First and last name .....

Question 1/87

What does Zero Outage **not** consider a barrier to good IT security

A. Lacking transparency in the supply chain.
B. Contractual agreements not considering IT security.
C. Lacking cooperation and unclear responsibilities.
D. IT outsourcing / cloud computing.

Question 2/87

What does Zero Outage consider underestimated but indeed relevant for managing IT security?

A. Division of labour and industrialisation of IT service provisioning.
B. Governance.
C. Risk management.
D. Compliance.

Question 3/87

What does Zero Outage consider underestimated but indeed relevant with respect to IT security?

A. Governance.
B. Risk management.
C. Compliance.
D. Using an architectural, systematic approach.

Question 4/87

What trend is Zero Outage specifically considering when it comes to IT security?

A. Green IT.
B. Data privacy.
C. IT outsourcing / cloud computing.
D. Supply bottlenecks.

Question 5/87

What does Zero Outage provide?

A. We are talking about problems only.
B. We deliver news from the security community.
C. We provide daily updated information about vulnerabilities.
D. The emphasis is put onto solutions not problems.

Question 6/87

What is the philosophy of Zero Outage association?

A. Providing solutions that help organisations and people achieving appropriate IT security.
B. Identifying the underlying true problems is fairly enough.
C. Subscribe to our newsletter, that's almost everything you need.
D. Buy the service and products of Zero Outage members.

Question 7/87

What describes the philosophy of Zero Outage best?

A. We touch on topics that are currently in the news.
B. We touch on topics that other frameworks may not cover.
C. We pick up on topics that seem to be in vogue right now.
D. We pick up on topics that may grow the business of Zero Outage members.

Question 8/87

What is the scope of our security standards?

A. Consumer products only.
B. Business products only.
C. IT service and product provisioning.
D. IT service management.

Question 9/87

ZOIS publishes architectural models. Why?

A. Articles are actually provided but architecture sound much better.
B. As a means to e. g. help manage the complexity.
C. Want to emphasise that we also have diagrams.
D. ZOIS has an Architecture workstream.

Question 10/87

What is the ESARIS Security Taxonomy?

A. A powerful tool for measuring IT security risks.
B. A powerful tool for measuring the urgency of acting.
C. A classification and organisation schema showing all areas of activity.
D. A badge for Zero Outage members.

Question 11/87

What does the ESARIS Security Taxonomy show?

A. Different areas of activity.
B. Different level of detail and abstraction.
C. Topics with different urgency and criticality.
D. Topics measured according to their risk profile.

Question 12/87

Zero Outage promotes building a hierarchy of security standards. Why?

A. Each layer in the hierarchy is about a different topic. IT security is in the middle.
B. The layers in the hierarchy are like chapters in a book and nothing more.
C. The security standards need to be progressively refined and serve different purposes.
D. Standards on the top are important. The ones in the lower layers are not.

Question 13/87

Why does ZOIS recommend using a hierarchy of security standards?

A. There is Secure by Design on the top, then vulnerability management in the middle and so on.
B. There is cloud security on the top, then other topics below that.
C. Organisations require a document structure that auditors may not have seen before.
D. Organisations require standards for the overall management of IT security as well as very detailed ones that direct, guide and support implementation.

Question 14/87

Why does Zero Outage recommend using a hierarchy of security standards?

A. Admins prefer voluminous documents, where they finally find the information relevant to them on page 217.
B. Admins like to study the company's general security policies, but it's better to hide these from them.
C. Admins don't want to read guiding principles and managers may not read hardening guidelines.
D. Admins don't need to use technical specifications and instructions. That's why we have to deliver very general top-level guiding principles.

Question 15/87

Why does Zero Outage demand a modular specification?

A. Sounds good.
B. IT security is mostly vague, so that is requires frequent corrections.
C. The IT is a dynamic environment. Security demands may change. Modularity eases updates and maintains flexibility.
D. There is no reliable concept for IT security whatsoever. We only have snippets which we call modules.

Question 16/87

People are the backbone and the most valuable asset of every organization. What percentage of outages are caused by humans.

A. 50 – 70%
B. 40 – 60%
C. 60 – 80%
D. 70 – 90%

Question 17/87

What does PDCA stand for?

A. PLAN – DEDICATE – CHECK - ACT
B. PLAN – DO – CHECK – ACT
C. PLAY – DO – CHASE – AQUIRE
D. PLAN – DEMONSTRATE – CHECK – ACTION

Question 18/87

Choose three Methodical Competencies

A. Integration, execution, and improvement of Zero Outage within the organisation.
B. Practice lessons learned to aim for the best results based on customer experience.
C. Sense of urgency to reduce business impacts.
D. Integration of customer quality view and perception for Zero Outage processes and policies.

Question 19/87

Name the 4 phases of how the People Functional Lifecycle is aligned to IT4IT.

A. Plan, Believe, Drive, Run
B. Plan, Begin, Deliver, Run
C. Play, Build, Drive, Run
D. Plan, Build, Deliver, Run

Question 20/87

Which of the following are part of the Competency model?

a. Functional Competency
b. Interpersonal Competency
c. Organisational Competency
d. Methodical Competency

A. a, b, c
B. a, c, d
C. b, c, d
D. a, b, d

Question 21/87

According to ZOIS, a professional continuous improvement framework is key.

A. True
B. False

Question 22/87

Which of the following are part of the “Plan” activity from the Organisational Environment?

A. Measurable business objectives, targets & Service Levels.
B. Measurable competency and behaviour targets as per ZOIS people standards.
C. Financial and resource planning (body leasing, facility, training, tools, etc.).
D. All of the above.

Question 23/87

Which of the below are considered Interpersonal Competencies (choose 2)

A. Pro-active work approach & Communication.
B. Practice of standard management principles & Rigorous adherence of defined procedures and processes .
C. Teamwork & Sense for quality.
D. Review of the Service Levels & Learning from mistakes.

Question 24/87

Which is the best describtion of Methodical Competency?

A. Defining the standard competencies an employee needs to understand.
B. The minimum criteria an organisation or company needs to provide to successfully manage its people and their outcomes.
C. Defining the knowledge and experience needed to accurately perform tasks in accordance with Zero Outage standards.
D. The consequent implementation of defined procedures and processes

Question 25/87

Why is an organisational environment important? (choose 2)

A. To create perfection for its own sake.
B. To develop and sustain a “culture” in an organisation.
C. To have a professional continuous improvement framework.
D. To halt improvements and eliminate perfection.

Question 26/87

The competency model outlines what qualifications are required to meet Zero Outage criteria. In addition to functional skills, interpersonal and environmeltal competencies are just as vital for success.

A. True
B. False

Question 27/87

One interpersonal competency is the “art” of taking decisions. Which of the following 3 fall into the category of “Decision making”?

A. The decision maker gathers information.
B. The decision maker listens effectively.
C. The decision maker identifies problems.
D. The decision maker shares information.

Question 28/87

Working in Zero Outage environments requires key competencies to align with job roles to ensure people are best suited to perform their tasks.

A. True
B. False

Question 29/87

Which competencies do people working in Zero Outage environments need to possess?

A. Functional competencies
B. Methodical competencies
C. Interpersonal competencies
D. All of the above

Question 30/87

Who benefits most from the Competency Model?

A. People
B. Processes
C. Platforms
D. All of the above

Question 31/87

What are the aims of Zero Outage?

A. To ensure the least possible downtime for the customer's greatest possible business capability.
B. To define, introduce and implement standards.
C. To systematically sensitize all staff to the issue of quality.
D. Maximum resource utilization

Question 32/87

What does the Zero Outage value system focus on?

A. Making hasty decisions and trusting gut feelings.
B. Rejecting responsibility and defending oneself against accusations.
C. The concept of quality is anchored in the corporate culture over the long term.
D. If a risk is identified, pass on information and concerns to direct co-workers only.

Question 33/87

Ideally, how should staff/managers contribute to Zero Outage?

A. Always be up-to-date.
B. Comply with/exemplify standards.
C. Have a sense of urgency.
D. Attend customer meetings once a year.

Question 34/87

What can you do to contribute towards improvements in Zero Outage at your organization?

A. Get in to work early.
B. There should, if possible, be a chance to give direct feedback.
C. Do the Zero Outage training and put the content into practice in everyday work.
D. Carry out all tasks myself.

Question 35/87

Only a central quality department is responsible for implementing Zero Outage in an organization.

A. Yes
B. No

Question 36/87

Which prerequisites must Zero Outage platforms fulfill?

A. Standardized, high-performance and highly available
B. Standardized, high output efficiency and availability
C. Standardized, stable and high output efficiency

Question 37/87

Which of these are frequent causes of platform faults?

A. Faulty firmware
B. Obsolete hardware
C. Poor monitoring
D. Process errors

Question 38/87

What are often reasons for hardware changes?

A. To replace old or faulty hardware.
B. Maintenance is not assured anymore.
C. To close security loopholes.
D. Process errors

Question 39/87

What is the primary objective of Change Management?

A. To delay changes as much as possible.
B. To ensure standardized methods and procedures are used for efficient handling of all changes.
C. To create chaos in IT operations.
D. To bypass security measures for quick updates.

Question 40/87

What is the role of the Change Manager?

A. To implement changes directly.
B. To review and approve changes, ensuring compliance with policies.
C. To develop marketing strategies.
D. To handle customer complaints.

Question 41/87

What is a "Change Window"?

A. A period when no changes are allowed.
B. A designated time frame when changes can be implemented with minimal disruption.
C. A random time selected for changes.
D. A financial reporting period.

Question 42/87

What is a potential risk of not having a Change Management process

A. Increased efficiency.
B. Greater collaboration.
C. Higher likelihood of service disruptions and incidents.
D. Improved security.

Question 43/87

Which activity is part of the Change Implementation stage?

A. Risk assessment.
B. Post Implementation Review.
C. Communication with stakeholders.
D. Testing the change in a controlled environment.

Question 44/87

What is the role of testing in Change Management?

A. To skip testing to save time.
B. To verify that the change works as intended and does not negatively impact other systems.
C. To delay the implementation process.
D. To avoid detecting potential issues.

Question 45/87

What is the primary purpose of Event Management?

A. To schedule system updates.
B. To detect, correlate, and respond to events within an IT infrastructure.
C. To generate financial reports.
D. To conduct user training sessions.

Question 46/87

Which of the following is an example of an informational event?

A. A server crash.
B. A transaction completed successfully.
C. Memory utilization exceeding 75%.
D. A storage volume nearing maximum capacity.

Question 47/87

Which of the following is NOT an activity involved in Event Notification & Detection?

A. Polling a device by a management tool.
B. Generating a notification when certain conditions are met.
C. Creating financial reports based on event logs.
D. Interpreting notifications received from a CI.

Question 48/87

What is an example of an alert that would typically be escalated to the incident management team?

A. A successful login event.
B. A backup job completed successfully.
C. A server going offline unexpectedly.
D. A routine system update notification.

Question 49/87

What is a "Critical Event" according to the Zero Outage Industry Standard?

A. An event that is purely informational and does not require action.
B. An event that can be ignored without business impact.
C. An event where an Operational or Service Level Agreement has been breached and the business has been impacted.
D. An event indicating successful completion of a routine task.

Question 50/87

How are events categorized in the Zero Outage Industry Standard?

A. Randomly without any criteria.
B. Based on criticality, such as informational, warning, and exception events.
C. Only by their occurrence time.
D. By their financial impact.

Question 51/87

What is the primary objective of event monitoring in the Zero Outage Industry Standard?

A. To reduce the cost of IT services.
B. To detect and handle events to prevent outages.
C. To increase the number of events detected.
D. To eliminate the need for IT infrastructure.

Question 52/87

Which of the following is a key principle of event monitoring in the Zero Outage Industry Standard?

A. Manual intervention.
B. Reactive response to incidents.
C. Proactive detection of conditions affecting service availability.
D. Reducing the number of IT staff

Question 53/87

What type of events should be prioritized in the Zero Outage Industry Standard?

A. All events equally.
B. Events that have the potential to disrupt service availability.
C. Only events related to hardware failures.
D. Events that do not impact users.

Question 54/87

How should events be categorized according to their importance?

A. By their occurrence time.
B. By their potential impact on service availability.
C. By their source system.
D. By their frequency.

Question 55/87

What is the role of machine learning in event monitoring?

A. To automate the response to events.
B. To predict and prevent potential issues.
C. To increase manual intervention.
D. To reduce the amount of data collected.

Question 56/87

What is the role of continuous improvement in event monitoring?

A. To constantly refine and enhance monitoring practices.
B. To increase the number of alerts.
C. To reduce the effectiveness of monitoring.
D. To simplify IT infrastructure.

Question 57/87

What is the primary objective of incident management?

A. To permanently solve all IT issues.
B. To maintain business profitability.
C. To restore normal service operation quickly.
D. To train IT staff in incident resolution.

Question 58/87

What does 'normal service operation' mean in incident management?

A. All systems functioning without errors.
B. Services and CIs performing within agreed levels.
C. No customer complaints are being reported.
D. All services operating at maximum efficiency.

Question 59/87

During an incident, what is the key goal of the management process?

A. To conduct a thorough investigation of fault.
B. To restore service operation to normal levels as quickly as possible.
C. To update all system documentation.
D. To schedule meetings with stakeholders.

Question 60/87

What is an indicator of successful incident management?

A. Zero incidents reported.
B. Quick restoration of normal operations.
C. Increased IT budget.
D. More frequent software updates.

Question 61/87

What ensures the resilience of business operations during IT incidents?

A. Regular system downtime.
B. Strong leadership.
C. Effective incident management.
D. Frequent training programs.

Question 62/87

The primary focus during an IT incident should be on:

A. Collecting feedback from all users.
B. Documenting every step for future audits.
C. Restoring agreed service levels as swiftly as possible.
D. Discussing the incident in team meetings.

Question 63/87

Which best describes a proactive incident management approach?

A. Waiting for users to report issues.
B. Monitoring systems to preemptively address disruptions.
C. Scheduling regular meetings to discuss potential incidents.
D. Updating software only after an incident occurs.

Question 64/87

What is the primary goal of proactive problem management?

A. To document all problems after they occur.
B. To prevent problems before they occur.
C. To resolve problems only after significant impact.
D. To prioritize problems based on complexity.

Question 65/87

What is a common tool used for problem detection?

A. Customer surveys.
B. Automated monitoring systems.
C. Annual performance reviews.
D. Manual tracking methods.

Question 66/87

How should problems be resolved to ensure improvement in system reliability?

A. By applying quick fixes that are easy to implement.
B. Through comprehensive solutions that address root causes.
C. By outsourcing problem resolution to external vendors.
D. By resetting systems to their default settings.

Question 67/87

Which of the following is a primary tool in problem detection?

A. Customer feedback forms.
B. Incident reports from service desks.
C. Manual inspections by staff.
D. Periodic system upgrades.

Question 68/87

In problem management, what is the importance of identifying event risks?

A. It allows for the immediate dismissal of minor risks.
B. It prioritizes risks based on their potential impact on operations.
C. It is a procedural formality with no practical impact.
D. It ensures that all risks are documented, regardless of severity.

Question 69/87

How can problem management processes be optimized?

A. By focusing on the fastest possible solutions to all issues.
B. Through continuous improvement based on feedback and performance analysis.
C. By reducing the number of staff involved in problem resolution.
D. By increasing the complexity of problem solving procedures.

Question 70/87

What is the primary goal of the Platform Workstream in the context of a Zero Outage (ZO) IT implementation?

A. To reduce costs of IT infrastructure.
B. To describe architectural and design principles for uninterrupted uptime.
C. To create new software applications.
D. To eliminate the need for security protocols.

Question 71/87

What are the four phases of the Zero Outage Value Map that must be adhered to in a ZO implementation?

A. Plan, Build, Deploy, and Run
B. Design, Implement, Test, and Deploy
C. Plan, Build, Deliver, and Run
D. Design, Build, Deploy, and Operate

Question 72/87

Which of the following is NOT considered a building block in a Zero Outage architecture model?

A. Network components
B. Firewalls
C. User Interface Design
D. Servers

Question 73/87

In the context of a ZO implementation, what is the purpose of staging?

A. To train new IT personnel.
B. To isolate and test changes in a non-production environment.
C. To run backup processes.
D. To monitor network traffic.

Question 74/87

What kind of events can affect all layers of a Zero Outage implementation and cannot be addressed purely on an architectural level?

A. Hardware defects
B. Security issues
C. Environmental shortages
D. Software bugs

Question 75/87

Which deployment model is not considered when discussing ZOIS (Zero Outage Industry Standard) implementation?

A. On-premise
B. Cloud
C. Hybrid
D. Local Area Network (LAN)

Question 76/87

Why is it important to have clear boundaries in a ZO implementation?

A. To ensure that only selected vendors are used.
B. To clearly define which parts belong to the ZO implementation and to control them effectively.
C. To reduce the cost of operations.
D. To limit the scope of monitoring.

Question 77/87

What is the purpose of having redundant paths and links in a ZO-compliant network architecture?

A. To improve network speed.
B. To ensure continuous availability in case of link or node failure.
C. To reduce the complexity of the network.
D. To avoid the need for monitoring

Question 78/87

What will be checked during the release of a new software/hardware?

A. *Bug reports
B. *CERT Messages
C. *Availibity Ceck of hardware/software vendors
D. *Compliance check
E. Time for implementation/build up

Question 79/87

What are often reasons for hardware changes?

A. To replace old or faulty hardware.
B. Maintenance is not assured anymore.
C. To close security loopholes.
D. Process errors

Question 80/87

Which prerequisites must Zero Outage platforms fulfill?

A. Standardized, high-performance and highly available
B. Standardized, high output efficiency and availability
C. Standardized, stable and high output efficiency

Question 81/87

Which of these are frequent causes of platform faults?

A. Process errors
B. Obsolete hardware
C. Poor monitoring
D. Faulty firmware

Question 82/87

What are the aims of Zero Outage?

A. To ensure the least possible downtime for the customer’s greatest possible business capability.
B. Maximum resource utilization.
C. To define, introduce and implement standards.
D. To systematically sensitize all staff to the issue of quality.

Question 83/87

What does the Zero Outage value system focus on?

A. Making hasty decisions and trusting gut feelings.
B. Rejecting responsibility and defending oneself against accusations.
C. The concept of quality is anchored in the corporate culture over the long term.
D. If a risk is identified, pass on information and concerns to direct co-workers only.

Question 84/87

By what means can we increase high availability of an IT solution?

A. Introducing redundancy
B. Enabling data mirroring
C. Performing regular backups
D. All of above

Question 85/87

Ideally, how should staff/managers contribute to Zero Outage?

A. Comply with/exemplify standards.
B. Attend customer meetings once a year.
C. Always be up-to-date.
D. Have a sense of urgency.

Question 86/87

Only a central quality department is responsible for implementing Zero Outage.

A. Yes
B. No

Question 87/87

What is the 3-P principle?

A. Three-stage problem management.
B. When personnel, processes and platforms are in total harmony.
C. When 3% of the revenue is invested in quality.