oseph Gross
www.pacificcoastsecuritygroup.com

IT Security

- Security Threat Risk Assessment…
  - What is risk?
  - What is risk assessment?
- STRA is one tool in the toolbag…
  - Risk modeling
  - Threat modeling
  - Risk assessments
  - War gaming
  - Audit
  - Vulnerability assessment
  - Penetration test



Risk Assessment, Modeling and War Gaming: (8:29 minutes)

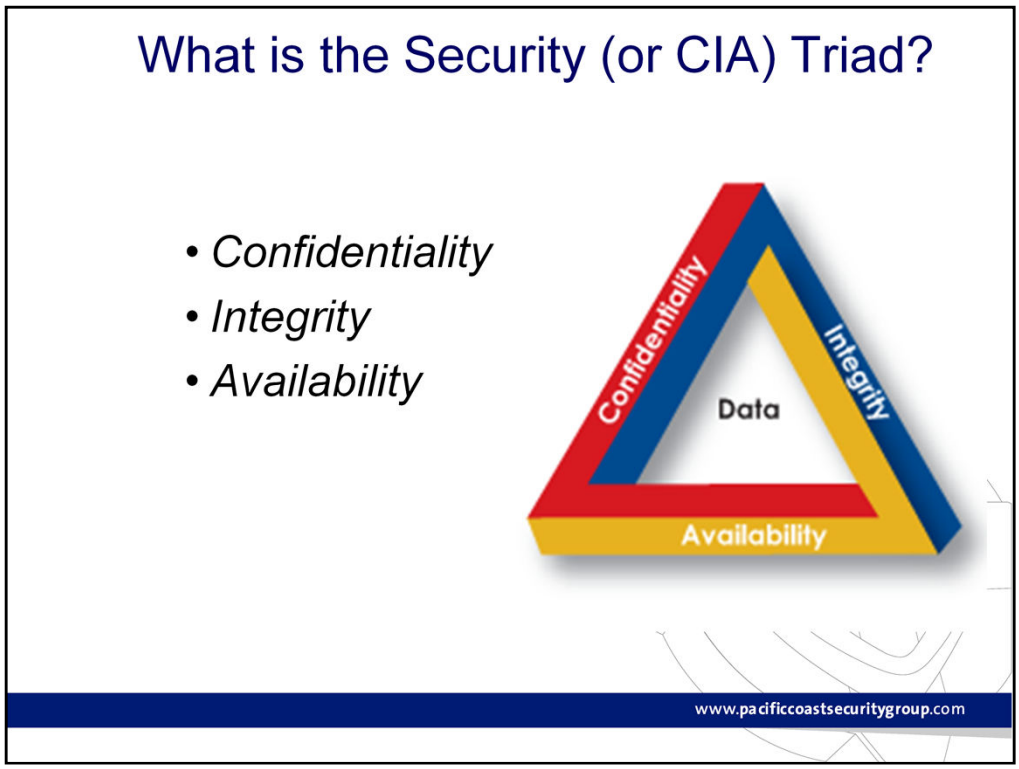
http://www.podtech.net/home/4482/security-plan-risk-assessment-modeling-and-war-gaming

It is a process.

Assessing potential impacts to:

- The people who operate the system
- The business functions that the system supports
- The tangible aspects of the system
- The intangible aspects of the organization

Recommending safeguards in accordance with the security triad



An organization's information security program must provide assurance that the core concepts of confidentiality, integrity and availability are understood and supported through the implementation of security safeguards designed to mitigate or reduce the risks of unauthorized disclosure, unauthorized modification or destruction, accidental corruption of information, and unplanned unavailability of information.

•A lack of security safeguards increases the risk to information in terms of viruses, destruction of data, external penetrations or denial of service attacks.

•The impacts to confidentiality, integrity and availability should be clearly understood when designing information systems processes.

•Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement.

Confidentiality

Only authorized users have access to information on a need-to-know basis.

Integrity

Information should be protected from intentional, unauthorized or accidental changes.

Availability

Information is accessible by users when needed.

No universally accepted security governance definition

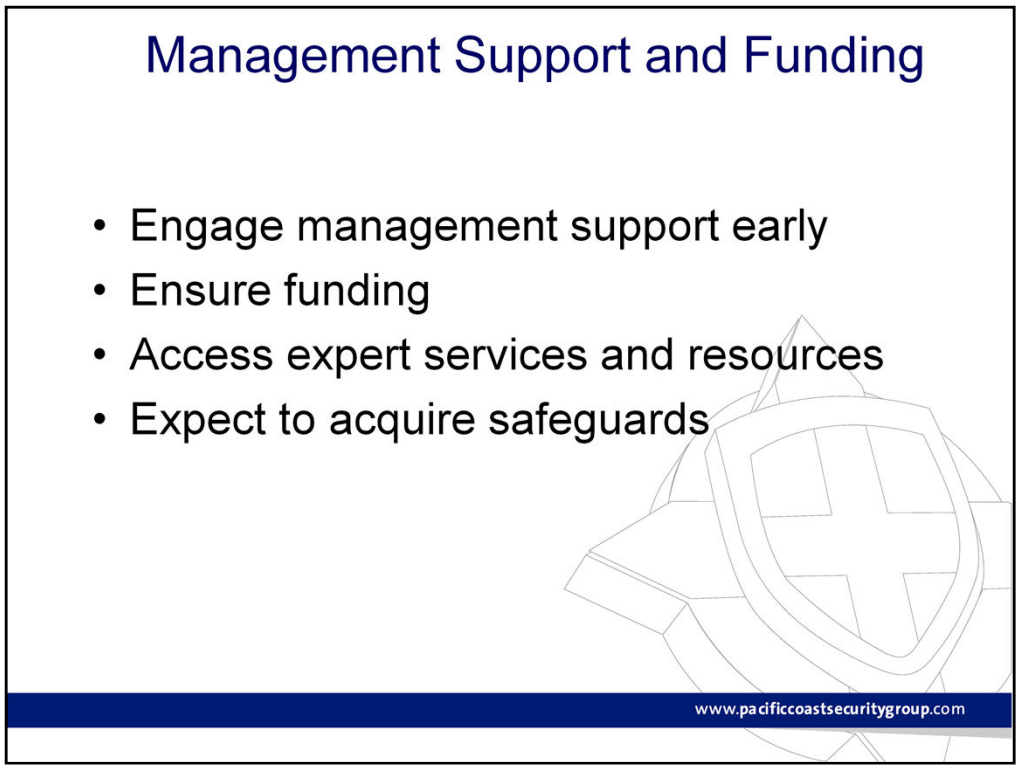
Further assurance that:

- Right activities are being performed
- The investment is being appropriately directed
- Executive management has access to program

Understanding applications, services, how they are designed, controls needed to secure them.

Desktop clients – think vs thin – risk, data security, ROI (5 minutes)

http://ipip.intel.com/go/tag/risk-assessment/



•Before engaging in a Security Threat Risk Assessment, it is essential that management support has been engaged and that funding has been allocated.

•A Security Threat Risk Assessment generally requires expert services and the dedication of a team of individuals to orchestrate the effort from beginning to end.

•Additionally, safeguards generally will require funding and resources to implement.

•Funding may involve both one-time and ongoing operating costs.

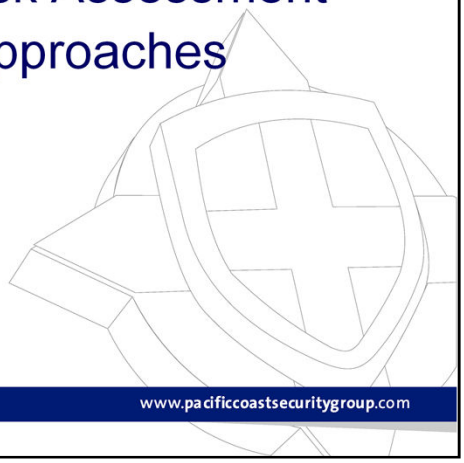
•Choose a standard to follow or comply with. What drives this choice?

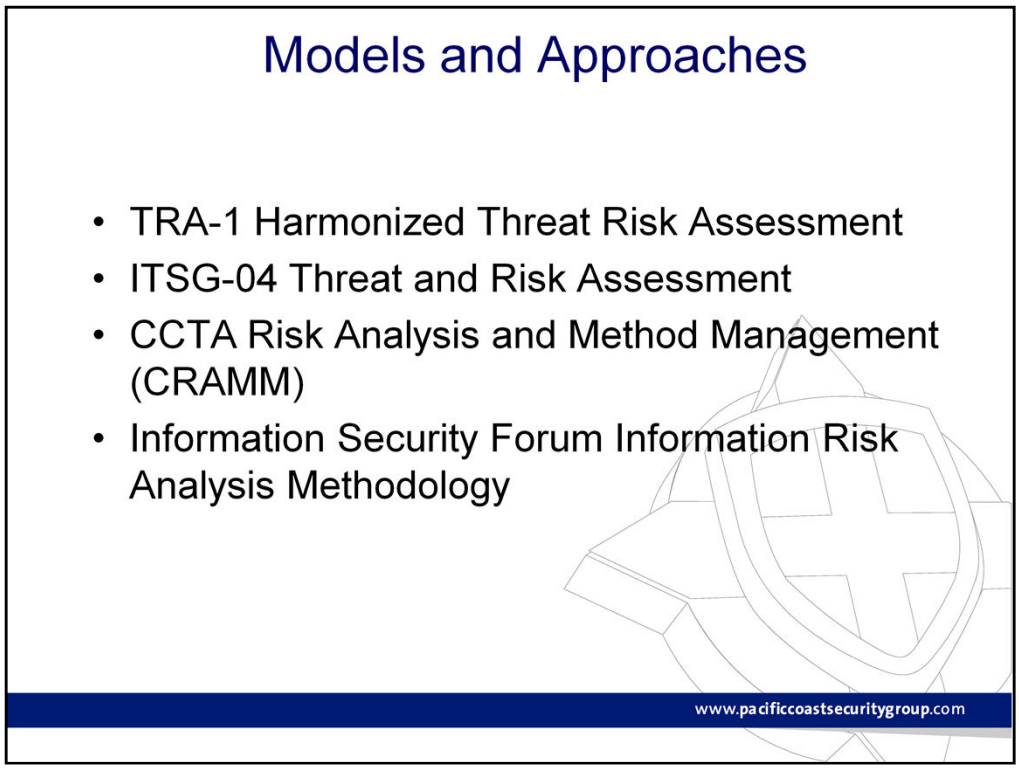
- •Your Industry might have it's own standard
- •You might be able to access open source (free) rather than costly license
- •Your country might have legislation

- Your business drivers could help you make this choice
- Personal biases or affiliation

- The important thing is that you pick your standard and can defend your choice!
- The next few slides contain some popular models and standards

Security Threat Risk Assessment Models and Approaches





Leading Threat Risk Assessment models:

•TRA-1 Harmonized Threat Risk Assessment Methodology was produced in 2007 by the RCMP and in use by the federal government

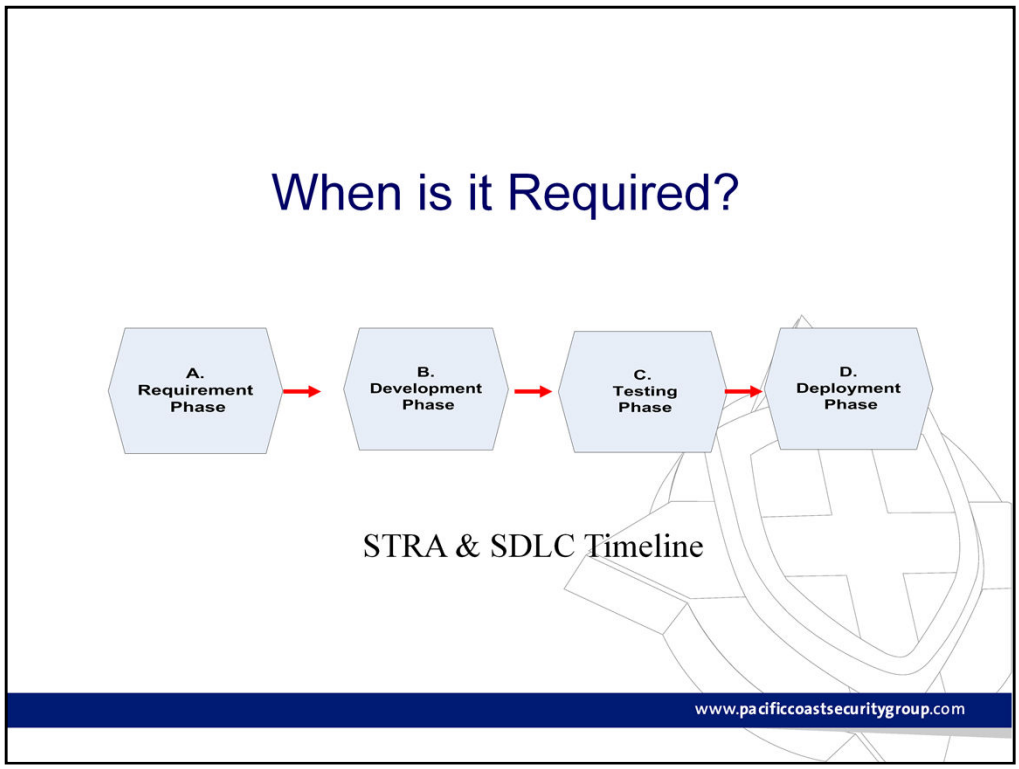
•ITSG-04 Threat and Risk Assessment Working Guide is a guide produced in 1999 by the federal government

•CCTA Risk Analysis and Method Management (CRAMM) is a risk analysis model produced in 1987, is usually associated with ITIL and ISO/IEC 17799.

Over the next few slides, we'll focus on the TRA-1 as it is a solid model that is readily accessible.

Obtaining the right balance

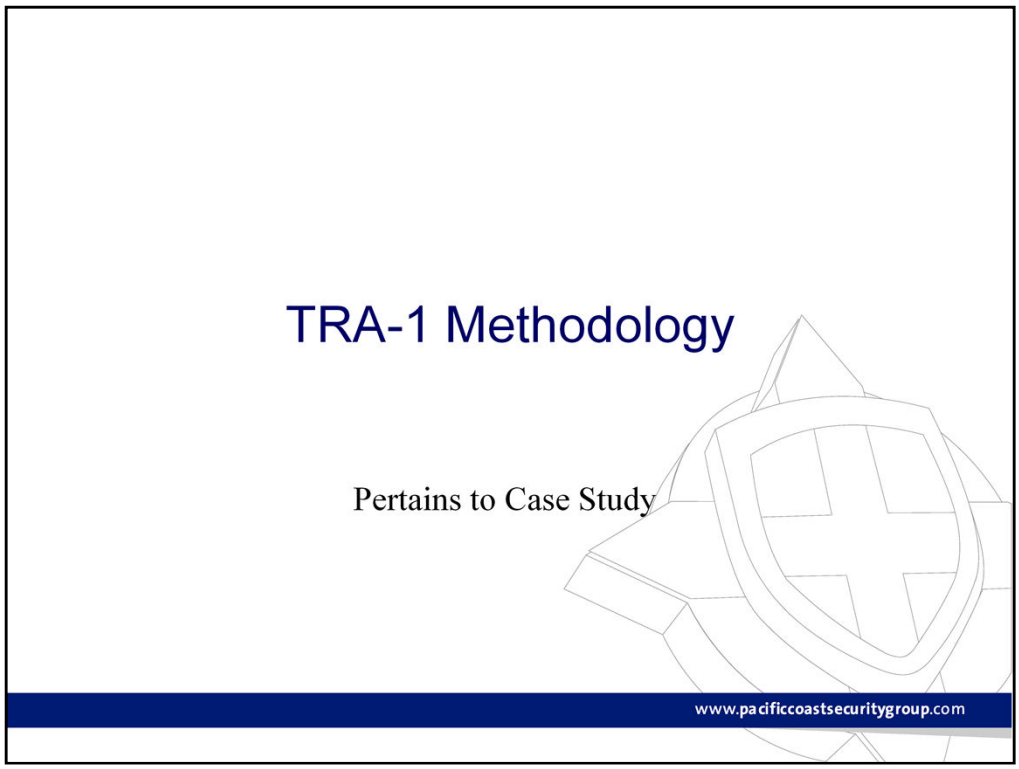
- Who is responsible?
  - Who determines “right balance”?
  - Who is the information owner, who is the custodian?
- What needs to be protected and why?
- What is the right level of security?



The manager responsible for the information asset establishes or formalizes the need and initiates the project.

Time bounding the assessment and managing it as a project will help to avoid scope creep and delays. It will also help to justify accessing and assigning resources.

The following five step process is based on the RCMP's Harmonized Threat Risk Assessment Methodology (TRA-1).

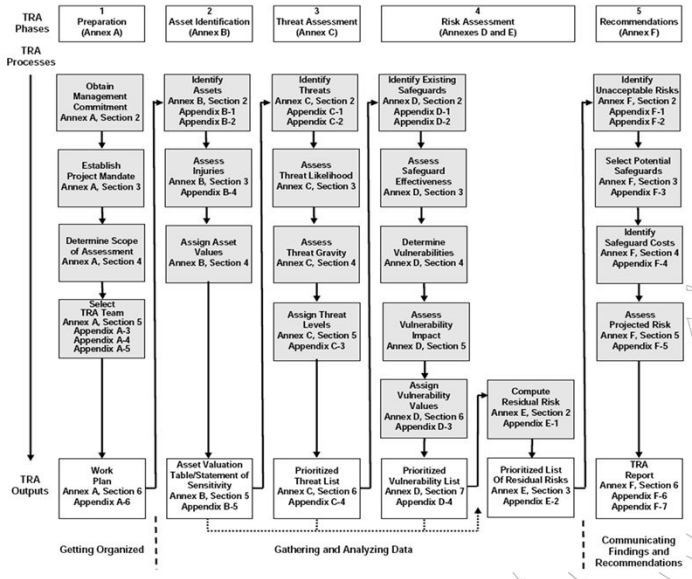


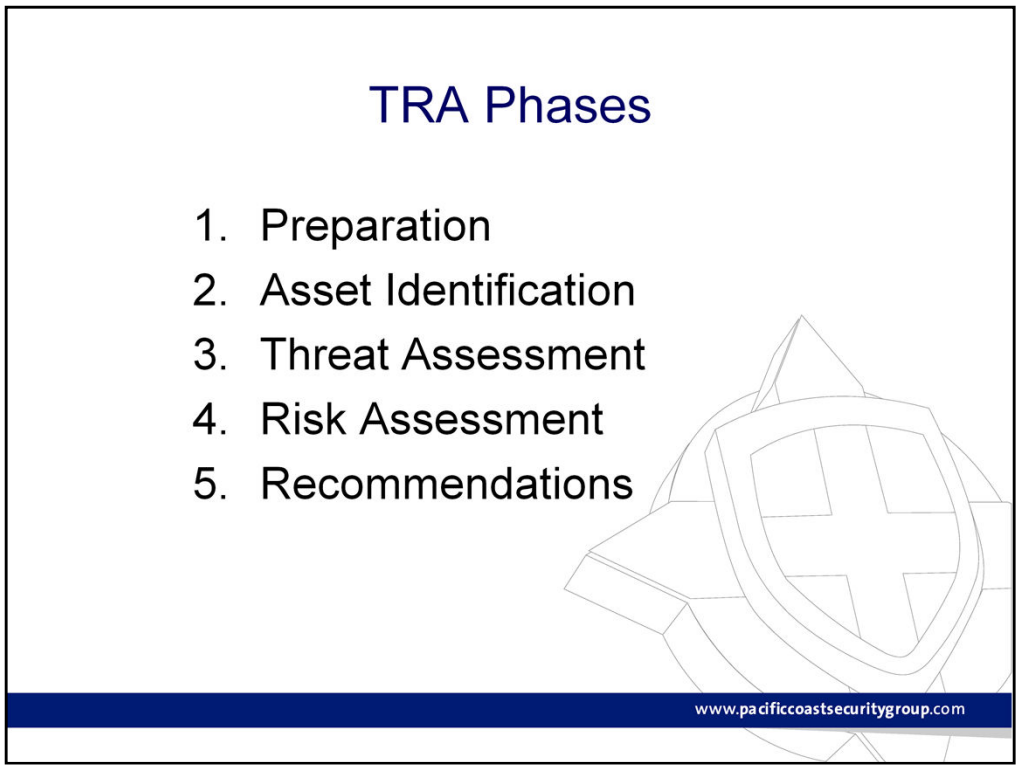
The following five step process is based on the RCMP's Harmonized Threat Risk Assessment Methodology (TRA-1). TRA-1 is well-suited for security threat risk assessments.

NOTE:

The course slides and handout materials include three templates and nine tables. In terms of the course slides and handout materials, the purpose of this course is not to go into detailed assessment and calculation but rather to give an overview of the process. The templates and tables should only be used as samples. The TRA-1 Methodology is readily available (online) and should be used as supplementary course reference material.

Structured Methodology





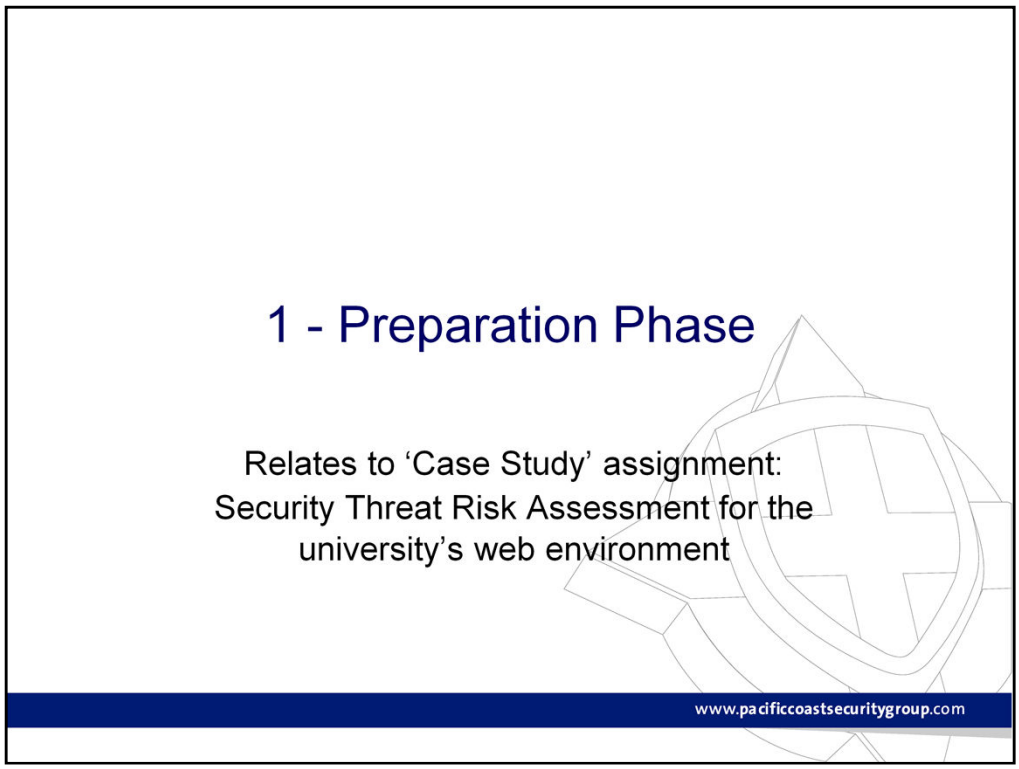
Here are the five phases associated with TRA-1.

Refer to the figures in the handout and we'll discuss flow.

It's worth mentioning again that threat risk assessments – any form – are linear and cyclical.

Linear – follow the process step-by-step (minor backing up is permitted)

Cyclical – repeat the process when required – periodic, contract expiration, change management driven, people changes, sourcing changes, etc.



Senior managers normally assign the responsibility for conducting a TRA to a single office or official with sufficient knowledge of both the business at hand and the selected TRA methodology. The designated official should first clarify the purpose of the TRA project in order to confirm both the feasibility of the exercise and the necessity for an assessment. Once these have been reviewed and accepted, relative roles and responsibilities should be specified, especially for the risk acceptance authority. Other issues to consider include project priorities, management expectations and reporting, all of which should be recorded in the TRA project Work Plan.

Establish TRA Project Mandate

1. Determine scope of assessment
2. Assign TRA Team
    - Team lead and members
    - Clear risk acceptance authority role
3. Prepare TRA Work Plan

While the actual level of detail will vary according to the scope and magnitude of the assessment, the TRA Work plan should record as a minimum:

- Mandate, purpose, scope and terms
- Team includes risk acceptance authority (who approves the TRA Work Plan)
- Project timelines

In an Security TRA, ensure to document the system scope and information assets

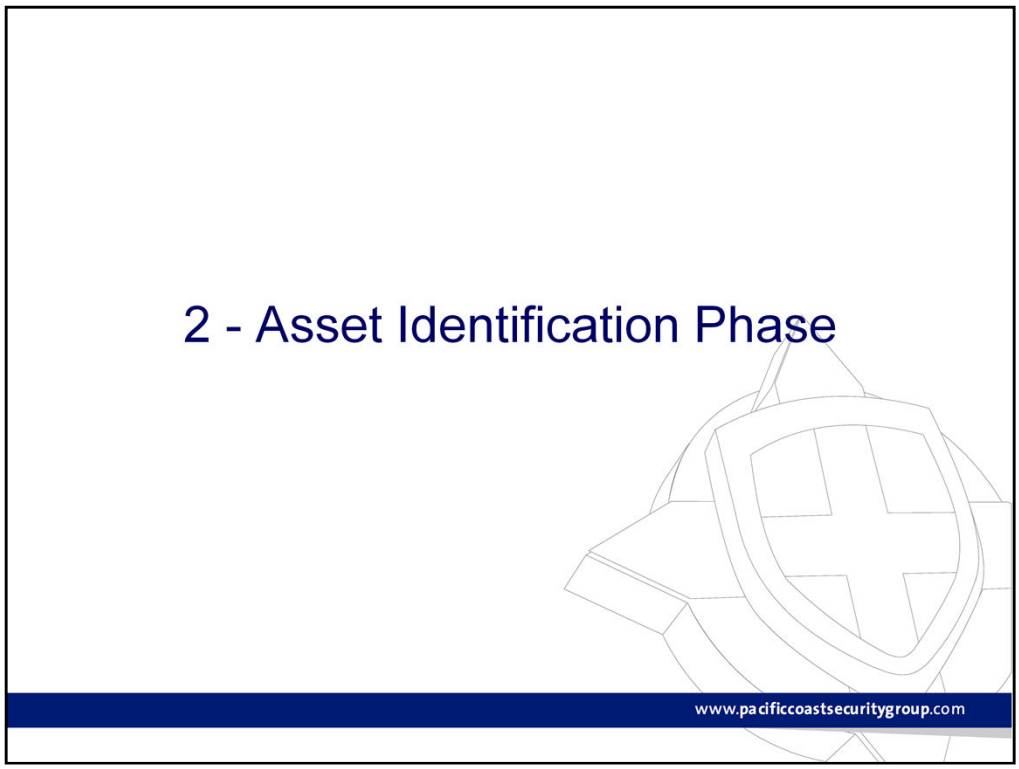
A project plan with target dates for each deliverable from:

- **the Asset Identification Phase**
- **to the final recommendations in the TRA Report**

Relevant logistics such as security screening, administrative support and resource requirements, including the source of funds for any related expenditures, such as consulting contracts.

Relevant inputs:

Previous TRA records
Privacy Impact Assessments
Business Impact Analysis
Design documentation, facility floor plans, inventory lists
Any relevant memoranda of understanding for the sharing of information or other assets.



Once the Preparation Phase is complete, the TRA team may commence asset identification and valuation. Purpose is to:

•facilitate the identification of assets at an appropriate level of detail,

•promote uniform asset valuation and permit comparative analysis amongst different assets or different values for the same asset, the guide also

Key output is a Statement of Sensitivity (Template 1)

•a list of employees, assets and services with relative values according to injury or impact.

Template on next slide.

Do this at an appropriate level of detail to determine who and what might require protection.

Using template, identify employee, tangible and intangible assets, and services at agreed upon level of detail.

Identify assets at *agreed level of detail*

•Assess the level of injury

•Categorize assets and services

•All assets have one or more CIA values

Asset Valuation Table

Template 1
Asset Valuation Table

				Asset Value					
Class	Category	Group	Univ IT Dept	Confid.	Avail Int	Avail op	Integrity	$	
People	Employees	Univ IT Dept Staff	Univ IT Dept		High	FB			
Tangible	Information	Univ IT Dept	Univ IT Dept	High	High		High		Cl
Tangible	Hardware	Univ IT Dept	Univ IT Dept		Medium				
Tangible	Firmware	Univ IT Dept	Univ IT Dept		Medium				
Tangible	Software	Univ IT Dept	Univ IT Dept		Medium				
Tangible	Facilities	University Campus	Univ IT Dept		High				
Tangible	Facilities	University Computer room	Univ IT Dept		High				Financial

To differentiate between varied threats and determine which are more likely to pose serious concerns.

Key output is Threat Assessment table (Template 2)

Note reference to Security Triad in template.

- **relative values reflecting their likelihood of occurrence and seriousness of their potential impact on confidentiality, availability and integrity.**

Helpful to group them in templates by asset affected

Here are steps that are covered over the next few slides:

1. Identify realistic or plausible threats
2. Classify threats by type
3. Assess threats
    - Likelihood of occurrence (Table 1)
    - Gravity should it materialize (Table 2)

- Threat Level (Table 3)

1. To reduce variability in response, use supporting tables provided
2. Compile and prioritize

Threat Assessment Table

Template 2
Threat Assessment Table

Asset Assessed:						Threat Levels Affecting			
ID No.	Class	Agent	Event	Likeli-hood	Gravity	Confid.	Avail.	Integrity	Univ IT Dept
31.	Deliberate	Individuals	Network Exploitation						Univ IT Dept
32.	Deliberate	Individuals	Social Engineering						Univ IT Dept
40.	Deliberate	Groups/Individuals	Delete/Destroy Records						Univ IT Dept
41.	Deliberate	Groups/Individuals	Corrupt Data						Univ IT Dept
42.	Deliberate	Groups/Individuals	Encrypt Files						Univ IT Dept
43.	Deliberate	Groups/Individuals	Misconfigure Software						Univ IT Dept
44.	Deliberate	Groups/Individuals	Misconfigure Hardware						Univ IT Dept
46.	Deliberate	Wannabees	Denial of Service Attacks						Univ IT Dept
47.	Deliberate	Wannabees	Malicious Code						Univ IT Dept
48.	Deliberate	Wannabees	File Corruption						Univ IT Dept
60.	Deliberate	Script Kiddies	Web Defacement						Univ IT Dept
94.	Deliberate	Hackers	Identity Theft						Univ IT Dept
103.	Deliberate	Companies	Patent Infringement						Univ IT Dept
106.	Deliberate	Individuals	Spam						Univ IT Dept
108.	Deliberate	Individuals	Unauthorized Use						Univ IT Dept
118.	Accidents	Individuals	Inaccurate Data Input						Univ IT Dept
121.	Accidents	Office Staff	Delete Files						Univ IT Dept
122.	Accidents	Office Staff	Spill Coffee/Other Liquids						Univ IT Dept
126.	Accidents	Cleaning Staff	Unplug Equipment						Univ IT Dept
127.	Accidents	Individuals	Lose Notebook Computers						Univ IT Dept
129.	Accidents	Data Entry Clerks	Data Entry Errors						Univ IT Dept
130.	Accidents	Data Base Admin.	Operating Errors						Univ IT Dept
131.	Accidents	Companies	Software Bugs						Univ IT Dept
132.	Accidents	Organizations	Software Integration Errors						Univ IT Dept
133.	Accidents	Individuals	Coding Errors						Univ IT Dept
134.	Accidents	Individuals	Software Configuration Errors						Univ IT Dept
135.	Accidents	Companies	Design Flaws						Univ IT Dept
136.	Accidents	Companies	Equipment Malfunction						Univ IT Dept
137.	Accidents	Organizations	Installation Errors						Univ IT Dept
138.	Accidents	Individuals	Hardware Configuration Errors						Univ IT Dept
139.	Accidents	Individuals	Operator Errors/Misuse						Univ IT Dept
147.	Accidents	Individuals	Inadvertent Misuse						Univ IT Dept
156.	Accidents	Equipment Operators	Disrupt Production						Univ IT Dept
208.	Natural Hazards	Dust	Media Contamination						Univ IT Dept

Note: Seccuris tables include approximately 300 threats. I've selected approximately 50 threats to do with information security

Threat Likelihood Table

Table 1
Threat Likelihood Table

Past Frequency	Same Location Similar Assets	Remote Location but Similar Assets OR Same Location but Different Assets	Remote Location Other Assets
Daily	High	High	High
1-10 Days	High	High	Medium
10-100 Days	High	Medium	Low
100-1,000 Days	Medium	Low	Very Low
1,000-10,000 Days	Low	Very Low	Very Low
Over 10,000 Days	Very Low	Very Low	Very Low

Select likelihood in pink column.

FOR EACH THREAT:

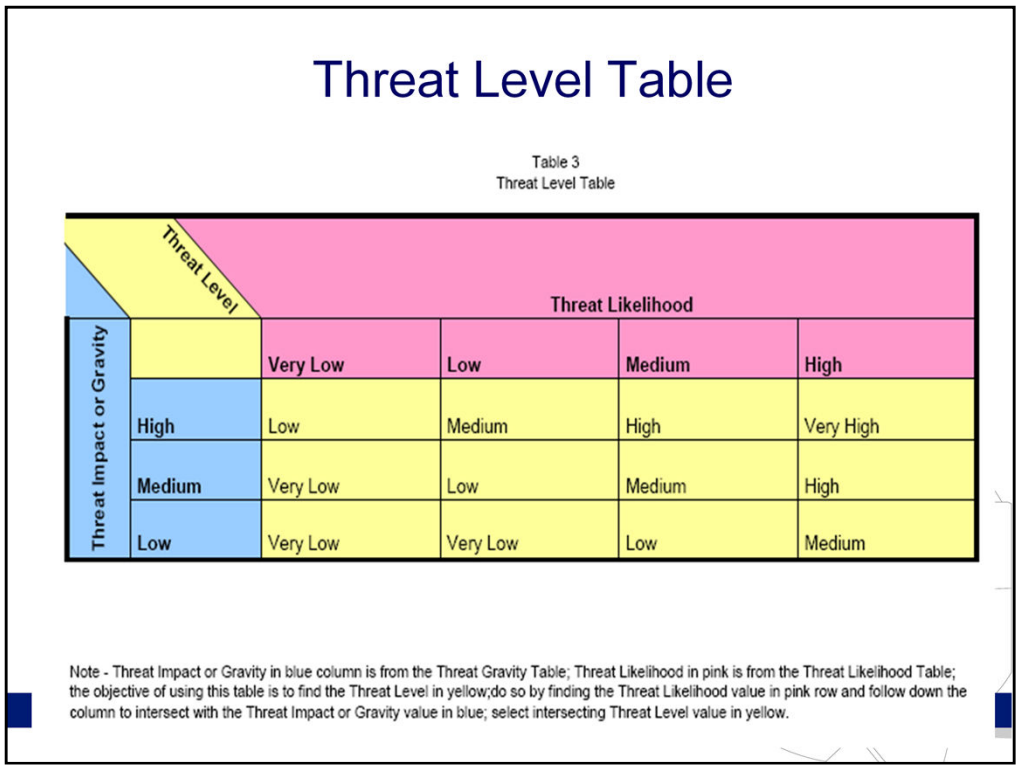
When did threat last materialize?

Threat Gravity Table

Table 2
Threat Gravity Table

Deliberate Threat Agent Capabilities	Magnitude of Accidents or Natural Hazards	Threat Impact or Gravity
Extensive Knowledge/Skill Extensive Resources	Highly Destructive Extremely Grave Error Widespread Misuse	High
Limited Knowledge/Skill Extensive Resources OR Extensive Knowledge/Skill Limited Resources OR Moderate Knowledge/Skill Moderate Resources	Moderately Destructive Serious Error Significant Misuse	Medium
Limited Knowledge/Skill Limited Resources	Modestly Destructive Minor Error Limited Misuse	Low

Select gravity based on threat agent or class. Look at threat in table. What type of threat is it? Look at Gravity table. Select appropriate entry.

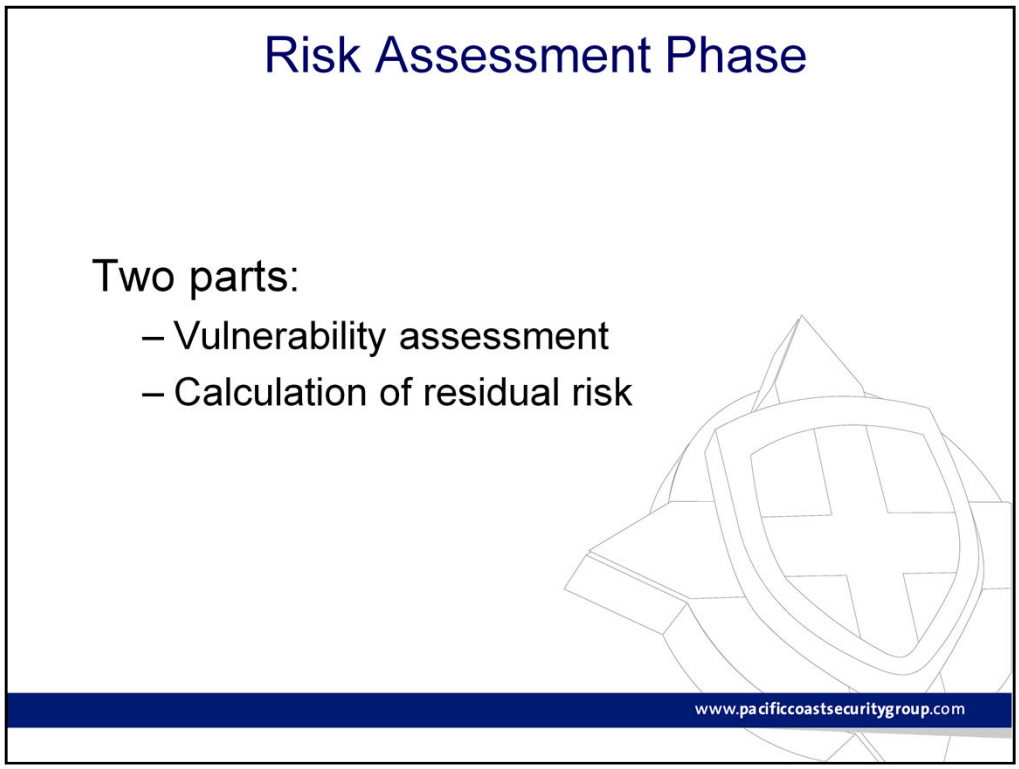


Explained on the slide.

Proceed to complete the threat assessment table.

You should now have a completed threat assessment template – template 2

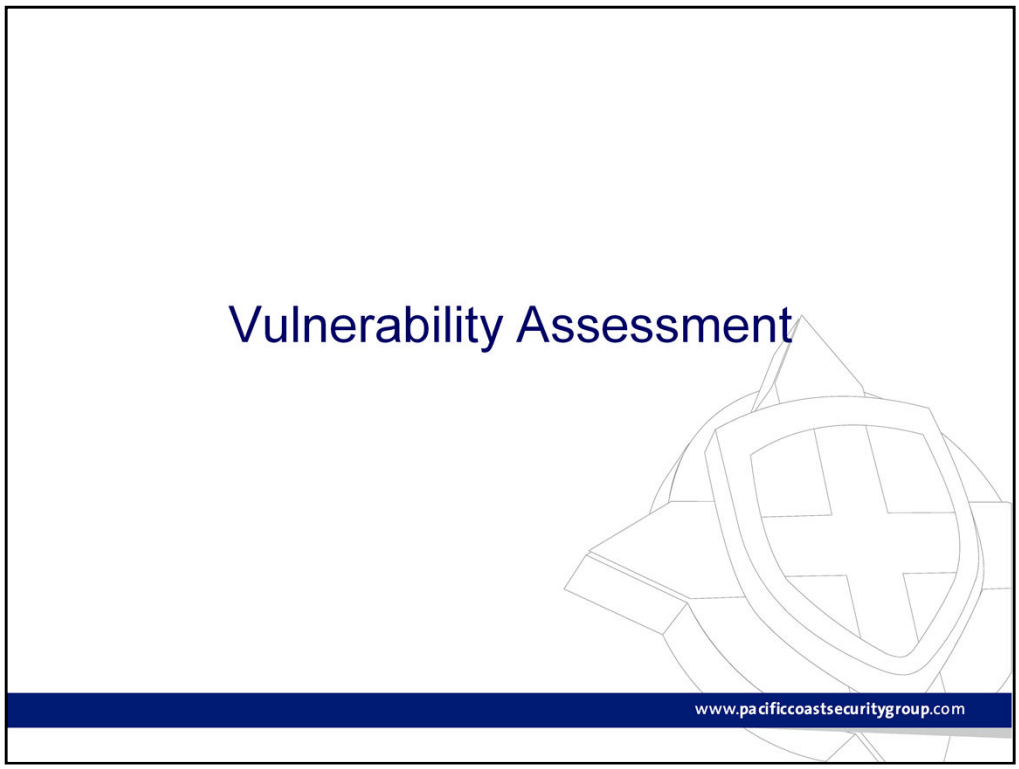
4 – Risk Assessment Phase



The TRA team must measure the effectiveness of existing safeguards and those pending implementation.

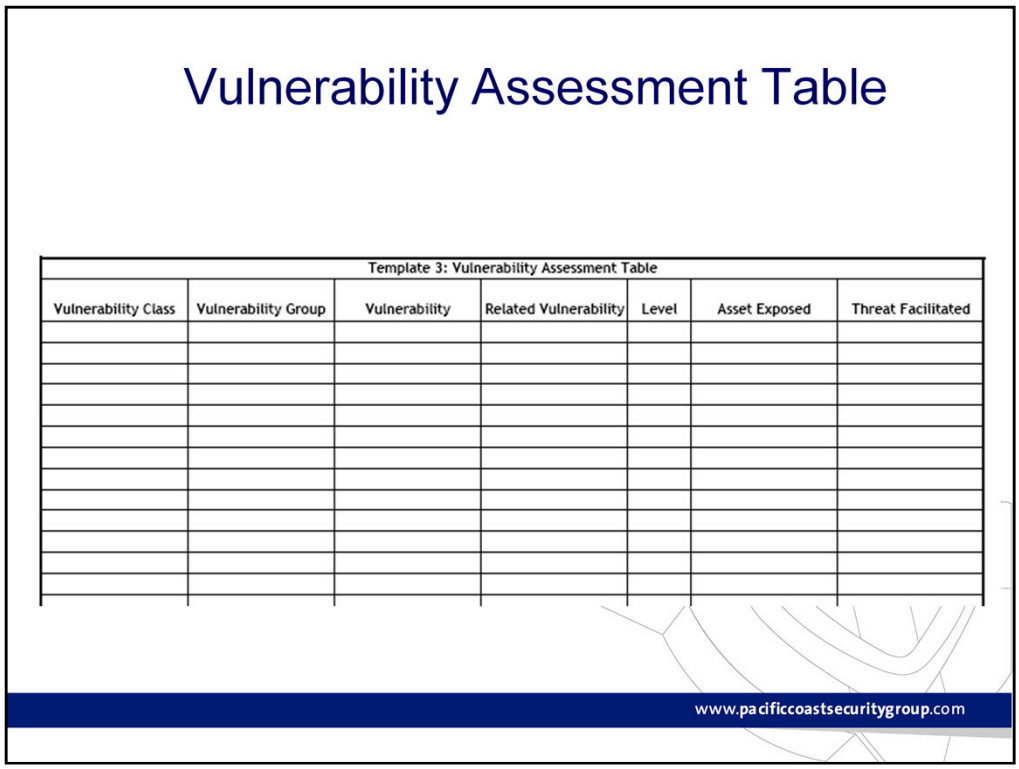
Analyzing data reveals attributes of employees and assets or the environment in which they operate that render them susceptible to compromise.

The assessment of vulnerabilities may be complicated by a common misperception that they are always security weaknesses or flaws.



Purpose is to identify and assess effectiveness of existing and proposed safeguards:

- Determine remaining vulnerabilities
- Assess impact (Table 5)
- Assess severity of outcome (Table 6)
- Assign vulnerability level (Table 7)
- Compile and prioritize the Vulnerability Assessment Table (Template 3)



While many vulnerabilities are negative attributes, others are positive qualities that simply have potentially adverse side effects.

As with asset and threat values, simple metrics are established to rate different vulnerabilities from Very Low to Very High.

Identify vulnerabilities.

Vulnerability Impact on Probability of Compromise

Table 5: Vulnerability Impact on Probability of Compromise (Prevention)		
Safeguard Effectiveness	**Associated Vulnerabilities**	**Probability of Compromise**
No Safeguard Safeguard Largely Ineffective Probability of Compromise > 75%	Easily Exploited Needs Little Knowledge/Skill/Resources Assets Highly Accessible Assets Very Complex/Fragile/Portable Employees Ill-Informed/Poorly Trained	High
Safeguard Moderately Effective Probability of Compromise 25-75%	Not Easily Exploited Needs Some Knowledge/Skill/Resources Assets Moderately Accessible Assets Fairly Complex/Fragile/Portable Moderate Employee Awareness/Training	Medium
Safeguard Very Effective Probability of Compromise < 25% (Safeguard Performs Only Detection, Response or Recovery Functions)	Difficult to Exploit Needs Extensive Knowledge/Skill/Resources Assets Highly Accessible Assets Very Simple/Robust/Static Employees Well-Informed/Trained	Low (Not Applicable)

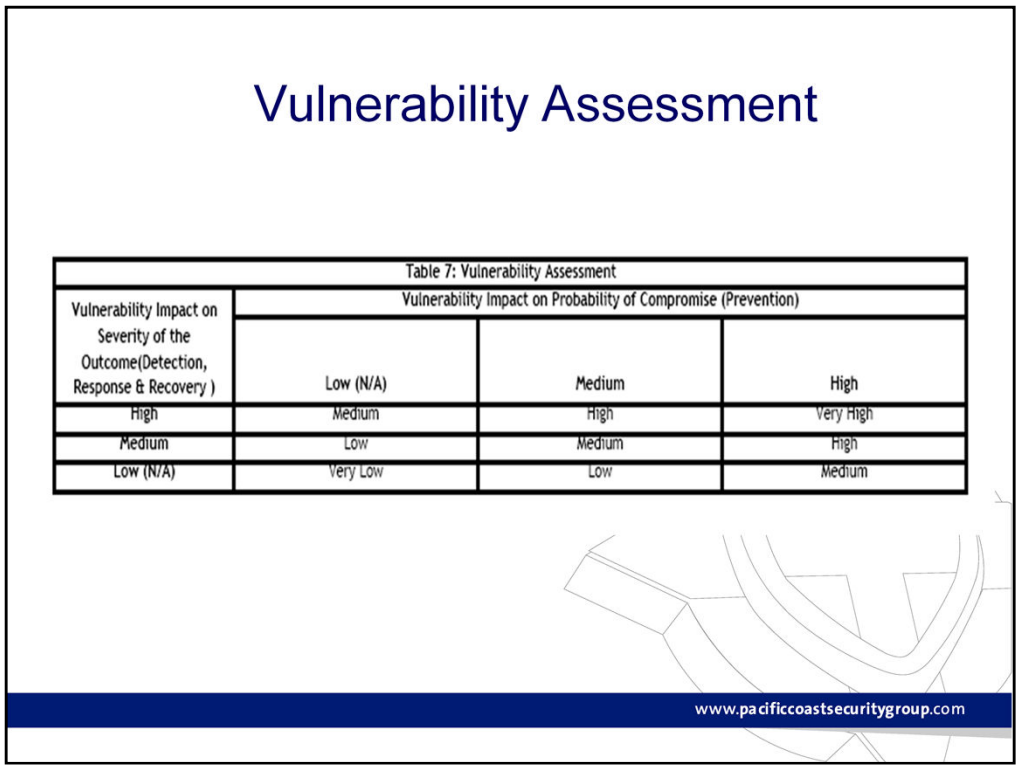
Prevention safeguard -- Identify safeguard effectiveness and select associated vulnerability and probability of compromise.

Vulnerability Impact on Severity of the Outcome

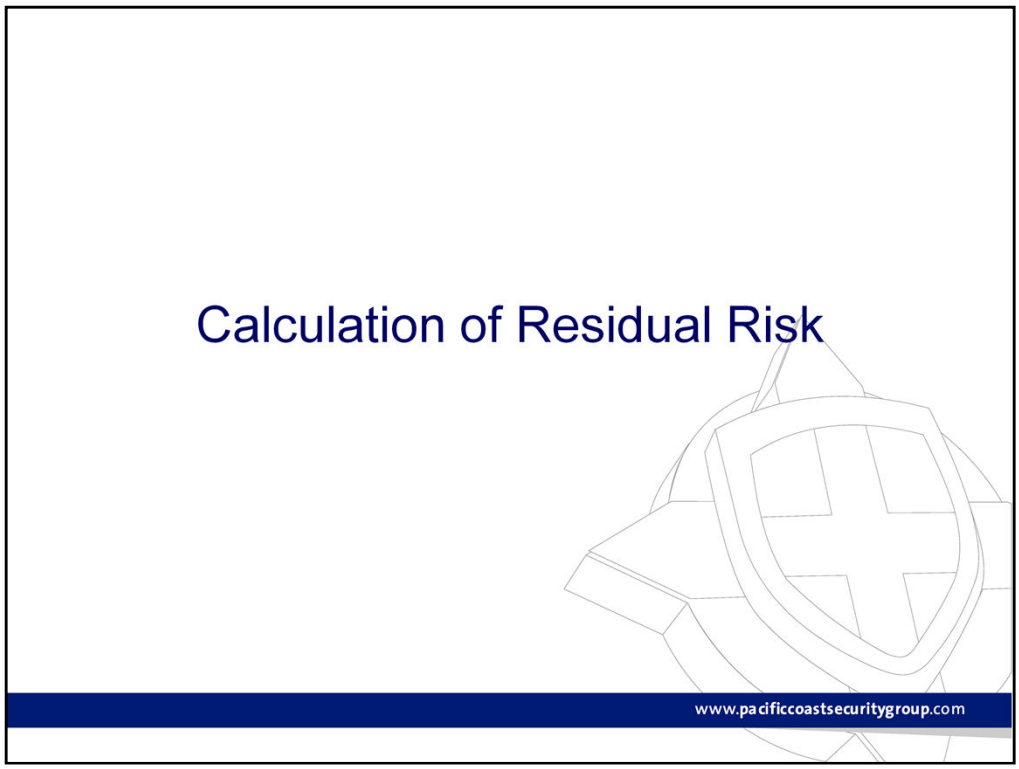
Table 6: Vulnerability Impact on Severity of the Outcome (Detection, Response or Recovery)

Safeguard Effectiveness	Associated Vulnerabilities	Severity of Outcome
No Safeguard Safeguards Largely Ineffective Assets Exposed to Extensive Injury	Unlikely to Detect Compromise Damage Difficult to Contain Prolonged Recovery Times/Poor Service Levels Assets Very Complex/Fragile Employees Ill-Informed/Poorly Trained	High
Safeguard Moderately Effective Assets Exposed to Moderate Injury	Compromise Probably Detected Over Time Damage Partially Contained Moderate Recovery Times/Service Levels Assets Fairly Complex/Fragile Moderate Employee Awareness/Training	Medium
Safeguard Very Effective Assets Exposed to Limited Injury (Safeguard Performs Only a Prevention Function)	Compromise Almost Certainly Detected Quickly Damage Tightly Contained Quick and Complete Recovery Assets Very Simple/Robust Employees Well-Informed/Trained	Low (Not Applicable)

Detection, Response or Recovery Safeguard -- Identify safeguard effectiveness and select associated vulnerability and severity of outcome.



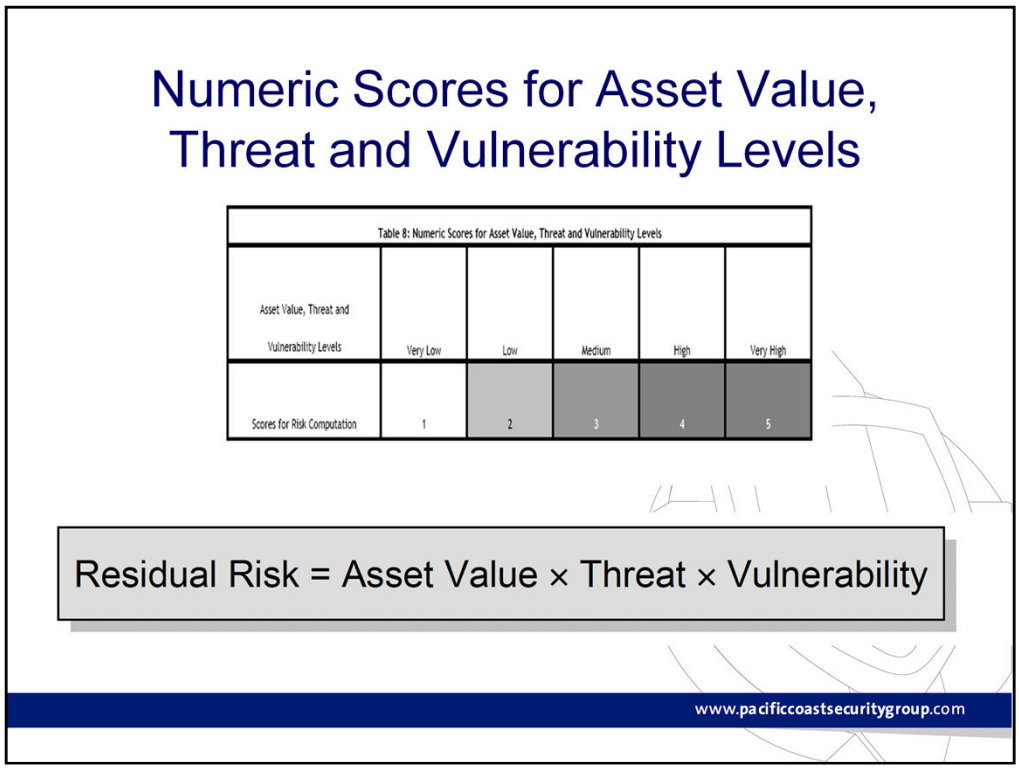
Using the values from previous tables, select vulnerability of impact on probability of compromise and enter into vulnerability assessment template 3.



Compute Residual Risk

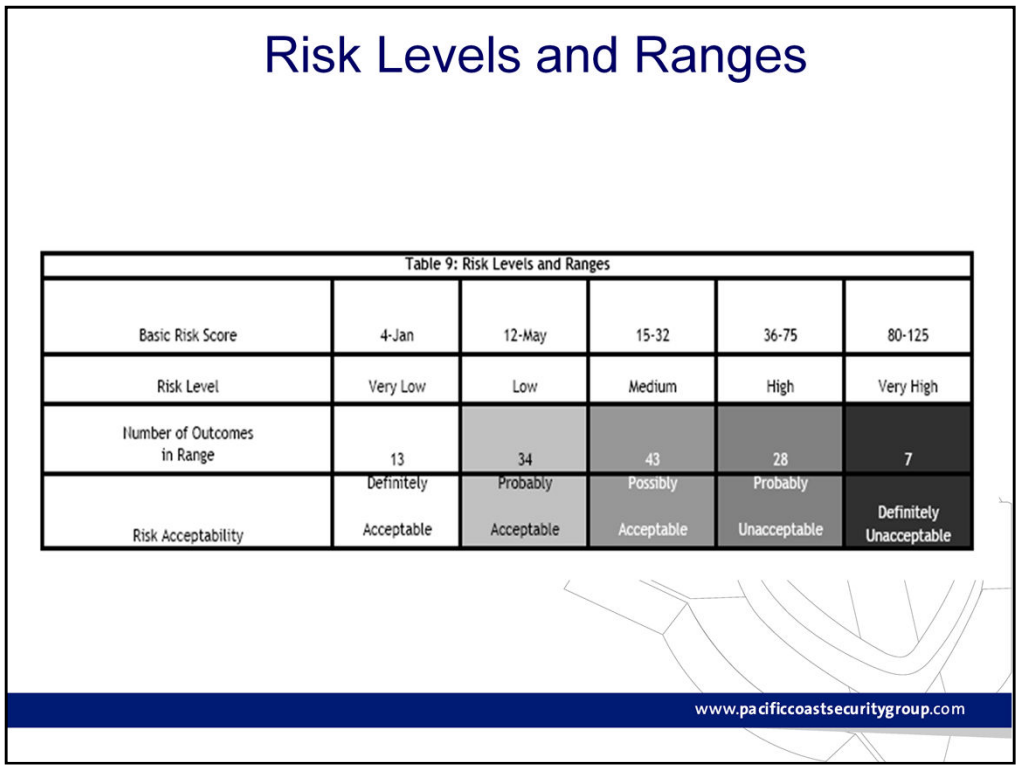
- Basic risk calculation (Table 8))
- Risk levels (Table 9)

Compile Prioritized List of Assess Residual Risks



Can be extensive!

This table illustrates the numeric scores for the vulnerability levels.



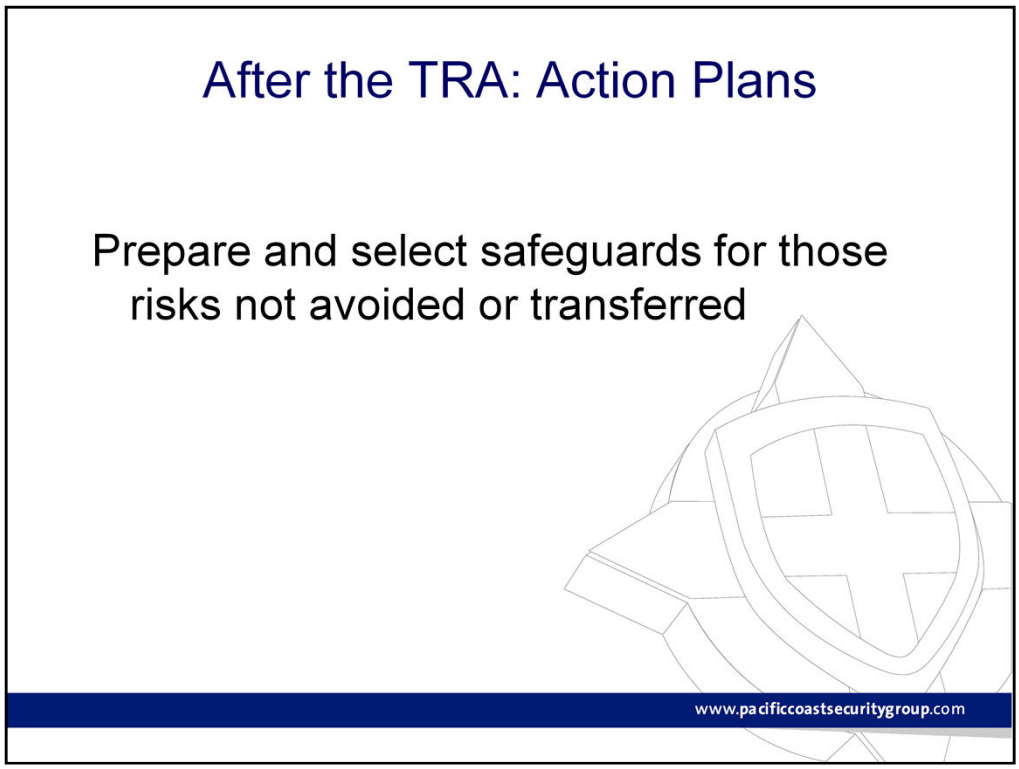
This table illustrates the risk levels and ranges.

NOTE:

This has been a very fast snapshot of the threat risk assessment process. The TRA-1 Methodology includes these templates and detailed description of uses as well as examples. It is publicly available.

Once the assessed residual risks have been identified, assigned relative levels from Very Low to Very High and subsequently prioritized, the TRA team must prepare suitable recommendations for the risk acceptance authority.

- Identify unacceptable residual risks
- Select potential security safeguards
- Identify direct / indirect costs and benefits
- Assess projected residual risks
- Prepare final TRA Report



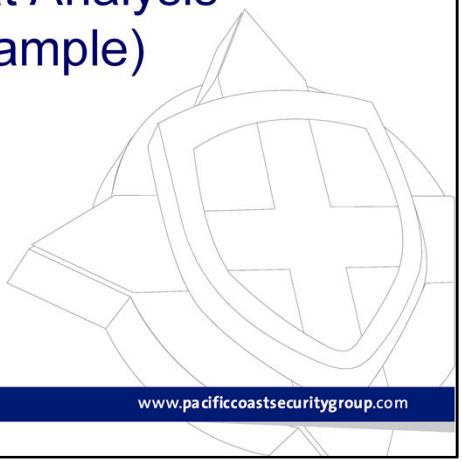
This is a cyclical process, meaning that the program does not end when the safeguards are implemented, but rather risks will again be assessed to assure that the safeguard and control remains effective.

Once recommendations have been accepted,

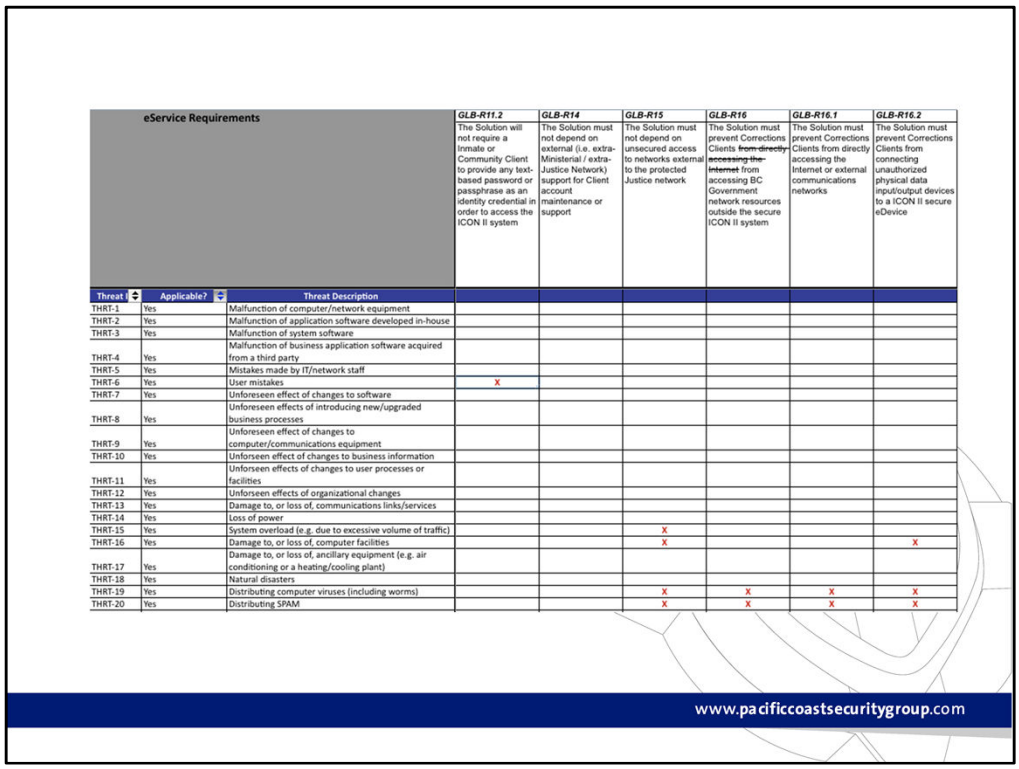
Safeguards will be constructed and implemented, certified, accredited, and integrated into operations.

An acceptance process is certified and accredited by the risk acceptance authority.

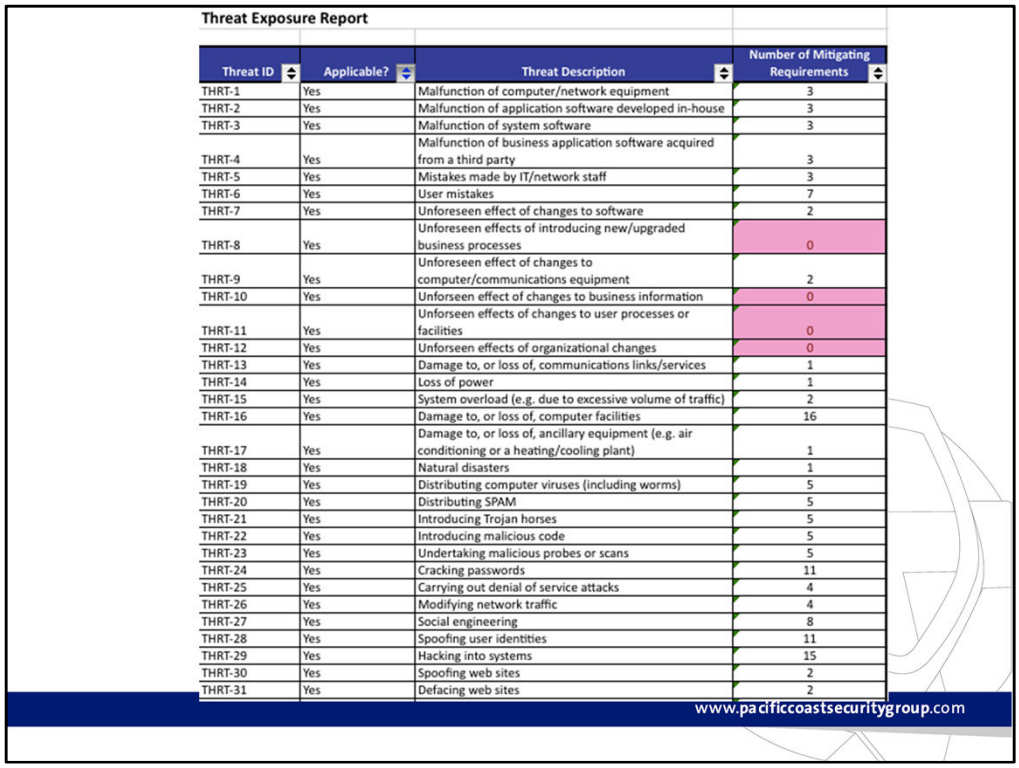
Internal Threat Analysis
(A Live Example)



Threat ID	Category of Threat	Source	Applicable	Threat Description	Additional Threat Information
THRT-38	Internal Misuse/Abuse	IRAM Threat Data Tool	Yes	Disclosing business information	Unauthorized disclosure of business information (e.g. confidential financial information)
THRT-39	Internal Misuse/Abuse	IRAM Threat Data Tool	Yes	Changing system preferences without authorization	Changing system privileges to either enable or deny access to information or functionality
THRT-40	Internal Misuse/Abuse	IRAM Threat Data Tool	Yes	Gaining unauthorised access to systems or networks	Deliberately gaining access to computer systems or networks to which a user is not authorized (e.g. by means of password theft or other covert action)
THRT-41	Internal Misuse/Abuse	IRAM Threat Data Tool	Yes	Modifying or inserting transactions, files or databases without authorization	Changing or adding transactions, files, or databases to produce unauthorized system behaviour or actions
THRT-42	Internal Misuse/Abuse	IRAM Threat Data Tool	Yes	Changing or adding software without authorization	Changing or adding software to produce unauthorized system behavior or action (e.g. to bypass mechanisms introduced to prevent fraud)
THRT-43	Internal Misuse/Abuse	IRAM Threat Data Tool	Yes	Misusing systems to cause disruption	Using authorized system facilities in a malicious or excessive manner to adversely affect system performance and availability (e.g. by downloading or uploading high volume .mp3 or .mpeg files)
THRT-44	Internal Misuse/Abuse	IRAM Threat Data Tool	Yes	Misusing systems to commit fraud	Using authorized systems to defraud the organization (e.g. diverting goods to false delivery addresses)
THRT-45	Internal Misuse/Abuse	Biometric Working Grou	Yes	Low level of registration and credential assurance levels for ICON system administrators with access to Bio Store	System administrators that have access to the bio store may have a lower level of registration and credential assurances than required by accessible data, leading to possibility for misidentification and compromised credentials
THRT-46	Theft	IRAM Threat Data Tool	Yes	Theft of portable computers and storage devices	Easily portable computers and components including PCs, PDAs, memory chips, and other detachable devices
THRT-47	Theft	IRAM Threat Data Tool	Yes	Theft of proprietary business information	Theft of business information (e.g. customer lists, product designs, intellectual propery)
THRT-48	Theft	IRAM Threat Data Tool	Yes	Theft of authentication information/devices (e.g. passwords or smart cards)	Theft of authentication information (e.g. user id, passwords, or PIN numbers)
THRT-49	Theft	IRAM Threat Data Tool	Yes	Theft of identity information (e.g. as a result of phishing)	Theft of personally identifiable information (e.g. credit card numbers, employment IDs, personal health details)
THRT-50	Theft	IRAM Threat Data Tool	Yes	Theft of licensed software	Theft of licensed software is typically known as software piracy (ie. the illegal copying and use of unlicensed software)
THRT-51	Theft	IRAM Threat Data Tool	Yes	Theft of computer programs or methodologies	Theft of computer programs or methodologies typically developed in house
THRT-52	Internal Misuse/Abuse	Provisioning Working Gr	Yes	Database administrators accessing/viewing personally identifiable information and/or edisclosure information	
				Prison riot	
				Attack on prison / community office from outside	
THRT-53	External Attack	RCMP TRA Methodolog	No	War: military invasion by nation states	Deliberate
THRT-54	External Attack	RCMP TRA Methodolog	No	War: information operations by nation states	Deliberate
THRT-55	External Attack	RCMP TRA Methodolog	No	War: insurrection by revolutionaries	Deliberate
THRT-56	External Attack	RCMP TRA Methodolog	No	War: guerrilla warfare by rebels	Deliberate
THRT-57	External Attack	RCMP TRA Methodolog	No	Espionage: COMINT by hostile intelligence services	Deliberate
THRT-58	External Attack	RCMP TRA Methodolog	No	Espionage: ELINT by hostile intelligence services	Deliberate
THRT-59	External Attack	RCMP TRA Methodolog	No	Espionage: FISINT by hostile intelligence services	Deliberate
THRT-60	External Attack	RCMP TRA Methodolog	No	Espionage: Emanations interception by hostile intelligence services	Deliberate
THRT-61	External Attack	RCMP TRA Methodolog	Maybe	Espionage: Network Exploitation by hostile intelligence services	Deliberate
THRT-62	External Attack	RCMP TRA Methodolog	Maybe	Espionage: HUMINT by hostile intelligence services	Deliberate
THRT-63	External Attack	RCMP TRA Methodolog	No	Espionage: IMINT by hostile intelligence services	Deliberate
THRT-64	External Attack	RCMP TRA Methodolog	No	Espionage: Open Source Collection by hostile intelligence services	Deliberate
THRT-65	External Attack	RCMP TRA Methodolog	No	Espionage: Break and Enter by hostile intelligence services	Deliberate
THRT-66	External Attack	RCMP TRA Methodolog	No	Espionage: Emanations interception by other state sponsored organizations	Deliberate
THRT-67	External Attack	RCMP TRA Methodolog	No	Espionage: Network Exploitation by other state sponsored organizations	Deliberate



eService Requirements			GLB-R11.2 The Solution will not require a Inmate or Community Client to provide any text-based password or passphrase as an identity credential in order to access the ICON II system	GLB-R14 The Solution must not depend on external (i.e. extra-Ministerial / extra-Justice Network) support for Client account maintenance or support	GLB-R15 The Solution must not depend on unsecured access to networks external to the protected Justice network	GLB-R16 The Solution must prevent Corrections Clients ~~from directly accessing the Internet~~ from accessing BC Government network resources outside the secure ICON II system	GLB-R16.1 The Solution must prevent Corrections Clients from directly accessing the Internet or external communications networks	GLB-R16.2 The Solution must prevent Corrections Clients from connecting unauthorized physical data input/output devices to a ICON II secure eDevice
Threat I	Applicable?	Threat Description						
THRT-1	Yes	Malfunction of computer/network equipment						
THRT-2	Yes	Malfunction of application software developed in-house						
THRT-3	Yes	Malfunction of system software						
THRT-4	Yes	Malfunction of business application software acquired from a third party						
THRT-5	Yes	Mistakes made by IT/network staff						
THRT-6	Yes	User mistakes	x					
THRT-7	Yes	Unforeseen effect of changes to software						
THRT-8	Yes	Unforeseen effects of introducing new/upgraded business processes						
THRT-9	Yes	Unforeseen effect of changes to computer/communications equipment						
THRT-10	Yes	Unforseen effect of changes to business information						
THRT-11	Yes	Unforseen effects of changes to user processes or facilities						
THRT-12	Yes	Unforseen effects of organizational changes						
THRT-13	Yes	Damage to, or loss of, communications links/services						
THRT-14	Yes	Loss of power						
THRT-15	Yes	System overload (e.g. due to excessive volume of traffic)			x			
THRT-16	Yes	Damage to, or loss of, computer facilities			x			x
THRT-17	Yes	Damage to, or loss of, ancillary equipment (e.g. air conditioning or a heating/cooling plant)						
THRT-18	Yes	Natural disasters						
THRT-19	Yes	Distributing computer viruses (including worms)			x	x	x	x
THRT-20	Yes	Distributing SPAM			x	x	x	x

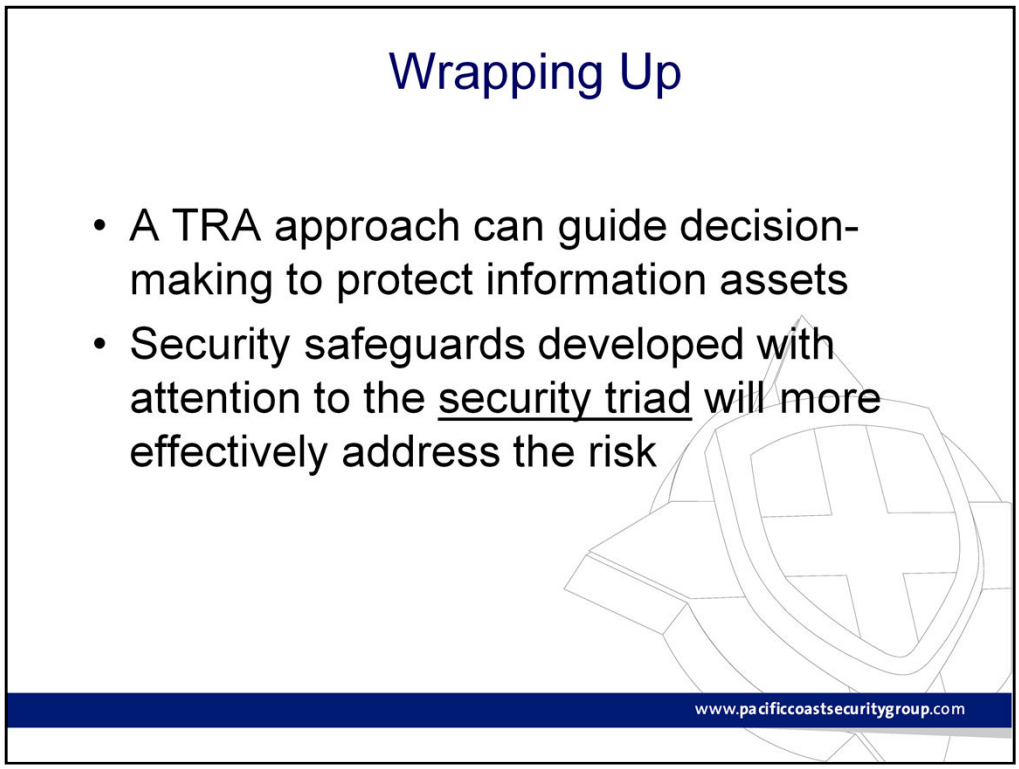


Threat Exposure Report

Threat ID	Applicable?	Threat Description	Number of Mitigating Requirements
THRT-1	Yes	Malfunction of computer/network equipment	3
THRT-2	Yes	Malfunction of application software developed in-house	3
THRT-3	Yes	Malfunction of system software	3
THRT-4	Yes	Malfunction of business application software acquired from a third party	3
THRT-5	Yes	Mistakes made by IT/network staff	3
THRT-6	Yes	User mistakes	7
THRT-7	Yes	Unforeseen effect of changes to software	2
THRT-8	Yes	Unforeseen effects of introducing new/upgraded business processes	0
THRT-9	Yes	Unforeseen effect of changes to computer/communications equipment	2
THRT-10	Yes	Unforseen effect of changes to business information	0
THRT-11	Yes	Unforseen effects of changes to user processes or facilities	0
THRT-12	Yes	Unforseen effects of organizational changes	0
THRT-13	Yes	Damage to, or loss of, communications links/services	1
THRT-14	Yes	Loss of power	1
THRT-15	Yes	System overload (e.g. due to excessive volume of traffic)	2
THRT-16	Yes	Damage to, or loss of, computer facilities	16
THRT-17	Yes	Damage to, or loss of, ancillary equipment (e.g. air conditioning or a heating/cooling plant)	1
THRT-18	Yes	Natural disasters	1
THRT-19	Yes	Distributing computer viruses (including worms)	5
THRT-20	Yes	Distributing SPAM	5
THRT-21	Yes	Introducing Trojan horses	5
THRT-22	Yes	Introducing malicious code	5
THRT-23	Yes	Undertaking malicious probes or scans	5
THRT-24	Yes	Cracking passwords	11
THRT-25	Yes	Carrying out denial of service attacks	4
THRT-26	Yes	Modifying network traffic	4
THRT-27	Yes	Social engineering	8
THRT-28	Yes	Spoofing user identities	11
THRT-29	Yes	Hacking into systems	15
THRT-30	Yes	Spoofing web sites	2
THRT-31	Yes	Defacing web sites	2

STRA Trends

- More frequent, narrower scope
- User self-assessments, more informal assessments
- Trending/tracking/reporting tools (catching up to the audit world)
- External (contracted) assessments only for major projects
- Penetration tests / vulnerability assessments becoming more prominent as a complement to STRAs. Often contracted together.



This slide sums it up and ties the concept of the security triad to the security threat risk assessment process.

Questions?