Domains of Computer Security, 2001, John Wiley & Sons, Page 313.
http://www.duhaime.org/LegalDictionary/E/ExigentCircumstances.aspx

QUESTION 554
Which of the following is an advantage of a qualitative over a quantitative risk analysis?

A. It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
B. It provides specific quantifiable measurements of the magnitude of the impacts.
C. It makes a cost-benefit analysis of recommended controls easier.
D. It can easily be automated.

Correct Answer: A
Explanation:
The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. It does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-analysis of any recommended controls difficult. Since it involves a consensus of export and some guesswork based on the experience of Subject Matter Experts (SME's), it can not be easily automated.

Reference used for this question:
STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for Information Technology Systems, 2001 (page 23).

QUESTION 555
In addition to the Legal Department, with what company function must the collection of physical evidence be coordinated if an employee is suspected?

A. Human Resources
B. Industrial Security
C. Public Relations
D. External Audit Group

Correct Answer: A
Explanation:
If an employee is suspected of causing an incident, the human resources department may be involved--for example, in assisting with disciplinary proceedings.

Legal Department. The legal experts should review incident response plans, policies, and procedures to ensure their compliance with law and Federal guidance, including the right to privacy. In addition, the guidance of the general counsel or legal department should be sought if there is reason to believe that an incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit, or if there may be a need for a memorandum of understanding (MOU) or other binding agreements involving liability limitations for information sharing.

Public Affairs, Public Relations, and Media Relations. Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public.

The Incident response team members could include:

Management
Information Security

Legal / Human Resources
Public Relations
Communications
Physical Security
Network Security
Network and System Administrators
Network and System Security Administrators
Internal Audit

Events versus Incidents
An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This guide addresses only adverse events that are computer security- related, not those caused by natural disasters, power failures, etc.

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Examples of incidents are:
An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.

Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.

An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.

A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

The following answers are incorrect:

Industrial Security. Is incorrect because it is not the best answer, the human resource department must be involved with the collection of physical evidence if an employee is suspected.

public relations. Is incorrect because it is not the best answer. It would be an important element to minimize public image damage but not the best choice for this question.

External Audit Group. Is incorrect because it is not the best answer, the human resource department must be involved with the collection of physical evidence if an employee is suspected.

Reference(s) used for this question:
NIST Special Publication 800-61

QUESTION 556
Which of the following teams should NOT be included in an organization's contingency plan?

A. Damage assessment team
B. Hardware salvage team
C. Tiger team

D. Legal affairs team

Correct Answer: C
Explanation:
According to NIST's Special publication 800-34, a capable recovery strategy will require some or all of the following functional groups: Senior management official, management team, damage assessment team, operating system administration team, systems software team, server recovery team, LAN/WAN recovery team, database recovery team, network operations recovery team, telecommunications team, hardware salvage team, alternate site recovery coordination team, original site restoration/salvage coordination team, test team, administrative support team, transportation and relocation team, media relations team, legal affairs team, physical/personal security team, procurements team. Ideally, these teams would be staffed with the personnel responsible for the same or similar operation under normal conditions. A tiger team, originally a U.S. military jargon term, defines a team (of sneakers) whose purpose is to penetrate security, and thus test security measures. Used today for teams performing ethical hacking.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 23).

QUESTION 557
Devices that supply power when the commercial utility power system fails are called which of the following?

A. power conditioners
B. uninterruptible power supplies
C. power filters
D. power dividers

Correct Answer: B
Explanation:
From Shon Harris AIO Fifth Edition:

Protecting power can be done in three ways: through UPSs, power line conditioners, and backup sources.

UPSs use battery packs that range in size and capacity. A UPS can be online or standby.

Online UPS systems use AC line voltage to charge a bank of batteries. When in use, the UPS has an inverter that changes the DC output from the batteries into the required AC form and that regulates the voltage as it powers computer devices.

Online UPS systems have the normal primary power passing through them day in and day out. They constantly provide power from their own inverters, even when the electric power is in proper use. Since the environment's electricity passes through this type of UPS all the time, the UPS device is able to quickly detect when a power failure takes place. An online UPS can provide the necessary electricity and picks up the load after a power failure much more quickly than a standby UPS.

Standby UPS devices stay inactive until a power line fails. The system has sensors that detect a power failure, and the load is switched to the battery pack. The switch to the battery pack is what causes the small delay in electricity being provided. So an online UPS picks up the load much more quickly than a standby UPS, but costs more of course.

QUESTION 558

The MOST common threat that impacts a business's ability to function normally is:

A. Power Outage
B. Water Damage
C. Severe Weather
D. Labor Strike

Correct Answer: A
Explanation:
The MOST common threat that impacts a business's ability to function normally is power. Power interruption cause more business interruption than any other type of event.

The second most common threat is Water such as flood, water damage from broken pipe, leaky roof, etc...

Threats will be discovered while doing your Threats and Risk Assessments (TRA). There are three elements of risks: threats, assets, and mitigating factors (countermeasures, safeguards, controls).

A threat is an event or situation that if it occured would affect your business and may even prevent it from functioning normally or in some case functioning at all. Evaluation of threats is done by looking at Likelihood and Impact of possible threat. Safeguards, countermeasures, and controls would be used to bring the threat level down to an acceptable level.

Other common events that can impact a company are:

Weather, cable cuts, fires, labor disputes, transportation mishaps, hardware failure, chemical spills, sabotage.

References:
The Official ISC2 Guide to the CISSP CBK, Second Edition, Page 275-276

QUESTION 559
Which of the following recovery plan test results would be most useful to management?

A. elapsed time to perform various activities.
B. list of successful and unsuccessful activities.
C. amount of work completed.
D. description of each activity.

Correct Answer: B
Explanation:
After a test has been performed the most useful test results for manangement would be knowing what worked and what didn't so that they could correct the mistakes where needed.

The following answers are incorrect:

elapsed time to perform various activities. This is incorrect because it is not the best answer, these results are not as useful as list of successful and unsuccessful activities would be to managment.
amount of work completed. This is incorrect because it is not the best answer, these results are not as useful as list of successful and unsuccessful activities would be to managment.
description of each activity. This is incorrect because it is not the best answer, these results are not as useful as list of successful and unsuccessful activities would be to managment.

QUESTION 560
To protect and/or restore lost, corrupted, or deleted information, thereby preserving the data integrity and availability is the purpose of:

A. Remote journaling.
B. Database shadowing.
C. A tape backup method.
D. Mirroring.

Correct Answer: C
Explanation:
The purpose of a tape backup method is to protect and/or restore lost, corrupted, or deleted information, thereby preserving the data integrity and ensuring availability.

All other choices could suffer from corruption and it might not be possible to restore the data without proper backups being done.

This is a tricky question, if the information is lost, corrupted, or deleted only a good backup could be use to restore the information. Any synchronization mechanism would update the mirror copy and the data could not be recovered.

With backups there could be a large gap where your latest data may not be available. You would have to look at your Recovery Point Objective and see if this is acceptable for your company recovery objectives.

The following are incorrect answers:

Mirroring will preserve integrity and restore points in all cases of drive failure. However, if you have corrupted data on the primary set of drives you may get corrupted data on the secondary set as well.

Remote Journaling provides Continuous or periodic synchronized recording of transaction data at a remote location as a backup strategy. (http://www.businessdictionary.com/definition/remote-journaling.html) With journaling there might be a gap of time between the data updates being send in batch at regular interval. So some of the data could be lost.

Database shadowing is synonymous with Mirroring but it only applies to databases, but not to information and data as a whole.

Reference(s) used for this question:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 68.

QUESTION 561
After a company is out of an emergency state, what should be moved back to the original site first?

A. Executives
B. Least critical components
C. IT support staff
D. Most critical components