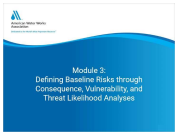
Course 3 - Risk and Resilience Management – Module 3

1

1.1 Defining Baseline Risks

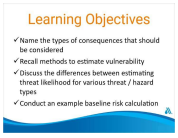


Notes:

This is Module 3, Defining Baseline Risks through Consequence, Vulnerability, and Threat Likelihood Analyses

2

1.2 Learning Objectives



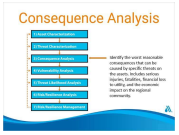
Notes:

These are the learning objectives for this module. After successfully completing this module, course participants will be able to:

- Name the types of consequences that should be considered
- Recall methods to estimate vulnerability
- Discuss the differences between estimating threat likelihood for various threat / hazard types
- Conduct an example baseline risk calculation

3

1.3 Consequence Analysis



Notes:

In this Module, we want to illustrate how to conduct baseline risk calculations using the J100 risk equation of Risk = Consequence x Vulnerability x Threat Likelihood. To do this, we first must discuss how to develop and/or obtain values for Consequence, Vulnerability, and Threat Likelihood. Let's start with a detailed look at the Consequence Analysis step and discuss:

- The cost components that Consequence is comprised of
- Sources of consequence data, and
- Suggestions on how to select practical cost estimating methods

4

1.4 Components of Consequence

Notes:

Consequence is comprised of four major cost components:

- Fatalities
- Serious injuries
- Financial loss to utility
- Regional economic impact

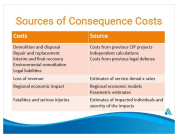
Note that there are many sub-components of utility's financial impact, including things like:

- Demolition and disposal
- Repair and replacement
- Interim and final recovery - for example during interim recovery, you may need to rent temporary equipment
- Legal liabilities
- Environmental remediation
- Loss of revenue when you can't bill your customers for days when you weren't providing them water

Now let's take a closer look at a few of these cost components

5

1.5 Sources of Consequence Costs



Notes:

Here are some example sources for consequence costs. The best source of costs for any repair or replacement activity is always historical costs from recent similar projects. Of course you can always create new cost estimates using unit prices and cost estimating resources such as R.S. Means, but this takes a lot of time and effort and cost estimates that degree of accuracy are not really needed. To estimate loss of revenue you need estimates of the number of impacted customers, the durations of service denial, and the billing rates. To estimate regional economic impacts, you can use economic models or parametric estimates such as "2 to 3 orders of magnitude higher than the owners loss." To estimate fatalities and serious injuries, you need an estimate of the impacted individuals and the severity of the impacts.

6

1.6 Fatalities and Serious Injuries

Fatalities and Serious Injuries

- Express these consequences two ways
  - Numbers of impacted individuals
  - Value of a statistical life ($7.4 M in 2006 $)
- Always report the results both ways
  - Use dollar values to calculate financial consequence
  - Use numbers of impacted individuals to emphasize tragic human impacts

Notes:

We discussed in Module 1, that consequence is expressed in dollars. When it comes to fatalities and serious injuries, we actually express these consequences in two ways:

- Numbers of impacted individuals, and
- Then in terms of dollars, by using the number of impacted individuals x the value of a statistical life. EPA has indicated that the value of a statistical life is $7.4M in 2006 $.

The value of a statistical serious injury is considered to be 25% of the value of a statistical life.

Always report these results two ways:

- We have to use dollar values to calculate financial consequence and conduct cost/benefit analyses, but
- We always use numbers of impacted individuals to emphasize tragic human impacts - never lose sight of these serious human impacts

The new J100 references this website for value of a statistical life ($7.4M in 2006$):
https://www.epa.gov/environmental-economics/mortality-risk-valuation#whatvalue

7

1.7 Regional Economic Impact

Regional Economic Impact

- Regional economic impact resulting from
  - Actual water disruptions or water quality issues
  - Threats, negative media, loss of public confidence
- Impacted sectors
  - Manufacturing, businesses, retail sales, tourism, hotels, restaurants, etc.
- Example
  - 3-day water incident during basketball tournament
  - $5 M negative impact to the local economy

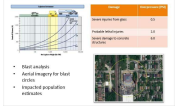
Notes:

Regional economic impact can be one of the largest components of consequence. This component estimates the community or region's indirect losses from reduced economic activity; this is sometimes referred to as the "ripple effect." This can result from water disruptions or water quality issues, or they could simply result from threats or negative media that lead to loss of public confidence. Some examples of regional economic impact include business losses in manufacturing, retail sales, tourism, hotels, restaurants, etc. For example in 2017, there was a 3-day water incident in a small college town during a high-profile basketball tournament. The game had to be postponed and relocated to another city. This incident had an estimated $5M negative impact on the local economy. For a large utility, the regional economic impact of an extended water crisis could be billions of dollars.

8

1.8 Practical Cost Estimating Methods

Practical Cost Estimating Methods



Damage	Overpressure (PSI)
Severe injuries from glass	0.5
Probable fatal injuries	1.3
Severe damage to concrete structures	4.0

- Plant analysis
- Aerial imagery for blast circles
- Impacted population estimates

Notes:

There is a lot of cost estimating required to conduct a J100 assessment. In order to minimize costs and level of effort, it is important to make practical decisions about cost estimating methods. This is a practical example of how to estimate the potential consequences of a bomb blast. You can use the nomogram in the upper left, which was obtained from a FEMA document, to estimate the overpressure at various radii from the blast center. Then use the table in the upper right to estimate the structural damage, fatalities, and serious injuries caused by various overpressure conditions. Then you can draw isobars on the aerial photograph that illustrate zones of high, medium, and low damage. Finally, you can use the aerial photography to estimate the number of structures and individuals in each zone. As an alternative, you could hire a demolition modeling expert to develop a sophisticated blast model and run computer simulations. This would probably generate slightly more accurate data, but it would cost thousands of dollars for a single calibrated model on one location, and during a J100 assessment you may need to do this calculation for 20 or 30 assets. The method we just showed you can be done in less than an hour and generally provides data of sufficient accuracy for a J100 assessment.

Graphic source: FEMA 426, Figure 4-10, Incident Overpressure Measured in Pounds Per Sq. Inch, as a Function of Stand-Off Distance and Net Explosive Weight

The aerial photo is a random photo from a large city using Google Earth. It is not a water system asset.

9

1.9 Activity (Multiple Choice, 10 points, 3 attempts permitted)

Activity

Which of the following are components of consequences that should be considered?

- ○ Removal of damaged structures
- ○ Environmental cleanup costs
- ○ Temporary pumping equipment
- ○ Loss of hotel and conference center revenue
- ◉ All of the above

Correct	Choice
	Removal of damaged structures
	Environmental cleanup costs
	Temporary pumping equipment
	Loss of hotel and conference center revenue
X	All of the above

Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect: You did not select the correct response. Please review slide 5.

Notes:

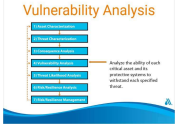
Now let's check your understanding of Consequence costs. In this activity, select the components of consequence that should be considered.

a) Incorrect - Removal of damaged structures is one of the correct answers, but e) is the most correct answer
b) Incorrect - Environmental cleanup costs is one of the correct answers, but e) is the most correct answer
c) Incorrect - Temporary pumping equipment is one of the correct answers, but e) is the most correct answer
d) Incorrect - Loss of hotel and conference center revenues one of the correct answers, but e) is the most correct answer
e) Correct - All of the above is the most correct answer

10

1.10 Vulnerability Analysis

Vulnerability Analysis



Notes:

Now let's take a detailed look at the Vulnerability Analysis step of J100 and discuss:

- How the definition of vulnerability varies for malevolent threats versus natural hazards
- Some considerations that go into estimating vulnerability, and
- Some vulnerability estimating methods

11

1.11 Vulnerability Definitions

Vulnerability Definitions

- Malevolent events
  - Estimate of the likelihood that an adversary will be successful in executing a specific attack mode on an asset, given that the attack occurs
- Natural, dependency, and proximity hazards
  - Estimate of the likelihood that, given the hazard occurs, the estimated consequences will result

Notes:

The definition of vulnerability varies depending on whether we are discussing malevolent events vs natural, dependency, and proximity hazards.

For Malevolent events the definition is:

- An estimate of the likelihood that an adversary will be successful in executing a specific attack mode on an asset, given that the attack occurs

For natural, dependency, and proximity hazards the definition is:

- An estimate of the likelihood that, given the hazard occurs, the estimated consequences will result

12

1.12 Vulnerability Considerations from G430

Vulnerability Considerations from G430

- Access control and intrusion detection
  - Control physical access to critical assets
  - Control personnel access authorizations and methods
  - Maintain a means of detecting and assessing intrusion

Notes:

As was discussed in Course 2, the G430 Standard on Security provides guidelines for enhancing security for a water utility. When utilities implement measures recommended by G430, these can generally reduce the vulnerability of critical assets to malevolent threats and natural hazards. For example, Section 4.6 in G430 provides recommendations regarding Access Control and Intrusion Detection for selected critical assets. These measures include such things as:

- Controlling physical access to critical assets with fences, barriers, and locked gates, hatches, and doors
- Controlling personnel, visitor, and vendor access with background checks, policies and procedures, badging, electronic access control systems, and key control programs
- And maintaining a means of detecting and assessing intrusion with intrusions detection systems and surveillance

All of these measures would tend to reduce vulnerability.

13

1.13 Vulnerability Considerations

Vulnerability Considerations

- Building material structural properties (walls, doors, windows)
- Building code design standards and year constructed
- Countermeasures and mitigation measures
- Crime Prevention through Environmental Design (CPTED)

Notes:

There are a number of things that should be considered when estimating the vulnerability of a threat-asset pair:

- For example, if you are evaluating the vulnerability of a building to high winds, you should consider the structural properties of the building, walls, doors, windows, etc.
- You should also consider the building code design standards and year constructed -
  - For example, after hurricane Andrew hit southern FL in 1992, they changed the building codes, so structures built after 1992 are more resistant to wind damage
- You also need to consider any existing countermeasures and mitigation measures. The photo on this slide shows a CPTED technique of using large, heavy planters to create set back distance and reduce the vulnerability of this building to vehicular attack.

(Picture source: Ketchum, "Trends in Water Security. Fostering Critical Infrastructure Resiliency", ppt slide 23)

14

1.14 Vulnerability Considerations

Vulnerability Considerations

- Weaknesses in protection systems
- Interdependencies, process flow, and operational practices
- Policies and procedures
- Personnel behavior and interactions

Notes:

Other things that you should consider when estimating vulnerability include:

- Weaknesses in protection systems and interdependencies that could increase vulnerability
- Also Policies and procedures can potentially reduce vulnerabilities, but only if employees actually follow them, so understanding actual personnel behaviors is important

Photo source: Perry Gayle, J100 on a Budget: Maximizing the Benefits Derived from a J100 RAMCAP Risk Assessment while Managing Costs, AWWA Water Infrastructure Conference, Oct 2015 (AECOM photo)

15

1.15 Vulnerability Estimation Methods

Vulnerability Estimation Methods

- Malevolent threats
  - Event trees
  - Path analysis
  - Vulnerability logic diagrams
  - Direct expert elicitation (professional judgment)
  - Hybrid methods

Notes:

There are a number of methods of estimating vulnerability for a threat-asset pair. And the methods are generally different for malevolent threats than for natural hazards. Let's first look at some of the methods that can be used to estimate vulnerability to malevolent threats. These include such things as:

- Event trees
- Path analysis
- Vulnerability logic diagrams
- Direct expert elicitation (professional judgment)
- Hybrid methods

16

1.16 Security Concepts

Security Concepts for Defeating an Attack

Notes:

Before we get into discussing methods for estimating vulnerability for malevolent threats, let's review the security principles of deter, detect, delay, and respond:

- Deter features are things you do to discourage an attack or make the adversary chose another target. These include warning signs, lights, security patrols, etc.
- Detect features are things that alert you that an attack is occurring such as sensors, surveillance cameras, and witnesses
- Delay features are things that slow the adversary down and increase the time it takes for the adversary to complete the attack. These include fences, barriers, hardened doors, and ideally multiple layers of delay.
- Respond features are things you do to stop the attack and these may include communications, utility personnel, and law enforcement

17

1.17 Event Trees

Event Trees

- Event trees map the sequence of events during an attack
- Each "branch" represents the likelihood of success or failure at that junction
- The sum of the probabilities of all branches on which the attack succeeds is the vulnerability estimate

Notes:

This is an example of an event tree for estimating the vulnerability of a critical asset to a particular malevolent attack:

Event trees map the sequence of events between the initiation of the attack and the terminal event

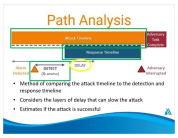
Each "branch" represents the likelihood of success or failure at that junction

The sum of the probabilities of all branches on which the attack succeeds is the vulnerability estimate

In this case, there is a 69% probability of success.

18

1.18 Path Analysis

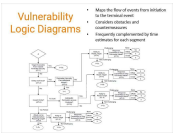


Notes:

Path analysis is a method of comparing the attack timeline to the detection and response timeline. It also considers the layers of delay that can slow the attack. This provides an estimate of whether the combination of detection, delay, and response interrupts the adversary before the attack can be completed.

19

1.19 Vulnerability Logic Diagrams



Notes:

This is an example of a Vulnerability Logic Diagram. It is similar to other logic diagrams or logical flow charts. In this case it is mapping the logical flow of how an adversary could access a protected facility, defeat the countermeasures, and complete an attack.

20

1.20 Hybrid of Event Tree

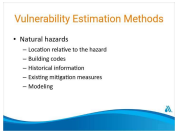
Notes:

This is a hybrid method that can be used when estimating the vulnerability of a malevolent attack on a critical asset. It is a hybrid of an event tree and a path analysis. The event tree portion helps calculate the probability of success, while the path analysis portion helps establish the timeline of the attack and the response.

Don't be confused by the odd shape of the event tree on this slide. Only a portion of the event tree is shown, because it won't all fit on the page.

21

1.21 Vulnerability Estimation Methods



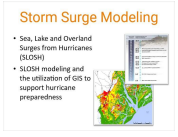
Notes:

Now let's look at some methods of estimating vulnerability of critical assets to Natural Hazards. These include such things as:

- Location relative to the hazard, for example being in a 100-year floodplane
- Building codes that were in place when structures were built that may have required resistance to hurricanes or seismicactivity
- Historical information about the location and magnitude of previous natural hazard events
- Existing mitigation measures that may have been implemented following previous events
- And various types of modeling

22

1.22 Storm Surge Modeling



Notes:

Here is an example of a method for estimating vulnerability of an asset to hurricane storm surge. It uses a SLOSH model to estimate storm surge elevations for various hurricane categories. Then the upper chart shows the first floor elevations of various critical assets. Using the combination of these two information sources, you can predict which assets may flood based upon the expected hurricane intensity.

Source: Ken Jordan and Perry Gayle, Achieving Operational Resilience Through Assessment and Continuous Improvement, NC AWWA-WEA Annual Conference, Nov 2016

23

1.23 Historical Information

Notes:

Another less complicated method for estimating vulnerability to natural hazards is historical observation. This is an example of flash flooding caused by Hurricane Matthew in 2016. These assets are not in the 100-year flood zone of a river, rather this is inland flash flooding caused by 11 inches of rainfall in just a few hours.

Photo source: Ken Jordan and Perry Gayle, Achieving Operational Resilience Through Assessment and Continuous Improvement, NC AWWA-WEA Annual Conference, Nov 2016

24

***1.24 Activity* (Multiple Choice, 10 points, 3 attempts permitted)**

Correct	Choice
X	Event trees and building codes
	Asset criticality and repair costs
	Owners financial loss and regional economic impact
	None of the above

Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response. Please reference slides 13 and 15.

Notes: Now let's test you knowledge of vulnerability estimating. In this activity, select which of the following would be useful in estimating vulnerability.

Correct answer: a

a)Correct - Event trees and building codes would be useful in estimating vulnerability
b)Incorrect - Asset criticality would be useful in selecting critical assets and repair costs would be useful in estimating Consequences
c) Incorrect - Owners financial loss and regional economic impact would be useful in estimating Consequences
d) Incorrect - None of the above is incorrect because answer a) is correct

25

1.25 Threat Likelihood Analysis

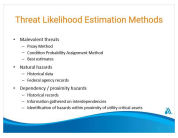
Notes:

Now let's take a detailed look at the Threat Likelihood step of J100 and discuss:

- The differences between calculating Threat Likelihood for malevolent threats vs natural, dependency, and proximity hazards
- Some threat Likelihood Estimation Methods, and
- Some sources of threat likelihood data

26

1.26 Threat Likelihood



Notes:

There are a number of methods for estimating threat likelihood, and the methods differ depending on the nature of the threat or hazard:

For Malevolent threats, you can use

- The Proxy Method - which we talk about on the next slide
- Condition Probability Assignment Method - which is basically assigning a probability of 1.0 to an event that is highly likely
- Or Best estimates - which is basically professional judgment

For Natural hazards, you can use

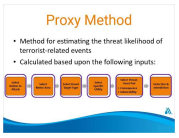
- Historical data (return periods), and
- Federal agency records

For Dependency / proximity hazards, you can use

- Historical records
- Information gathered on interdependencies
- Identification of hazards within proximity of utility critical assets

27

1.27 Proxy Method



Notes:

Let's take a look at the proxy method for estimating the threat likelihood of terrorist-related threats. Basically, the Proxy Method is calculated using these 6 inputs:

- First, what is the current likelihood of a terrorist event in the U.S. this year
- Next, what is the likelihood that it is going to happen in this particular metropolitan region
- Then, what is the likelihood of the target being something of similar attractiveness to a critical water systems asset. This step categorizes assets using the RAND/RMS target groups. For example, Water Treatment Plants and major pump stations are considered similar to industrial facilities, oil and gas processing facilities, ports, etc.
- Next, what is the likelihood of the adversary attacking this specific utility in this specific region
- Then, what is the likelihood of the adversary attacking this particular asset at this utility.
- Lastly, you adjust for the likelihood of pre-attack detection and interdiction based on the hazard type

If you multiply all these probabilities together you get an estimate of an attack on the specific critical asset at this specific utility.

4 of these components are lookup values and the other 2 require calculations.

28

1.28 Sources for Natural Hazard Data

Notes:

To estimate the threat likelihood of most natural hazards, you can draw upon information and models from various local and federal agencies. For example:

- You can obtain the local Hazard Mitigation Plan from the local Emergency Planning Office or sometimes you can find these online. These contain good information about natural hazards that are relevant to the community.
- You can obtain earthquake frequency and intensity data from USGS
- NOAA maintains data for hurricanes, tornados, ice storms, and droughts
- You can use FEMA Flood Insurance Rate Maps (FIRM) for flood zone information
- And you can use various hydrologic studies to estimate changes in hydrologic patterns, such as salt water intrusion, and sea level elevations

29

1.29 Activity

(Multiple Choice, 10 points, 3 attempts permitted)

Correct	Choice
	a. FEMA maps
X	b. USGS data
	c. NOAA data
	d. Both a & b
	e. Both a & c

Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

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

Notes:

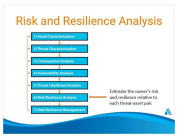
Now let's check your understanding of where to obtain threat likelihood data. In this activity, which of the choices would be most useful in estimating earthquake threat likelihood?

Correct answer: b

a) Incorrect - FEMA maps would be most helpful in estimating flood hazard frequency
b) Correct - USGS data would be most useful in estimating earthquake threat likelihood
c) Incorrect - NOAA data would be most useful in estimating weather related events like hurricanes
d) Incorrect - Both a & b is incorrect because e) is incorrect
e) Incorrect - Both a & c is incorrect because both a) and c) are incorrect

30

1.30 Risk and Resilience Analysis



Notes:

Now that we have discussed how to calculate or obtain estimates of consequence, vulnerability, and threat likelihood, we are ready to talk about the Risk and Resilience Analysis step of J100. This is where you calculate baseline risk and resilience. In the next few slides we will discuss:

- The risk equation
- Some example calculations, and
- Some tools that are available to help conduct large numbers of calculations more efficiently

31

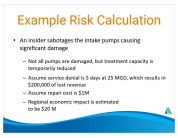
1.31 Risk and Resilience Analysis

Notes:

Let's review the risk equation. Risk = Consequence x Vulnerability x Threat Likelihood. During Risk and Resilience Analysis, you calculate the baseline risk for each threat-asset pair. As you have seen in previous slides, the value of consequence can vary widely. If the scenario results in lost lives and significant regional economic impacts, the consequence can be in the billions of dollars. Vulnerability ranges from zero (not vulnerable at all) to 1.0 (completely vulnerable). Threat Likelihood ranges from 1.0 (certain to happen) to numbers as small as 10 -17

32

1.32 Example Risk Calculation



Notes:

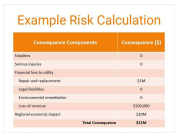
Now let's look at an example risk calculation for insider sabotage against a critical pump. This is the scenario:

An insider sabotages the raw water intake pumps causing significant damage

- Not all pumps are damaged, but treatment capacity is temporarily reduced
- Assume service denial is 5 days at 25 MGD, which results in $200,000 of lost revenue
- Assume repair cost is $1M and the regional economic impact is $20M

33

1.33 Example Risk Calculation



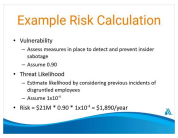
Notes:

This table shows how we sum up the total consequence costs. As you can see, there are no fatalities, serious injuries, legal liabilities, or environmental remediation.

We add together repair and replacement costs, loss of revenue, and regional economic impact. The total consequence is rounded to approximately $21 M.

34

1.34 Example Risk Calculation



Notes:

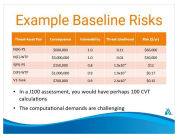
Now we need estimates of Vulnerability and Threat Likelihood. So we assess the measures in place to detect and prevent sabotage and estimate the Vulnerability is 0.9 using one of the methods discussed earlier in this module.

We estimate threat likelihood by considering previous incidents of disgruntled employees and, for this example, we assume a value of 1x10-4

Then we can multiply the three components of the risk equation and calculate the risk to be $1,890 per year

35

1.35 Example Baseline Risks



Notes:

This table shows multiple baseline risk calculations and how the baseline risk can vary significantly between different threat-asset pairs. The first two rows are hurricane and flood hazards, while the last three rows are sabotage, proximity, and vehicle bomb threats. Note that the Threat Likelihood for the natural hazards is much greater than the Threat Likelihood of the malevolent threats. This makes the Risk much higher for the natural hazards.

In a J100 assessment, you'd have to make perhaps 50 to 100 Consequence, Vulnerability, and Threat Likelihood calculations

That means you first have to estimate C, V, and T for 50 to 100 threat-asset pairs

So, it'll be an understatement to say the computational demands are challenging

36

1.36 Risk and Resilience Analysis Tools

Risk and Resilience Analysis Tools

- Program to Assist Risk & Resilience Examination (PARRE)
  - AEM Engineering software
- Vulnerability Self-Assessment Tool (VSAT)
  - VAS web-based tool
- Both PARRE and VSAT have SAFETY Act designation
- Proprietary spreadsheets and databases
- AWWA does not endorse a J100 software tool. This information is provided to help course participants research available options

Notes:

Most folks that conduct J100 assessments use some sort of computational tool to help with the calculations. Here are some of your choices and there may be others.

The first is PARRE which is an acronym for Program to Assist Risk & Resilience Examination. It was developed by AEM Engineering and is available for purchase. Another choice is VSAT which is an acronym for Vulnerability Self-Assessment Tool. It was developed by EPA and is available for free online. Both of these have SAFETY Act Designation, which means if you use them properly, you'll have certain liability protections.

Some risk assessment practitioners have developed proprietary spreadsheets and databases. In many cases these may work fine, but it's likely that they don't have SAFETY Act liability protections. But… if they use the spreadsheets to properly implement the J100 process, the J100 methodology itself has SAFETY Act designation, so you would probably have SAFETY Act liability protections anyway.

One way or another, you need a tool like one of these to support application of the J100 methodology. The computations are just too complicated and numerous to do by hand.

And just as a disclaimer: AWWA does not endorse a J100 software tool. This information is provided to help course participants research available options.

37

1.37 Activity **(Multiple Choice, 10 points, 3 attempts permitted)**

Activity

Feedback when correct:

That's right! You selected the correct response. This is the sum of repair and replacement, interim and final recovery, environmental remediation, loss of revenue, and regional economic impact.

Feedback when incorrect:

You did not select the correct response. Please review slide 33.

Notes:

Now let's check your understanding of how to conduct a baseline risk calculation. In this activity, calculate the value of the baseline risk using the inputs in the table on the right and select the correct answer.

correct answer: b

a) Incorrect - $1,000 is incorrect. The correct answer is the sum of repair and replacement, interim and final recovery, environmental remediation, loss of revenue, and regional economic impact.

b) Incorrect - $110,000 is incorrect. The correct answer is the sum of repair and replacement, interim and final recovery, environmental remediation, loss of revenue, and regional economic impact.

c) Incorrect - $500,000 is incorrect. The correct answer is the sum of repair and replacement, interim and final recovery, environmental remediation, loss of revenue, and regional economic impact.

d) Correct - $11,000,000 is correct. This is the sum of repair and replacement, interim and final recovery, environmental remediation, loss of revenue, and regional economic impact.

38

1.38 Resilience

Resilience

- Resilience is the ability to withstand an unwanted threat event while maintaining service or, if that is not possible, to restore service very quickly
- Threat-asset pair resilience
  - Assesses resilience of a single threat-asset pair
- Utility Resilience Index
  - Assesses overall utility resilience by evaluating operational and financial indicators that influence resilience

Notes:

Now let's discuss resilience. There are a variety of definitions for resilience. This is the definition that J100 uses.

"Resilience is the ability to withstand an unwanted threat event while maintaining service or, if that is not possible, to restore service very quickly"

J100 includes two different ways to look at resilience: Threat-asset pair resilience and Utility Resilience Index.

Threat-asset pair resilience assesses the resilience of a single threat-asset pair, whereas Utility Resilience Index assesses overall utility resilience by evaluating operational and financial indicators that influence resilience

39

1.39 Threat-Asset Pair Resilience

Threat-Asset Pair Resilience

- Threat-Asset pair resilience equation:

$$Re = D * S * V * T$$

Where
- Re = Resilience
- D = Duration
- S = Service denial
- V = Vulnerability
- T = Threat Likelihood

Notes:

This is the equation for Threat-Asset Pair Resilience. Duration × Service Denial × Vulnerability × Threat Likelihood.

Resilience is expressed in terms of dollars per year (lower is better). Duration = time period of service denial in days, Service Denial = amount of service denied in gallons per day, and Vulnerability and Threat Likelihood are the same terms from the Risk equation.

Threat-asset pair resilience is the ability to withstand an unwanted threat event while maintaining service or, if that is not possible, to restore service very quickly. A fully resilient asset would have no service outage risk, whereas an asset lacking in resilience could have a substantial risk of service outage. This calculation is very useful, because in an analysis containing many threat-asset pairs, some of which are critical to continuity of service and some not, it is useful to identify which threat-asset pairs contribute most to the overall service delivery failure. Note threat-asset pair resilience can be improved by through redundancy and response procedures.

40

1.40 Utility Resilience Index

Utility Resilience Index

- Two categories of URI indicator criteria
  - Operational Indicators – reflect the tactical capacity of the utility to react and respond to operational disruptions
  - Financial Indicators – reflect the fiscal capacity of the utility to react and respond to financial impacts

Notes:

The second way to look at resilience is using the Utility Resilience Index. URI is a decision support tool that can help a utility benchmark and monitor their overall capacity to respond to disruptive events. It used two categories of indicators.

- Operational indicators reflect the tactical capacity of the utility to react quickly and cope with various incidents that have the potential to disrupt services, and
- Financial indicators reflect the fiscal capacity of the utility to react quickly and cope with various incidents that have the potential to disrupt revenue and impact costs.

41

1.41 URI Indicators

URI Indicators

Operational Risk Indicators
- Emergency Response Plan (ERP)
- National Incident Management System (NIMS) compliance
- Mutual aid and assistance
- Emergency power for critical operations
- Ability to meet minimum daily demand
- Critical parts and equipment
- Critical staff resilience

Financial Risk Indicators
- Business Continuity Plan
- Utility Bond Rating
- GASB 34 Assessment
- Median Household Income
- Unemployment

Notes:

These are the URI Operational and Financial Risk Indicators.

Operational Risk Indicators include such things as:
- Does the utility have an Emergency Response Plan (ERP)
- Do they use the National Incident Management System
- Have they entered into Mutual aid agreements
- Do they have Emergency power for critical operations
- What is their ability to meet minimum daily demand during an emergency
- Do they maintain a bench stock of critical parts and equipment
- How resilient are their critical staff

Financial Risk Indicators include such things as:
- Do they have a Business Continuity Plan
- What is the Utility's Bond Rating
- Have they done a GASB 34 Assessment
- What is the Median Household Income of the community
- What is the unemployment rate in the community

42

1.42 URI Calculation Sheet

Notes:

This is a screen capture of a partial URI calculation sheet. As you can see, the various indicators are scored based upon how well the utility is considered to be doing in each functional area. The higher the total URI value, the greater the estimated utility resilience. What's important is to review where opportunities exist to improve resilience in the various categories. If the performance level for a given indicator is low, what can be done to improve it so we can increase the overall URI? For example, if a utility is not part of a mutual aid program like WARN, then joining a mutual aid group would improve the score in that functional area. If the utility has never exercised their emergency response plan, then conducting periodic exercises would improve the score in that area, and increase the overall URI score.

43

***1.43 Knowledge Check 1* (Multiple Choice, 10 points, 3 attempts permitted)**

Correct	Choice
	Previous CIP projects
X	Media reports
	Previous legal fees
	The duration that customers are without water

Feedback when correct:

That's right! You selected the correct response. Media reports are not a good source of consequence costs

Feedback when incorrect:

You did not select the correct response.

Notes:

Correct answer: b

a) Incorrect - Previous CIP projects is a potential source of consequence costs
b) Correct - Media reports are not a good source of consequence costs
c) Incorrect - Previous legal fees are a potential source of consequence costs
d) Incorrect - The duration that customers are without water is a potential source of consequence costs

44

***1.44 Knowledge Check 2* (True/False, 10 points, 2 attempts permitted)**

Correct	Choice
X	True
	False

Feedback when correct:

That's right! You selected the correct response. Loss of revenue from tourism is a potential regional economic impact that would be considered during a 1500 risk assessment.

Feedback when incorrect:

You did not select the correct response.

Notes:

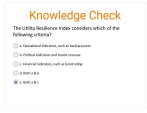
Correct answer: a

True is correct. Loss of revenue from tourism is a potential regional economic impact that would be considered during a 1500 risk assessment.

False is incorrect. Loss of revenue from tourism is a potential regional economic impact that would be considered during a 1500 risk assessment.

45

***1.45 Knowledge Check 3* (Multiple Choice, 10 points, 3 attempts permitted)**



Correct	Choice
	a. Operational indicators, such as backup power
	b. Political indicators and tourist revenue
	c. Financial indicators, such as bond rating
	d. Both a & b
X	e. Both a & c

Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

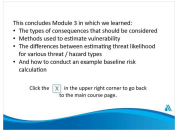
Notes:

Correct answer: e

a) Incorrect - Operational indicators, such as backup power is true, but it is a partial answer. Answer e) is most correct.
b) Incorrect - Political indicators and tourist revenue would not be considered in URI
c) Incorrect - Financial indicators, such as bond rating is true, but it is a partial answer. Answer e) is most correct.
d) Incorrect - Both a & b is incorrect, because b) would not be considered in URI
e) Correct - Both a & c is the most correct answer

46

.46 Closing



Notes:

47