Example Test Questions

14) As part of his role, Augie is responsible for implementation of business rules related to data, as well as for storage, and use of data and datasets. What data-related role does Augie hold?

a. Data owner

\*b. Data custodian

c. Data processor

d. Data subject

Let me solve this step by step:

1. Let's analyze Augie's responsibilities:
   * Implementation of business rules related to data
   * Storage of data
   * Use of data and datasets
   * Management of how data is handled
2. Let's examine each option:

a) Data Owner:

* + Has ultimate accountability for data
  + Makes strategic decisions
  + Doesn't typically handle implementation
  + More focused on policy than execution

b) Data Custodian:

* + Responsible for safe storage and maintenance
  + Implements business rules
  + Handles day-to-day data management
  + Focuses on proper use and storage
  + This matches Augie's role

c) Data Processor:

* + Processes data on behalf of the controller
  + Usually a third-party service provider
  + Doesn't set or implement business rules
  + Follows instructions from others

d) Data Subject:

* + The person whose data is being processed
  + Not involved in data management
  + Has rights regarding their data
  + Clearly not Augie's role

1. Conclusion: The answer is b. Data Custodian

19) Brian recently conducted a risk mitigation exercise and has determined the level of risk that remains after implementing a series of controls. What term best describes this risk?

a. Inherent risk

b. Control risk

c. Risk appetite

\*d. Residual risk

Let me solve this step by step:

1. Let's analyze what Brian has done:
   * He conducted a risk mitigation exercise
   * He implemented controls
   * He measured the risk that remains after these controls
   * He's looking at the "leftover" risk
2. Let's examine each option:

a) Inherent Risk:

* + This is the risk that exists before any controls
  + It's the "natural" level of risk
  + It's measured before mitigation efforts
  + Not what Brian is measuring

b) Control Risk:

* + This is the risk that controls themselves might fail
  + Related to the effectiveness of controls
  + Not the same as remaining risk after controls
  + Not what Brian is measuring

c) Risk Appetite:

* + This is how much risk an organization is willing to accept
  + It's a threshold, not a measurement
  + It's set by management
  + Not what Brian is measuring

d) Residual Risk:

* + This is the risk remaining after controls are implemented
  + It's what's left after mitigation
  + It's exactly what Brian measured
  + This matches the scenario perfectly

1. Conclusion: The answer is d. Residual Risk

This is correct because:

* Residual risk specifically refers to the risk that remains after controls are implemented
* It represents the "leftover" risk after mitigation efforts

To further clarify: If you think of risk like water in a bucket, inherent risk is the full bucket, the controls are like holes in the bucket that let water out, and residual risk is the water that remains after draining - which is exactly what Brian measured.

27) Gary is beginning his risk assessment for the organization and has not yet begun to implement controls. What risk does his organization face?

a. Residual risk

b. IP theft risk

c. Multiparty risk

\*d. Inherent risk

Let me solve this step by step:

1. Let's analyze Gary's situation:
   * He is just beginning risk assessment
   * He has not implemented any controls yet
   * He's looking at risk in its "raw" or "natural" state
   * This is before any mitigation efforts
2. Let's examine each option:

a) Residual Risk:

* + This is risk remaining after controls are implemented
  + Gary hasn't implemented controls yet
  + This can't be residual risk since no controls exist
  + Not the correct answer

b) IP Theft Risk:

* + This is a specific type of risk
  + Focuses only on intellectual property theft
  + Too narrow for Gary's general assessment
  + Not the correct answer

c) Multiparty Risk:

* + This involves risk from multiple parties or entities
  + Again, this is a specific type of risk
  + Not relevant to the stage of assessment
  + Not the correct answer

d) Inherent Risk:

* + This is the natural, unmitigated risk level
  + Risk before any controls are implemented
  + Raw risk that exists at the start
  + Matches Gary's situation perfectly

1. Conclusion: The answer is d. Inherent Risk

This is correct because:

* Inherent risk is the risk that exists before any controls or mitigation efforts
* Gary is at the beginning of his assessment, before implementing controls
* He's looking at the baseline risk level

Think of it this way: If you're measuring the natural flood risk of a building before building any flood barriers or implementing any flood protection measures, you're measuring the inherent risk of flooding.

31) Carmen’s organization wants to purchase cybersecurity insurance to offset the cost of potential breaches. What risk management strategy has her organization adopted?

\*a. Transfer

b. Accept

c. Avoid

d. Mitigate

Let me solve this step by step:

1. Let's analyze what Carmen's organization is doing:
   * They want to purchase cybersecurity insurance
   * They're looking to offset potential breach costs
   * They're not eliminating the risk
   * They're shifting the financial burden to another party (insurer)
2. Let's examine each risk management strategy:

a) Transfer:

* + Involves shifting risk burden to another party
  + Typically done through insurance or contracts
  + Financial impact is transferred to another entity
  + Exactly matches what Carmen's organization is doing

b) Accept:

* + Involves acknowledging and budgeting for risk
  + No attempt to change or shift the risk
  + Organization bears full responsibility
  + Not what Carmen's organization is doing

c) Avoid:

* + Involves eliminating the risk entirely
  + Usually by stopping the risky activity
  + Most extreme risk response
  + Not what Carmen's organization is doing

d) Mitigate:

* + Involves reducing risk through controls
  + Risk still exists but at a lower level
  + Organization still owns the risk
  + Not what Carmen's organization is doing

1. Conclusion: The answer is a. Transfer

This is correct because:

* Insurance is a classic example of risk transfer
* The organization is shifting the financial impact of breaches to the insurance company
* While the risk of a breach still exists, the financial consequences are transferred
* This perfectly matches the definition of a risk transfer strategy

41) Colleen’s organization has deployed web application firewalls (WAFs) to protect their web services from being impacted by a known SQL injection attack. What risk management strategy has the organization adopted?

a. Transfer

b. Accept

\*c. Avoid

d. Mitigate

Let me solve this step by step:

1. Let's analyze what Colleen's organization is doing:
   * They deployed Web Application Firewalls (WAFs)
   * They're specifically addressing SQL injection attacks
   * They're implementing security controls
   * They're reducing, but not eliminating, the risk
2. Let's examine each risk management strategy:

a) Transfer:

* + Involves shifting risk to another party
  + Typically done through insurance or contracts
  + Not what's happening here - they're handling it themselves
  + No transfer of responsibility

b) Accept:

* + Involves knowingly taking on risk
  + No attempt to reduce or change the risk
  + Organization just deals with consequences
  + Not what's happening - they're actively addressing it

c) Avoid:

* + Involves eliminating risk entirely
  + Usually by stopping the risky activity
  + Would mean taking web services offline completely
  + Not what's happening - services still running

d) Mitigate:

* + Involves reducing risk through controls
  + Risk still exists but at a lower level
  + Uses safeguards and countermeasures
  + Exactly matches using WAFs to reduce SQL injection risk

1. Conclusion: The answer is d. Mitigate

Common examples of mitigation include:

* Firewalls and security controls
* Training programs
* Access controls
* Security monitoring
* Backup systems

The organization is still exposed to some risk (residual risk), but they've reduced it to a more acceptable level through the implementation of WAFs.

56) Risk severity is calculated using the equation shown here. What information should be substituted for X?

Risk severity = X \* Impact

a. Inherent risk

b. MTTR (mean time to repair)

\*c. Likelihood of occurrence

d. RTO (recovery time objective)

Let me solve this step by step:

1. Let's analyze the equation:
   * Risk severity = X \* Impact
   * We need a factor that when multiplied by Impact gives severity
   * Impact represents the consequence of a risk
   * X must be the other key component of risk calculation
2. Let's examine each option:

a) Inherent risk:

* + This is the total risk before controls
  + It's an outcome, not a factor
  + Wouldn't make sense to multiply by impact
  + Not the correct factor

b) MTTR (mean time to repair):

* + This is a recovery metric
  + Measures time to fix issues
  + Not directly related to risk occurrence
  + Not the correct factor

c) Likelihood of occurrence:

* + This measures how likely a risk is to occur
  + When combined with impact, gives severity
  + Standard risk assessment component
  + Makes mathematical sense in the equation

d) RTO (recovery time objective):

* + This is a target recovery time
  + Another recovery metric
  + Not related to risk occurrence
  + Not the correct factor

1. Conclusion: The answer is c. Likelihood of occurrence

This is correct because:

* Risk severity is traditionally calculated by combining likelihood and impact
* This follows the standard risk assessment formula: Risk = Likelihood × Impact
* It makes logical sense: higher likelihood and higher impact mean higher severity
* None of the other options would give a meaningful measure of risk severity when multiplied by impact

70) Henry’s organization has set their RTO to 12 hours. What does this mean?

a. Outages must be less than 6 hours long.

\*b. Recovery from outages should take less than 12 hours.

c. Outages longer than 12 hours will require fail over to a warm site.

d. SLAs for third-party services should specify a 12 hour MTBF.

Let me solve this step by step:

1. First, let's understand what RTO (Recovery Time Objective) is:
   * It's the maximum acceptable time for restoring a business process after a disruption
   * It sets a target for how quickly recovery must be completed
   * It's a goal, not a guarantee
   * It helps determine what disaster recovery capabilities are needed
2. Let's analyze each option:

a) Outages must be less than 6 hours long:

* + This confuses RTO with actual outage duration
  + Mentions 6 hours, not 12
  + Not correct

b) Recovery from outages should take less than 12 hours:

* + This correctly defines RTO
  + Matches the 12-hour timeframe
  + Correctly focuses on recovery time
  + This is the right answer

c) Outages longer than 12 hours will require fail over to a warm site:

* + This is a specific recovery action
  + RTO doesn't mandate specific recovery methods
  + Not correct

d) SLAs for third-party services should specify a 12 hour MTBF:

* + This confuses RTO with MTBF (Mean Time Between Failures)
  + Different metric entirely
  + Not correct

1. Conclusion: The answer is b. Recovery from outages should take less than 12 hours.

This is correct because:

* It accurately reflects what RTO means
* It matches the specified 12-hour timeframe
* It focuses on recovery time, which is what RTO measures
* It represents the goal the organization has set for restoring services

Real-world example: If a critical system goes down at 2:00 PM, with a 12-hour RTO:

* The system should be restored by 2:00 AM the next day
* This gives IT teams a clear deadline
* Recovery plans should be designed to meet this timeline
* Business continuity plans should account for this duration

82) Irene’s organization needs to follow PCI DSS standards. If she engages a third party to assess this, what type of audit is she having performed?

a. An internal regulatory audit

b. An external regulatory audit

c. An internal compliance audit

\*d. An external compliance audit

Let me solve this step by step:

1. Let's analyze the key components of Irene's situation:
   * She needs PCI DSS compliance verification
   * She's using a third party (external) assessor
   * PCI DSS is an industry standard, not a government regulation
   * The focus is on compliance with this standard
2. Let's examine each option:

a) Internal regulatory audit:

* + Internal means done by organization's own staff
  + Regulatory refers to government regulations
  + Neither matches this scenario
  + Not correct

b) External regulatory audit:

* + While external is correct (third party)
  + PCI DSS is not a government regulation
  + It's an industry standard
  + Not correct

c) Internal compliance audit:

* + Internal means done by organization's own staff
  + Irene is using a third party
  + Not correct

d) External compliance audit:

* + External matches the third-party assessor
  + Compliance is correct as PCI DSS is a standard
  + This perfectly describes Irene's situation
  + This is the correct answer

1. Conclusion: The answer is d. External compliance audit

This is correct because:

* The audit is external (done by third party)
* PCI DSS is a compliance standard, not a regulation
* The purpose is to verify compliance with industry standards

Key distinctions:

* Internal vs External: Third-party assessment makes this external
* The combination of external + compliance perfectly describes a PCI DSS assessment by a third party

106) Olivia’s cloud service provider claims to provide zero data loss from storage, and Olivia’s company wants to take advantage of that service because loss of data would be extremely costly for the business. What business agreement can Oliva put in place to help ensure that the reliability that the vendor advertises is maintained?

a. An MOU

\*b. An SLA

c. An MSA

d. A BPA

Let me solve this step by step:

1. Let's analyze Olivia's requirements:
   * Needs guaranteed zero data loss
   * Loss would be extremely costly
   * Wants to ensure vendor maintains advertised reliability
   * Needs a binding agreement about service levels
2. Let's examine each option:

a) MOU (Memorandum of Understanding):

* + Non-binding agreement
  + Outlines general principles of cooperation
  + No enforcement mechanisms
  + Too weak for Olivia's needs

b) SLA (Service Level Agreement):

* + Defines specific service levels
  + Includes measurable targets
  + Has penalties for non-compliance
  + Perfect for guaranteeing service reliability
  + Exactly what Olivia needs

c) MSA (Master Service Agreement):

* + General framework for future agreements
  + Too broad for specific service levels
  + Doesn't include detailed performance metrics
  + Not specific enough

d) BPA (Business Partnership Agreement):

* + Wrong type of agreement

1. Conclusion: The answer is b. SLA (Service Level Agreement)

This is the best choice because:

* SLAs specifically define service levels and metrics (like zero data loss)
* They include penalties if service levels aren't met
* They provide legal recourse if the provider fails to deliver
* They're designed exactly for this type of service guarantee

119) The company that Leon works for has experienced a significant malware infection and has segmented their network to prevent further spread. What risk mitigation strategy have they chosen?

a. Avoid

b. Transfer

c. Accept

\*d. Mitigate

Let me solve this step by step:

1. Let's analyze what Leon's company is doing:
   * They experienced a malware infection
   * They responded by segmenting the network
   * They're trying to limit/contain the spread
   * They're taking active steps to reduce impact
   * They haven't eliminated the risk entirely
2. Let's examine each risk strategy:

a) Avoid:

* + Would mean completely eliminating the risk
  + Usually by stopping the activity entirely
  + Would require disconnecting from networks completely
  + Not what's happening here

b) Transfer:

* + Would involve shifting risk to another party
  + Typically through insurance or third-party services
  + No transfer is occurring here
  + Not the strategy being used

c) Accept:

* + Would mean taking no action
  + Just dealing with consequences
  + Clearly not the case as they're actively responding
  + Not the strategy being used

d) Mitigate:

* + Involves reducing risk through controls
  + Risk still exists but impact is reduced
  + Network segmentation is a mitigation control
  + Exactly matches what they're doing

1. Conclusion: The answer is d. Mitigate

This is correct because:

* Network segmentation is a control that reduces risk
* They're not eliminating the risk completely (avoid)
* They're not shifting it to someone else (transfer)
* They're not just accepting it (accept)
* They're actively working to reduce its impact (mitigate)

The company is using a classic mitigation strategy: implementing controls (network segmentation) to reduce the impact and spread of a threat while allowing necessary business operations to continue.

128) Valerie knows that her organization’s datacenter power infrastructure has an MTTR of 24 hours. What should she do if there is a critical component failure in her power infrastructure, and the organization has a warm site with an activation of 12 hours and needs to be back online as soon as possible?

a. Wait to see if the recovery can be done in less than 24 hours.

\*b. Immediately begin a move to the warm site.

c. Wait to see if the recovery can be done in less than 12 hours.

d. Wait for 12 hours, then begin the move to the warm site.

Let me solve this step by step:

1. Let's analyze the key information:
   * MTTR (Mean Time To Repair) for power = 24 hours
   * Warm site activation time = 12 hours
   * Need to be back online ASAP
   * Critical component failure has occurred
2. Let's do time calculations:
   * If they wait for full MTTR: 24 hours downtime
   * If they move to warm site: 12 hours downtime
   * 12 hours < 24 hours
   * Waiting risks longer downtime
3. Let's examine each option:

a) Wait to see if recovery can be done in < 24 hours:

* + Risks maximum downtime
  + Goes against "back online ASAP" requirement
  + Not the best choice

b) Immediately begin move to warm site:

* + Guarantees 12-hour recovery
  + Better than potential 24-hour downtime
  + Meets "back online ASAP" requirement
  + This is the best choice

c) Wait to see if recovery can be done in < 12 hours:

* + Risks extending total downtime
  + If repair fails, adds waiting time to warm site activation
  + Not optimal

d) Wait 12 hours, then move to warm site:

* + Guarantees at least 24 hours downtime (12 wait + 12 activation)
  + Worse than immediate warm site activation
  + Not a good choice

1. Conclusion: The answer is b. Immediately begin a move to the warm site.

This is correct because:

* Known MTTR (24 hours) is longer than warm site activation (12 hours)
* Moving immediately guarantees fastest recovery
* Any waiting adds potential downtime
* It best meets the requirement of being "back online ASAP"

136) What process reviews control objectives for an organization, system, or service to determine if controls do not meet the control objectives?

a. A penetration test

\*b. A gap analysis

c. A Boolean analysis

d. A risk analysis

Let me solve this step by step:

1. Let's analyze what the question is asking about:
   * Process that reviews control objectives
   * Compares existing controls against objectives
   * Looks for missing or inadequate controls
   * Identifies where controls don't meet objectives
2. Let's examine each option:

a) Penetration Test:

* + Tests security by simulating attacks
  + Focuses on finding vulnerabilities
  + Doesn't specifically compare against control objectives
  + Not the right answer

b) Gap Analysis:

* + Compares current state vs desired state
  + Identifies missing or inadequate controls
  + Specifically looks for gaps between objectives and reality
  + Exactly matches the description

c) Boolean Analysis:

* + Relates to logical operations (AND, OR, NOT)
  + Not related to control objectives
  + Not a security assessment process
  + Not the right answer

d) Risk Analysis:

* + Identifies and evaluates potential risks
  + Focuses on threats and vulnerabilities
  + Doesn't specifically compare against control objectives
  + Not the right answer

1. Conclusion: The answer is b. Gap Analysis

This is correct because:

* Gap analysis specifically looks at differences between current and desired states
* It identifies where controls are missing or inadequate
* It compares actual controls against control objectives
* It's designed to find areas where objectives aren't being met

142) What term describes the possibility of a risk occurring?

a. Impact

\*b. Likelihood

c. Potential

d. Rate of occurrence

Let me think about this step by step:

1. Let's examine what we're looking for:
   * Term that describes if a risk might happen
   * Measure of how probable a risk is
   * The chance of a risk becoming reality
   * Not how bad it would be, just how possible it is
2. Let's analyze each option:

a) Impact:

* + Measures the severity if risk occurs
  + Describes consequences, not probability
  + Answers "how bad?" not "how possible?"
  + Not the correct answer

b) Likelihood:

* + Measures probability of occurrence
  + Describes how likely something is to happen
  + Exactly matches what we're looking for
  + This is the correct answer

c) Potential:

* + Too vague and general
  + Could refer to impact or probability
  + Not a specific risk assessment term
  + Not precise enough

d) Rate of occurrence:

* + Measures how often something happens
  + More about frequency than possibility
  + Usually expressed as times per period
  + Similar but not exactly what we're looking for

1. Conclusion: The answer is b. Likelihood

This is correct because:

* Likelihood specifically refers to the probability of a risk occurring
* It's a standard term in risk assessment
* It's precisely focused on possibility of occurrence
* It's the technical term used in risk calculations (Likelihood × Impact)

151) Which of the following is not a commonly used business data classification?

a. Sensitive

b. Confidential

\*c. Top Secret

d. Public

Let me solve this step by step:

1. Let's examine typical business data classifications:
   * Public (openly shared)
   * Internal/Private (for company use)
   * Confidential (restricted sharing)
   * Sensitive (requires special handling)
   * Proprietary (business ownership)
2. Let's examine each option:

a) Sensitive:

* + Common in business settings
  + Used for personal data, financial info
  + Standard business classification
  + Is a commonly used classification

b) Confidential:

* + Very common in business
  + Used for restricted information
  + Standard business classification
  + Is a commonly used classification

c) Top Secret:

* + Military/government classification
  + Not typically used in business
  + Part of government classification system
  + NOT a common business classification

d) Public:

* + Common in business settings
  + Used for marketing materials, press releases
  + Standard business classification
  + Is a commonly used classification

1. Conclusion: The answer is c. Top Secret

This is correct because:

* "Top Secret" is a government/military classification
* It's not typically used in business environments
* Businesses use different terminology for their highest levels of classification
* The other options (Sensitive, Confidential, Public) are all standard business classifications

156) Which of the following techniques attempts to predict the likelihood a threat will occur and assigns monetary values should a loss occur?

a. Change management

b. Vulnerability assessment

c. Qualitative risk assessment

\*d. Quantitative risk assessment

Let me solve this step by step:

1. Let's analyze what we're looking for:
   * Predicts likelihood of threats
   * Assigns monetary values to losses
   * Focuses on numerical predictions
   * Deals with financial impact
2. Let's examine each option:

a) Change Management:

* + Process for controlling changes
  + Doesn't predict threats
  + Doesn't assign monetary values
  + Not focused on risk assessment

b) Vulnerability Assessment:

* + Identifies security weaknesses
  + Doesn't typically assign monetary values
  + Focuses on finding vulnerabilities
  + Doesn't predict likelihood

c) Qualitative Risk Assessment:

* + Uses descriptive terms (high/medium/low)
  + Doesn't use monetary values
  + More subjective approach
  + Not focused on numerical predictions

d) Quantitative Risk Assessment:

* + Uses numerical values
  + Assigns specific monetary values
  + Calculates probability
  + Uses formulas like ALE = SLE × ARO
  + Exactly matches what we're looking for

1. Conclusion: The answer is d. Quantitative Risk Assessment

Example calculation:

* Asset Value = $100,000
* Exposure Factor = 30%
* Single Loss Expectancy = $30,000
* Annual Rate of Occurrence = 0.1
* Annual Loss Expectancy = $3,000

162) You have an asset that is valued at $16,000, the exposure factor of a risk affecting that asset is 35 percent, and the annualized rate of occurrence is 75 percent. What is the SLE?

\*a. $5,600

b. $5,000

c. $4,200

d. $3,000

Let me solve this step by step:

1. Let's identify the formula for Single Loss Expectancy (SLE):
   * SLE = Asset Value (AV) × Exposure Factor (EF)
2. Let's identify the known values:
   * Asset Value (AV) = $16,000
   * Exposure Factor (EF) = 35% = 0.35
   * Annualized Rate of Occurrence (ARO) = 75% = 0.75 (Note: ARO isn't needed for SLE calculation)
3. Let's calculate SLE:
   * SLE = $16,000 × 0.35
   * SLE = $5,600
4. Conclusion: The answer is a. $5,600

This is correct because:

* We properly applied the SLE formula: AV × EF
* We used the correct values:
  + AV = $16,000
  + EF = 35% = 0.35
* The calculation $16,000 × 0.35 = $5,600
* Note: The ARO (75%) wasn't needed for this calculation as it's only used for calculating ALE (Annual Loss Expectancy)