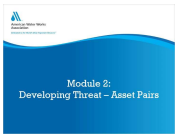
Course 3 - Risk and Resilience Management – Module 2

1

1.1 Developing Threat - Asset Pairs

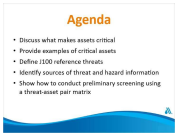


Notes:

In Module 2 we will learn more about Threat-Asset pairs

2

1.2 Agenda



Notes:

In this Module we are going todiscuss:

- What makes assets critical
- Provide examples of critical assets
- Define J100 reference threats
- Identify sources of threat and hazard information, and
- Show how to conduct preliminary screening using a threat-asset pair matrix

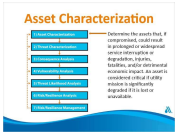
3

1.3 Learning Objectives

Notes:

These are the learning objectives for this module. After successfully completing this module, course participants will be able to select critical assets, identify common threats and hazards, and describe how to conduct preliminary screeningof Threat-Asset Pairs.

1.4 Asset Characterization



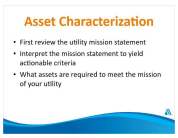
4

Notes:

In Module 1, we presentedthe definition of Asset Characterization. In the next few slides, we will:

- Drill down into what makes assets critical
- Discuss what the AWIA says about critical assets
- Explore resources you can use to help select critical assets, and
- Provide some examples

1.5 Asset Characterization

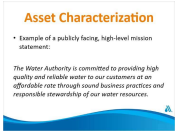


Notes:

Critical assets are those assets critical to delivering the mission of the utility. So before selectingcritical assets, it is useful to review the utility mission statement. Unfortunately many utility publicly-facing mission statements are very high-level. You may find the need to interpret your mission statement to yield more actionable missioncriteria that will help betterfocus on the utility's mostimportant priorities.

5

1.6 Asset Characterization



Notes:

Here is an example of a high-level missionstatementthat a utility may have on their website.

The Water Authority is committed to providing high quality and reliable waterto our customers at an affordable rate through sound businesspractices and responsible stewardship of our water resources.

This is a great mission statement, but it is too high-level to be used directly to make decisions about critical assets. The utility needs to decide which tanks and pumps are most important, and it is hard to make those kindsof decisions based upon a high-level missionstatement.

6

1.7 Asset Characterization

Asset Characterization

- These are examples of actionable mission criteria
  - Meet all quality and regulatory requirements 100% of the time
  - Provide adequate pressure, flow rate, and volume to meet the needs of all customers under all foreseeable circumstances
  - Adequately provide for fire protection, sanitation, potable, commercial, and industrial uses
  - Understand and meet the needs of critical customers
  - Continually manage critical assets in a priority manner and apply the necessary resources to prevent unexpected failures

Notes:

We are not suggesting that the utility re-write their mission statement, but it is a great exercise to conduct in a stakeholder workshop to "unpack", so to speak, the high-level mission statement into more actionable criteria.

Here is an example of doing that:

- Meet all quality and regulatory requirements 100% of the time
- Provide adequate pressure, flow rate, and volume to meet the needs of all customers under all foreseeable circumstances
- Adequately provide for fire protection, sanitation, potable, commercial, and industrial uses
- Understand and meet the needs of critical customers
- Continually manage critical assets in a priority manner and apply the necessary resources to prevent unexpected failures

With this level of granularity, we can begin to focus on the assets that are required to achieve these criteria.

7

1.8 Critical Components

Critical Components

Notes:

The AWIA requires, at a minimum, that these types of critical components be considered when conducting a risk and resilience assessment:

- Pipes
- Constructed conveyances
- Physical barriers
- Source water
- Raw water collection and intake
- Pretreatment
- Treatment
- Storage and distribution facilities
- Financial infrastructure
- Monitoring systems
- Electronic, computer, and other automated systems

8

1.9 Asset Characterization

Asset Characterization

- The AWIA list of critical components is a good starting point
- It is important to define specific critical assets for your utility
- Refer to your asset management program for asset criticality scores
- Consider the assets identified as critical in past vulnerability assessments

Notes:

The AWIA list of critical components is a good starting point, but it is important to define critical assets that are specific for your utility. A good place to start is your asset management program. This likely includes a list of assets prioritized by criticality scores. However, we can't rely 100% on the asset management programs to identify all your critical assets because the criteria for classifying an asset as critical in the asset management program is primarily based upon operational considerations, whereas in a risk and resilience assessment there are other considerations such as human, social, environmental, and regional impacts, as well as dependencies. Back in 2003 to 2005 when your utility performed a vulnerability assessment, the assets considered critical at that time can also inform your current day assessment.

9

1.10 Example Critical Assets

Example Critical Assets

- Pipes and constructed conveyances
  - Large diameter transmission mains, tunnels, aqueducts
  - Lines that create looping networks
  - Lines that supply a critical customer
  - Interconnect with an adjacent water system
  - Dead end line serving an island

Notes:

Now let's discuss some examples of critical assets. The first category we will consider is pipes and constructed conveyances. This category might include such things as:

- Large diameter transmission mains, tunnels, aqueducts
- Lines that create looping networks
- Lines that supply a critical customer, and
- Interconnects with an adjacent water system.

Consider a utility with a non-redundant, dead end line serving an island. Obviously, that line is pretty critical!

10

1.11 Example Critical Assets

Example Critical Assets

- Source water, intake structures, raw water collection and transmission
  - Surface water sources, dams, reservoirs
  - Groundwater sources, aquifers, wells, well fields
  - Intake structures
  - Aquifer storage and recovery systems
  - Raw water pumping and transmission, raw water canals
  - Raw water storage ponds or quarries

Notes:

Here are some example critical assets that fall within the category of Source water, intake structures, raw water collection, and transmission:

- Surface water sources, dams, reservoirs
- Groundwater sources, aquifers, wells, well fields
- Intake structures
- Aquifer storage and recovery systems -- many utilities use these types of systems for peak times in the summer; they may not be critical in winter, but because they are critical part of the year, they are still considered critical assets
- Any utility that uses a surface water source will have raw water pumping and transmission
- Water Treatment Plants may use raw water canals to convey water from the source to the plant.
- Many utilities have raw water storage ponds
- Some utilities may have storage in creative locations, such as an abandoned quarry for use as a raw water storage reservoir.

11

1.12 Example Critical Assets

Example Critical Assets

- Pretreatment and treatment processes
  - Pretreatment for zebra mussels
  - PAC pretreatment for TTHM precursors
  - Preozonation
  - Conventional flash mix, coagulation, sedimentation, filtration
  - Membrane technologies
  - Disinfection
  - Corrosion control

Notes:

Here are some examples of critical assets that fall within the category of Pretreatment and treatment processes:

- Pretreatment for zebra mussels at a raw water intake
- Powdered Activated Carbon pretreatment for Total Trihalomethane precursors
- Preozonation
- Conventional flash mix, coagulation, sedimentation, filtration
- Membrane technologies
- And, of course, Disinfection and Corrosion control

12

1.13 Example Critical Assets

Example Critical Assets

- Storage and distribution facilities
  - Reservoirs, elevated tanks, standpipes, hydro-pneumatic tanks
  - High service pumping
  - Distribution system network
  - Pressure zone interconnects and PRVs
  - Dead end lines

Notes:

Here are some examples of critical assets that fall within the category of Storage and distribution facilities

- Reservoirs, elevated tanks, standpipes, hydro-pneumatic tanks
- High service pumping
- Distribution system network
- Pressure zone interconnects and PRVs
- Perhaps dead end lines, depending on the criticality of what that line is serving.

Published by Articulate® Storyline www.articulate.com

13

1.14 Example Critical Assets

Example Critical Assets

- Electronic, computer, and other automated systems
  - Process Control Systems
  - Enterprise Systems
- Financial infrastructure
  - Computer networks that are critical to customer billing, procurement, etc.
- All of these assets are vulnerable to cyber attacks

Notes:

In the category of Electronic, computer, and other automated systems, we need to consider both

- Process Control Systems
- Enterprise Systems

The term "financial infrastructure" is a reference to the accounting and financial business systems operated by a utility, such as customer billing and payment systems.

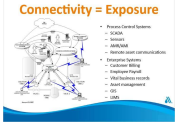
All of these assets are vulnerable to cyber attacks

Published by Articulate® Storyline www.articulate.com

14

1.15 Connectivity = Exposure

Connectivity = Exposure



- Process Control Systems
  - SCADA
  - Sensors
  - AMR/AMI
  - Remote asset communications
- Enterprise Systems
  - Customer Billing
  - Employee Payroll
  - Vital business records
  - Asset management
  - GIS
  - LIMS

Notes:

Water utilities generally have at least two different network platforms: Process Control Systems and Enterprise Systems.

The Process Control Systems include things like

- Operational controls for treatment, chemicals, pumping, valves
- Sensors for water quality, tank levels, flow meters
- Life safety systems
- Historical operational data
- And perhaps security systems, cameras, access control systems

Enterprise Systems include things like

- Customer information, billing
- Human Resources information, payroll, insurance
- Vital business records, contracts, legal records
- Asset management systems, work order generation, procurement
- Geographic Information Systems (GIS)
- And Laboratory Information Management Systems

In many cases, there is a high degree of interconnectivity between these network platforms, and that introduces vulnerabilities to cyber attacks

Published by Articulate® Storyline www.articulate.com

15

1.16 Which of the following would likely be considered critical water system assets? Check all that apply.

(Multiple Response, 10 points, 3 attempts permitted)

Correct	Choice
X	a. Water main serving a hospital
	b. Irrigation line to a soccer field
X	c. Interconnect with an adjacent water system
X	d. Aquifer storage and recovery system
X	e. Supervisory Control and Data Acquisition System (SCADA)

Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Notes:

Correct answer: a, c, d, and e

a) Correct - Water main serving a hospital would be a critical asset

b) Incorrect - An irrigation line to a soccer field would not be critical to the utility mission

c) Correct - An interconnect with an adjacent water system would also be a critical asset

d) Correct - An aquifer storage and recovery system would also be a critical asset

e) Correct - A Supervisory Control and Data Acquisition System (SCADA) would also be a critical asset

1.17 Threat Characterization

Published by Articulate® Storyline www.articulate.com

16

Threat Characterization

Notes:

We discussed the definition of Threat Characterization in Module 1. Now we will drill down more into this topic and discuss:

- J100 reference threats and hazards
- Example custom threats, and
- Sources of threat and hazard information

Published by Articulate® Storyline www.articulate.com

17

1.18 J100 Reference Threats

J100 Reference Threats

- J100 provides a detailed list of reference threats and hazards
  - Natural hazards
  - Dependency and proximity hazards
  - Malevolent threats
- This is an example of how J100 takes an all-hazards approach

Notes:

One great thing about J100 is that it provides us with a list of reference threats and hazards and a lot of detailed characterization information. These reference threats and hazards fall within the following categories:

- Natural hazards
- Dependency and proximity hazards
- Malevolent threats

This is an example of how J100 takes an all-hazards approach

Please click on the link in the upper right hand corner to download a handout of the J100 reference threats and hazards. This will be useful when taking the quizzes contained within this Module.

Published by Articulate® Storyline www.articulate.com

18

1.19 J100 Reference Threats

J100 Reference Threats

- Natural hazards
  - Hurricanes
  - Earthquakes
  - Tornadoes
  - Floods
  - Wildfires
  - Ice storms

Notes:

The natural hazard category has reference threats for:

- Hurricanes
- Earthquakes
- Tornadoes
- Floods
- Wildfires, and
- Ice storms

And each of these is divided into multiple levels of intensity. For example, J100 hurricane intensities range from 1 thru 5, which align with the Saffir-Simpson scale categories.

Photo: wiki commons (publicdomain) Hurricane Isabel from ISS (https://commons.wikimedia.org/wiki/File:Hurricane_Isabel_from_ISS.jpg)

19

1.20 J100 Reference Threats

J100 Reference Threats

- Dependency and proximity hazards
  - Utilities
  - Key suppliers
  - Key employees
  - Key customers
  - Transportation
  - Proximity

Notes:

The dependency and proximity hazards category includes reference threats for

- Utilities
- Key suppliers
- Key employees
- Key customers
- Transportation
- Proximity

Some of these can be sub-divided further. For example, utilities can include things such as electric power, natural gas, and communications. Key suppliers can include such things as water treatment chemicals, diesel fuel, and temporary equipment rental.

20

1.21 J100 Reference Threats

J100 Reference Threats

- Malevolent threats
  - Contamination
  - Directed / sabotage (physical, active shooter)
  - Theft or diversion (physical, cyber)
  - Cyber insider or outsider
  - Maritime
  - Aircraft
  - Vehicle Borne Bomb
  - Assault teams

Notes:

The malevolent threat category includes reference threats for:

- Contamination
- Directed threat such as physical sabotage or an active shooter
- Theft or diversion (either physical or cyber)
- Cyber insider or outsider
- Maritime
- Aircraft
- Vehicle Borne Bomb
- Assault teams

Again, many of these have multiple levels of magnitude or specificity, such as 4 different sizes of vehicle bombs and 5 different types of contamination.

21

1.22 J100 Reference Threats

J100 Reference Threats

- Consider all of the reference threats and select the ones that are applicable to your utility
- Set aside inappropriate, highly unlikely, or low consequence threats and hazards.
- Document the rationale for your decisions
- Also consider custom threats unique to your utility

Notes:

If you want your J100 assessment to achieve SAFETY Act designation, you must consider all of the reference threats. That does not mean you have to select all of them, but you must consider the **"worst reasonable"** threats and hazards that are applicable to each of your critical assets. Then you may set aside inappropriate, highly unlikely, or low consequence threats and hazards. For example, in North Dakota we would likely select Tornado as a hazard, but not Hurricane. Urban areas in Pennsylvania would likely select Ice Storm, but not Wildfire.

Make sure you document that you considered all of the reference threats and then document why you chose not to follow through with some of them. You should also consider custom threats unique to your utility.

22

1.23 Example Custom Threats

Example Custom Threats

- Hydrologic changes
- Derecho
- Workplace violence
- Ransomware
- Tertiary supply chain dependencies

Notes:

Here are some examples of custom threats that are not in the 2010 version of J100. Some of them are under consideration and may be included in future versions of J100. But in the meantime, it is appropriate for you to consider all relevant threats and hazards that could potentially cause negative impacts to your critical assets. Here are a few examples of potential custom threats and hazards:

- Hydrologic change
- Derecho
- Workplace violence
- Ransomware
- Tertiary supply chain dependencies

Hydrologic changes can included drought, salt water intrusion, and sea level rise. A Derecho is a strong straight line wind not associated with a hurricane or tornado. Derechos devastated several utilities in the Eastern US a few summers ago; many lost power and spilled millions of gallons of sewage. Workplace violence can include active shooter or other types of stalking or bullying that can have negative impact on the utility's mission. There have been multiple gun-related fatalities at water utilities across the U.S. Ransomware cyber attacks are in the news a lot these days and these have impacted water utilities. Tertiary supply chain dependencies were a big deal during the recent hurricane season. In eastern NC, there are multiple distributors that could supply alum, but it turns out they all get their alum from a single manufacturer on the Gulf Coast. Sometimes you need to peel the onion to fully understand your dependencies.

Photo: publicdomainpictures.net (publicdomain) Drought Lake (https://www.publicdomainpictures.net/en/view-image.php?image=195863&picture=drought-lake)

23

1.24 Sources of Threat

Sources of Threat and Hazard Information

- Local hazard mitigation plan
- EPA, FEMA, USGS, NOAA
- Water ISAC, InfraGard
- Local law enforcement, FBI, DHS
- ICS-CERT
- Previous real-life experiences

Notes:

Now let's talk about some sources of threat and hazard information. One source is the local hazard mitigation plan. This is a publicly-available document that can be obtained from the local planning commission that discusses the natural hazards in the area along with their probabilities.

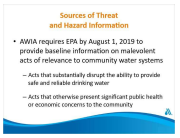
There are also many federal agencies and law enforcement organizations that can provide valuable insight into applicable threats and hazards. We can obtain flood information from FEMA, earthquake information from USGS, and hurricane information from NOAA.

Local law enforcement and the FBI are good sources of criminal and perhaps terrorist activity. Both DHS and ICS-CERT are good sources of cybersecurity information.

Of course, one of the best sources is previous real-life experiences. If it has happened before, and it has not been completely mitigated, then it may happen again.

24

1.25 Sources of Threat



Notes:

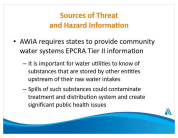
There are a couple of new requirements contained in the AWIA that will make additional threat and hazard information available to utilities. First, by August 1, 2019, EPA is required to provide baseline information on malevolent acts of relevance to community water systems. This includes:

- Acts that substantially disrupt the ability to provide safe and reliable drinking water
- Acts that otherwise present significant public health or economic concerns to the community

EPA will be developing this information in consultation with appropriate departments and agencies of the Federal Government and with State and local governments.

25

1.26 Sources of Threat



Notes:

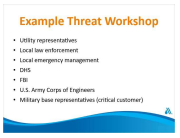
The second new development contained in the AWIA is that it will become easier for utilities to obtain EPCRA Tier II data for entities that could pose proximity threats to their source water or assets.

As you may know, the Emergency Planning and Community Right to Know Act (or EPCRA) requires facilities to report emergency and hazardous chemical information each year to their state and local emergency response officials and local fire departments. Many utilities have to do EPCRA reporting themselves because they store reportable quantities of certain hazardous chemicals such as chlorine gas, and strong acids and bases. But, it is also important for water utilities to know of substances that are stored by other entities upstream of their raw water intakes because a spill of such substances could contaminate the treatment and distribution system and create significant public health issues.

A real life example of this threat occurred in 2014 when Freedom Industries spilled achemical into the Elk River upstream of the Charleston, WV raw water intake. This resulted in 300,000 people having non-potable water for over a month. The impacts of this incident led to the new provisions on source water protection in AWIA.

26

1.27 Example Threat Workshop



Notes:

You can obtain and assemble a lot of the required threat data through phone calls and internet searches, but we highly recommend conducting a threat workshop, where you invite all relevant stakeholders to a meeting to discuss and prioritize threats and hazards. Here are some example entities that we included in a threat workshop for a recent risk assessment project:

- Utility representatives such as Operations, Maintenance, Engineering, IT, Security, and Safety
- Local law enforcement
- Local emergency management
- DHS
- FBI
- U.S. Army Corps of Engineers, and
- Military base representatives – in this case the military base was a critical customer, plus they have their own intelligence organization.

27

***1.28 Malevolent threats* (Multiple Response, 10 points, 3 attempts permitted)**

Correct	Choice
X	Ransomware
	Earthquake
X	Process sabotage
X	Activeshooter
	Telephones
X	Intentional contamination
	Electric power
	Drought
X	Truck bomb
	Wildfire

Feedback when correct:

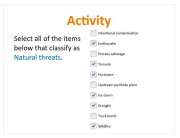
That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

28

***1.29 Natural threats* (Multiple Response, 10 points, 3 attempts permitted)**



Correct	Choice
	Intentional contamination
X	Earthquake
	Process sabotage
X	Tornado
X	Hurricane
	Upstream pesticide plant
X	Ice Storm
X	Drought
	Truck bomb
X	Wildfire

Feedback when correct: That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

29

***1.30 Dependency threats* (Multiple Response, 10 points, 3 attempts permitted)**

Correct	Choice
	Ransomware
	Earthquake
X	Electric Power
	Tornado
X	Diesel Fuel
	Upstream pesticide plant
X	Process chemicals
	Drought
	Truck bomb
X	Telephones

Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

30

***1.31 Proximity threats* (Multiple Response, 10 points, 3 attempts permitted)**

Correct	Choice
	Ransomware
	Earthquake
X	Upstreampesticideplant
	Activeshooter
	Telephones
	Intentional contamination
	Electric power
	Drought
	Truck bomb
	Wildfire

Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

31

1.32 Threat – Asset Pairs

Notes:

So now we have talked about critical assets and about threats. This brings us to a discussion of threat-asset pairs (T-A pairs). This is a very important concept in J100 because both baseline risks and risk mitigation measures are based upon T-A pairs.

Threat-asset (T-A) pairs are created by combining credible threats with critical assets, such as:

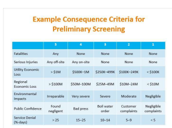
- Tornado - Pump station
- Process sabotage - Chemical metering

This can result in an extremely large number of T-A pairs.

In the next few slides, we will explain how T-A pairs can be screened to select highest priority T-A pairs based upon initial estimates of worst reasonable consequences. The lower priority T-A pairs are dropped from the analysis, and then quantitative consequences are calculated for those T-A pairs that "make the cut".

32

1.33 Example Consequence Criteria for Preliminary Screening


Example Consequence Criteria for Preliminary Screening

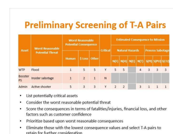
	5	4	3	2	1
Fatalities	Any	None	None	None	None
Serious Injuries	Any off-site	Any on-site	None	None	None
Utility Economic Loss	> $1M	$500K–1M	$250K–499K	$100K–249K	< $100K
Regional Economic Loss	> $100M	$50M–100M	$25M–49M	$10M–24M	< $10M
Environmental Impacts	Irreparable	Very severe	Severe	Moderate	Negligible
Public Confidence	Found negligent	Bad press	Boil water order	Customer complaints	Negligible complaints
Service Denial (%-days)	> 25	15–25	10–14	5–9	< 5

Notes:

In order to conduct screening of Threat-Asset pairs based upon estimates of worst reasonable consequences, we must first develop consequence rating criteria that are calibrated for the size and budget of the utility. J100 provides the typical consequence categories to consider, and these can be adjusted by a utility. These are not all a one-size-fits all criteria and this is best accomplished using a stakeholder workshop to achieve consensus on the criteria. This table shows an example of consequence rating criteria for a water system that has a customer base of about 70,000 people. Using a stakeholder workshop, the utility reached a consensus that a $100,000 economic loss to the utility was a relatively low impact, whereas an economic loss of greater than $1M was a very high impact. The regional economic impact criteria were proportional to this, but about two orders of magnitude higher. Another utility that serves 5 million customers reached a consensus that $1M was a relatively low impact and greater than $300M was a very high impact. So, we can see the financial consequence rating criteria can vary depending on the utility size and budget. In contrast, the decisions about how to rate consequence criteria for fatalities and serious injuries are often similar regardless of the size of the utility. A fatality is a tragic consequence, and no utility considers that acceptable.

33

1.34 Preliminary Screening


Preliminary Screening of T-A Pairs

Asset	Worst Reasonable Potential Threat	Worst Reasonable Potential Consequence			Critical	Estimated Consequence to Mission						
						Natural Hazards				Process Sabotage		
		Human	$ Loss	Other		N(F)	N(H)	N(E)	N(T)	S(PI)	S(PU)	S(CU)
WTP	Flood	1	5	5	Y	5	5		4	3	3	3
Booster PS	Insider sabotage	1	2	1	N							
Admin	Active shooter	5	3	3	Y	2	2		3	1	1	1

- List potentially critical assets
- Consider the worst reasonable potential threat
- Score the consequences in terms of fatalities/injuries, financial loss, and other factors such as customer confidence
- Prioritize based upon worst reasonable consequences
- Eliminate those with the lowest consequence values and select T-A pairs to retain for further consideration

Notes:

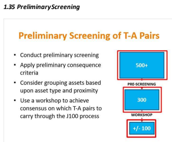
So, once you have developed your list of threat-asset pairs, and your consequence screening criteria, you can then construct a matrix like the one shown in this slide and conduct preliminary screening of T-A pairs.

- Start by considering the worst reasonable potential threat to each T-A pair
- Then score the consequences in terms of fatalities/injuries, financial loss, and other factors such as customer confidence and environmental impacts
- Prioritize the T-A pairs based upon worst reasonable consequences
- Then you can look for a natural break point in the data and eliminate the lower consequence T-A pairs and select the higher consequence T-A pairs to retain for further consideration

A word of caution though. You have to use some professional judgment here because this screening method is based solely upon consequence and not also on threat probability. It is biased towards keeping high consequence T-A pairs regardless of whether they are high probability, and may screen out medium consequence T-A pairs that are highly probable. Feel free to over-ride the bottom cutting for high probability pairs.

34

1.35 Preliminary Screening



Notes:

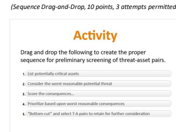
You may be asking yourself, why do we do this bottom cutting? Why not just consider all of the T-A pairs we have identified? The reason is - it is not practical or cost-effective to take all of your initial T-A pairs through the J100 process. You may start off with over 500 T-A pairs. It would take a lot of time and effort to fully evaluate that many. Using the pre-screening method we have just shown you, you may be able to reduce this list to less than 300. Then we recommend that you conduct a stakeholder workshop and use a facilitated consensus building process to whittle the list down to about 100, plus or minus 25%. This is generally a manageable number and will capture your highest priority scenarios.

Another strategy that you can use is to group similar assets and consider assessing a percentage of these and applying the results to the grouping. For example, maybe you have 20 pump stations of approximately the same size, that are all in areas with similar crime statistics, and that serve customers of similar criticality. You might consider assessing the physical security of just 5 of these and then apply the results to the whole group. You can use a similar strategy when evaluating dependency on electric power, critical assets in the same flood zone, etc.

35

1.36 Drag and drop the following to create the proper sequence for preliminary screening of threat-asset pairs.

(Sequence Drag-and-Drop, 10 points, 3 attempts permitted)



Correct Order
List potentially critical assets
Consider the worst reasonable potential threat
Score the consequences...
Prioritize based upon worst reasonable consequences
"Bottom-cut" and select T-A pairs to retain for further consideration

Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response. Please review the previous slide.

36

1.37 Knowledge Check 1

(Multiple Response, 10 points, 3 attempts permitted)

Correct	Choice
X	Surface water sources, dams, reservoirs
X	Groundwater sources, aquifers, wells, wells fields
X	Intake structures
	Flash mix, coagulation, sedimentation, filtration
X	Aquiferstorage and recovery systems

Feedback when correct:

That's right! You selected the correct response.

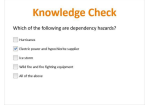
Feedback when incorrect:

You did not select the correct response.

Published by Articulate® Storyline www.articulate.com

37

***1.38 Knowledge Check 2* (Multiple Response, 10 points, 3 attempts permitted)**



Correct	Choice
	Hurricanes
X	Electricpower and hypochloritesupplier
	Icestorm
	Wildfireandfirefighting equipment
	All of theabove

Feedback when correct:

That's right! You selected thecorrect response.

Feedback when incorrect:

You did not select thecorrect response.

Notes:

Correct answer: b

a) Incorrect - Hurricanes are a natural hazard
b) Correct - Electric power and hypochloritesupplier are adependencyhazards
c) Incorrect - Icestorms are natural hazards
d) Incorrect - Wildfire are natural hazards
e) Incorrect - Not all of theabovearedependencyhazards

Published by Articulate® Storyline www.articulate.com

38

***1.39 Knowledge Check 3* (Multiple Response, 10 points, 1 attempt permitted)**

Correct	Choice
	a. Screening based upon worst reasonableconsequences andbottomcutting
	b. Stakeholder workshops
	c. Grouping similar assets
	d. Noneof the above
X	e. a, b and c

Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correctresponse.

Notes:

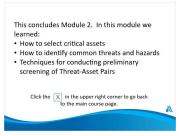
Correct answer: e

a) Incorrect - Screening basedupon worst reasonableconsequences andbottomcutting is correct, but it is a partial answer. Answer e) is most correct.
b) Incorrect - Stakeholder workshops is correct, but it is a partialanswer. Answere) is most correct.
c) Incorrect - Groupingsimilar assets is correct, but it is apartial answer. Answer e) is most correct.
d) Incorrect - Noneof theabovers not correct
e) Correct - a, b, and c are all techniques can beused to conduct preliminaryscreeningofT-Apairs

Published by Articulate® Storyline www.articulate.com

39

1.40 Closing



Notes:

Published by Articulate® Storyline www.articulate.com

40