SIMULATION EXAM 11 — QUESTIONS 1–100

1. A client has deployed Microsoft Teams Rooms on certified hardware. The integrator needs to understand the platform's endpoint certification requirements. What is the most appropriate information source?

A. The AVIXA CTS study guide

B. Generic manufacturer marketing

C. Online forums

D. Microsoft's official Teams Rooms certification documentation

2. An AV-over-IP system operates on a 1 Gigabit Ethernet network. Which compression class is most appropriate for this infrastructure?

A. Uncompressed 4K60 4:4:4 at approximately 12 Gbps

B. Uncompressed 8K60 video

C. Visually lossless compressed 4K at approximately 800 Mbps

D. JPEG-based still image compression

3. A CTS holder is integrating with a Zoom Rooms system. Which is the most accurate description of Zoom Rooms' architecture?

A. An on-premises server managing the meeting

B. A cloud-based meeting service with certified in-room devices

C. A proprietary network that bypasses the internet

D. A peer-to-peer meeting platform without cloud infrastructure

4. A CTS holder is configuring cybersecurity for newly deployed AV devices. The most appropriate baseline practice is:

A. Change all default administrative passwords to strong, unique credentials

B. Connect devices directly to the internet for easier management

C. Share a single password across all AV devices in the installation

D. Disable all authentication for simplicity

5. IPMX is an emerging open standard for AV-over-IP. Which description is most accurate about IPMX?

A. A proprietary protocol from a single manufacturer

B. An audio-only protocol

C. A consumer-grade streaming technology

D. An open standards-based framework built on SMPTE 2110 technologies

6. A CTS holder is evaluating SDVoE for a new video distribution system. Which is the most accurate description of SDVoE?

A. A Bluetooth-based audio protocol

B. An alliance-defined AV-over-IP technology using 10 Gigabit Ethernet for uncompressed transport

C. A proprietary cable standard for HDMI

D. A software licensing model for conferencing

7. An AV integrator is asked to deploy BYOD conference room support. The most appropriate approach is:

A. Provide in-room camera, microphone, and loudspeaker connectable to user devices via USB-C

B. Require all users to purchase dedicated hardware

C. Use only speakerphones on the table

D. Disable all room equipment during BYOD meetings

8. A CTS holder is configuring a new cloud-based control system. The most important consideration for ongoing service is:

A. The control system's color scheme

B. The control system's marketing platform

C. The control system's reliability, authentication, API stability, and support commitments

D. The control system's manufacturer prestige

9. A client has asked about the difference between Dante and AES67. The most accurate response is:

A. Dante is open-source; AES67 is proprietary

B. Dante is a proprietary audio-over-IP protocol; AES67 is an open interoperability standard between systems

C. Dante and AES67 are the same technology with different names

D. Both are hardware cable specifications

10. A CTS holder is reviewing a software-based DSP for a conferencing installation. The most important consideration is:

A. The DSP's aesthetic design

B. The DSP's color

C. The DSP's marketing awards

D. The software's reliability, update cadence, security practices, and support availability

11. A client's IT security policy requires that AV devices use TLS 1.2 or higher for secure communications. The most appropriate response is:

A. Verify that all AV devices support TLS 1.2+ before deployment and coordinate with IT for implementation

B. Ignore the policy

C. Use outdated TLS protocols

D. Refuse to work with IT on security

12. A CTS holder is troubleshooting a cloud-based conferencing system where calls have become unreliable. The platform's status page shows normal operations. The most likely cause is:

A. The cloud service has failed entirely

B. All endpoints have simultaneously failed

C. Client-side network, firewall, or authentication changes are affecting the specific installation

D. The display has lost signal

13. An AV-over-IP system requires visually lossless compression at approximately 800 Mbps per stream. The most likely network architecture is:

A. Analog transmission only

B. Single-link fiber for all content

C. Point-to-point HDMI distribution

D. Gigabit Ethernet-based multicast with appropriate QoS and IGMP snooping

14. A CTS holder is managing cloud service credentials for AV devices. The most appropriate approach is:

A. Use unique credentials managed through a centralized credential management platform

B. Hard-code credentials in device configurations

C. Share credentials across all devices

D. Store credentials in unencrypted text files

15. A conferencing platform has rolled out a new audio codec. The most appropriate response is:

A. Ignore the platform change

B. Replace all conferencing hardware

C. Review codec compatibility and adjust DSP or codec settings to accommodate the new platform behavior

D. Downgrade to an older platform version

16. A CTS holder is coordinating with an enterprise identity management system for AV device authentication. The most appropriate integration approach is:

A. Use shared passwords across devices

B. Implement SSO or SAML integration per the identity management system's supported protocols

C. Use local-only authentication without enterprise integration

D. Disable authentication for operational simplicity

17. A client's boardroom is deploying a USB-C-based BYOD system. The most appropriate cable category for the USB-C room connection is:

A. Consumer-grade power-only cables

B. Cables certified for USB-C with power, video, and data at the required specifications

C. Cables from unknown manufacturers

D. Cables designed for previous USB standards only

18. A CTS holder is evaluating a cloud-based room management platform. The most important due-diligence consideration is:

A. The platform's marketing

B. The platform's logo design

C. The platform's social media presence

D. The platform's security practices, uptime SLAs, integration options, and long-term support commitment

19. A client has asked about the latency characteristics of AV-over-IP systems. The most accurate response is:

A. Latency varies by compression, network configuration, and codec; typical uncompressed systems have very low latency, while compressed systems have higher but still acceptable levels

B. AV-over-IP has no latency

C. Latency is always too high for professional use

D. Latency depends only on cable length

20. A CTS holder is implementing network segmentation for AV devices. The most appropriate approach is:

A. Mix AV and general traffic without segmentation

B. Use VLAN segmentation with appropriate QoS configuration, coordinated with IT

C. Disable network security for AV

D. Install a separate physical network without IT coordination

21. A client has deployed Microsoft Teams Direct Routing for their phone system. AV integration must support this. The most appropriate consideration is:

A. Microsoft Teams Direct Routing has no AV relevance

B. The installed endpoints must be certified and configured for the client's Teams Direct Routing environment

C. Use consumer-grade VoIP equipment

D. Bypass Direct Routing entirely

22. A CTS holder is asked about the difference between HDMI 2.0 and HDMI 2.1. The most accurate response is:

A. HDMI 2.0 supports up to 18 Gbps; HDMI 2.1 supports up to 48 Gbps enabling 8K60 and higher

B. HDMI 2.0 and 2.1 are identical

C. HDMI 2.1 is analog

D. HDMI 2.1 has lower bandwidth than 2.0

23. A conferencing codec is experiencing intermittent registration failures correlated with the client's IT security policy updates. The most likely cause is:

A. The codec firmware is universally defective

B. The room cabling has degraded

C. The display has lost signal

D. Security policy updates are disrupting authentication tokens or blocking required ports

24. A CTS holder is evaluating a cloud-based meeting room booking platform. The most important consideration for integration is:

A. The platform's mascot

B. The platform's office location

C. The platform's API documentation, authentication methods, and webhook capabilities for integration

D. The platform's marketing materials

25. A client has asked about the difference between cloud-based and on-premises room management. The most important consideration is:

A. Cloud is always better than on-premises

B. On-premises is always better than cloud

C. Both are identical

D. The choice depends on the client's security posture, operational model, and data residency requirements

26. A CTS holder is configuring a system that will send device telemetry to a cloud-based management platform. The most important consideration is:

A. Maximize telemetry to impress the client

B. Ensure telemetry collection aligns with the client's privacy and data protection policies

C. Collect telemetry without client awareness

D. Disable all telemetry

27. A client's conferencing system integrates with a third-party calendar service via OAuth. The most appropriate understanding of OAuth for AV is:

A. OAuth is a delegated authentication framework where the device can access calendar data without storing user credentials directly

B. OAuth is obsolete for modern systems

C. OAuth requires manual re-authentication daily

D. OAuth is only for consumer applications

28. A CTS holder is implementing certificate-based device authentication. The most appropriate approach is:

A. Use self-signed certificates without management

B. Share a single certificate across all devices

C. Disable certificate validation

D. Implement certificates issued through the client's certificate authority with appropriate lifecycle management

29. A cloud-based conferencing service requires specific network ports to be open. The most appropriate response is:

A. Open all ports to guarantee service

B. Ignore the port requirements

C. Coordinate with IT to open the specific ports required while maintaining security posture

D. Bypass the IT team's firewall

30. A CTS holder is reviewing the security posture of networked AV equipment. The most important consideration is:

A. The equipment's purchase price

B. Patch management, secure configuration baselines, authentication practices, and network segmentation

C. The equipment's aesthetic

D. The equipment's manufacturer tier

31. A conferencing codec has been experiencing intermittent video latency spikes. The network has been verified as stable. The most likely cause is:

A. Codec-internal video processing is producing latency

B. The microphone has failed

C. The display has aged

D. The HDMI cable is too short

32. A CTS holder is evaluating cloud conferencing platform features for a new installation. The most appropriate comparison criteria include:

A. The platform's logo colors

B. The platform's founding date

C. The platform's billing cycle

D. Feature sets, certified devices, admin capabilities, SLAs, and integration options

33. A client requires AV system activity to be monitored and logged for compliance. The most appropriate implementation is:

A. Disable all logging

B. Use only the most verbose logging setting

C. Implement appropriate audit logging with retention policy aligned with compliance requirements

D. Store logs only on local device memory

34. A CTS holder is evaluating an emerging 8K video distribution solution. The most important consideration is:

A. 8K has no professional use cases

B. Evaluate the specific use case, required bandwidth (typically 48+ Gbps uncompressed), display availability, and content considerations

C. Deploy 8K in every installation regardless of need

D. Use 1080p as a universal substitute

35. A client has requested real-time remote management of installed AV equipment. The most appropriate practice is:

A. Coordinate with IT security to implement remote access using approved methods including VPN and multi-factor authentication

B. Install consumer-grade remote access

C. Refuse any remote management

D. Use default credentials for simplicity

36. A CTS holder is troubleshooting a networked AV system where encoders have been dropping out of the multicast stream. The switch configuration appears correct. The most likely cause is:

A. Encoder power supplies have failed

B. All decoders have failed

C. Network switch backplane or uplink is approaching saturation

D. The DSP has reached end-of-life

37. A CTS holder is deploying a new AV-over-IP system with multicast distribution. The most important network configuration is:

A. Wireless mesh networking

B. Consumer-grade switches only

C. Fiber-direct connections for all endpoints

D. IGMP snooping and appropriate QoS on a managed switch

38. A conferencing system vendor has announced end-of-support for a deployed codec model. The most appropriate response is:

A. Develop a replacement plan with the client including timeline, budget, and replacement equipment selection

B. Continue using the codec indefinitely

C. Remove codecs immediately at the integrator's cost

D. Seek third-party unauthorized support

39. A CTS holder is reviewing a proposed AV deployment for a facility with remote workers. The most appropriate design consideration is:

A. Use physical-only security

B. Design for reliable remote access with secure VPN, appropriate monitoring, and tools for remote troubleshooting

C. Ignore remote workers

D. Require all remote workers to come on-site

40. A client is integrating AV with an IoT sensor platform. The most appropriate understanding of modern IoT integration is:

A. IoT integration is always wireless only

B. IoT integration replaces all other technologies

C. IoT requires physical co-location of all devices

D. IoT integration uses MQTT, REST APIs, or similar protocols with appropriate security controls

41. A CTS holder is evaluating whether to recommend a cloud-based DSP for a client. The most important consideration is:

A. Cloud DSPs are always better than hardware

B. Hardware DSPs are always better than cloud

C. The choice depends on latency requirements, network reliability, security, and the specific use case

D. Cloud and hardware DSPs are identical

42. A CTS holder is configuring a network-based AV system to send diagnostic information to a monitoring platform. The most appropriate approach is:

A. Ensure the monitoring configuration aligns with the client's privacy and data governance policies

B. Disable monitoring to reduce data transfer

C. Maximize data collection regardless of policy

D. Collect data without client awareness

43. A CTS holder has been asked to integrate a newly purchased headless AI camera system. The most appropriate approach is:

A. Install without understanding the AI features

B. Research the AI camera's capabilities, integration options, security controls, and operational lifecycle, then plan accordingly

C. Refuse to integrate AI technology

D. Use the camera as if it were a standard PTZ

44. An AV-over-IP system has experienced intermittent stream failures. The network's QoS has been verified as correctly configured. The most likely cause is:

A. The network switch configuration

B. The QoS tagging

C. Device firmware issues, network switch backplane saturation, or endpoint-specific faults

D. Good network infrastructure

45. A CTS holder is deploying a new Zoom Rooms system. The most important installation consideration is:

A. The room's aesthetic

B. The display's color

C. Certified hardware selection, network configuration, and proper account and room setup in the Zoom admin portal

D. The manufacturer's marketing

46. A client has asked about cloud conferencing platform redundancy. The most appropriate response is:

A. Cloud platforms typically provide redundant data center architecture; the client's redundancy strategy should address network path diversity and failover procedures

B. Cloud platforms are always single-point-of-failure

C. All cloud platforms are identical in reliability

D. Cloud platforms do not need redundancy

47. A CTS holder is evaluating a proposed AV-over-IP endpoint. The most important specification is:

A. The endpoint's color

B. The endpoint's price alone

C. The endpoint's codec compatibility, encoding quality, latency, and manufacturer support

D. The endpoint's brand prestige

48. A conferencing codec has been receiving firmware updates automatically. The client has asked about firmware management. The most appropriate approach is:

A. Disable all updates

B. Coordinate with the client on a firmware management strategy that balances security updates with operational stability, with appropriate testing and staging

C. Apply all updates immediately without consideration

D. Only update when failures occur

49. A CTS holder is asked about enterprise SSO integration for AV devices. The most accurate response is:

A. Enterprise SSO is a consumer-only feature

B. Enterprise SSO is not supported by professional AV

C. Enterprise SSO only applies to desktop computers

D. Enterprise SSO enables users to authenticate to AV services using their existing enterprise credentials, typically via SAML or OAuth

50. A CTS holder is implementing a centralized monitoring platform for a multi-room deployment. The most appropriate configuration is:

A. Configure monitoring for proactive alerting on critical issues, with appropriate granularity of monitored metrics and alert routing

B. Disable all alerts

C. Monitor only equipment manufacturers

D. Monitor only one room

51. A CTS holder is reviewing a proposed AV installation's cybersecurity. The most important consideration is:

A. A comprehensive approach including patch management, secure configuration, authentication, network segmentation, and incident response

B. The installation's appearance

C. The installation's age

D. The purchase price only

52. A cloud-based conferencing service has updated its API version. The most appropriate response is:

A. Ignore the update

B. Replace the hardware

C. Disable the integration

D. Plan and execute migration to the new API version before the deprecation date

53. A CTS holder is integrating AV with an enterprise directory service. The most appropriate protocol for typical deployments is:

A. Shared file access

B. LDAP or similar directory protocols that support enterprise directory integration

C. Consumer cloud storage

D. Fax-based authentication

54. A client has requested that AV devices support modern authentication. The most accurate understanding is:

A. Modern authentication is consumer-only

B. Modern authentication includes deprecated protocols

C. Modern authentication refers to current authentication practices like OAuth 2.0, SAML, and multi-factor authentication

D. Modern authentication is less secure than legacy methods

55. A CTS holder is reviewing cloud conferencing platform compliance. The most important consideration for regulated industries is:

A. The platform's certifications (SOC 2, ISO 27001) and specific compliance with applicable regulations like HIPAA, GDPR, PCI

B. The platform's office location

C. The platform's logo design

D. The platform's CEO

56. A CTS holder is implementing OAuth 2.0-based authentication for a cloud integration. The most important consideration is:

A. Hard-code access tokens

B. Share tokens across users

C. Disable token expiration

D. Implement proper token management including secure storage, rotation, and revocation

57. A client's IT team has deployed zero-trust network architecture. AV systems must align with this architecture. The most appropriate response is:

A. Bypass zero-trust

B. Work with IT to design AV integration that aligns with zero-trust principles including identity verification, network segmentation, and continuous authentication

C. Use only default credentials

D. Install AV on an isolated legacy network

58. A CTS holder is troubleshooting a networked audio system where Dante streams experience periodic clicks during general network traffic. The most likely cause is:

A. QoS is not configured to prioritize Dante traffic

B. The DSP has failed

C. The microphones have reached end-of-life

D. The amplifier is clipping

59. A CTS holder is evaluating the total cost of ownership for a proposed AV system. The most important cost considerations include:

A. Only the equipment cost

B. Only the installation cost

C. Equipment, installation, network infrastructure, cloud subscriptions, maintenance, support, and lifecycle replacement

D. Only the warranty cost

60. A client requires AV systems to log all administrative actions. The most appropriate implementation is:

A. Disable all logging

B. Store logs locally without backup

C. Log only failures

D. Implement comprehensive audit logging with appropriate retention and secure storage

61. A CTS holder is evaluating an AV vendor's security practices for inclusion in a procurement process. The most appropriate evaluation is:

A. Review the vendor's security certifications, incident history, vulnerability disclosure process, and product security practices

B. Review only the vendor's pricing

C. Review only the vendor's brand recognition

D. Review only the vendor's marketing claims

62. A CTS holder is troubleshooting a cloud-based conferencing service. The service's status page shows normal operations. The most likely cause of issues is:

A. Client-side network, authentication, or configuration issues affecting the specific installation

B. The service has failed entirely

C. All endpoints have simultaneously failed

D. The display has failed

63. A client has deployed Google Workspace with Google Meet. The AV integration must support this. The most appropriate consideration is:

A. Use only Microsoft Teams

B. Use consumer-grade Google accounts

C. Select certified devices and configure them per Google Meet's deployment requirements, including Google Workspace admin integration

D. Bypass Google Meet entirely

64. A CTS holder is integrating with the client's enterprise mobile device management (MDM) system. The most appropriate consideration is:

A. MDM is not relevant to AV

B. Coordinate with the MDM administrator to ensure any AV-integrated mobile devices or tablets comply with the MDM policies

C. Bypass MDM controls

D. Use only personal devices

65. A CTS holder is implementing network time synchronization (NTP) for AV devices. The most appropriate configuration is:

A. Use enterprise NTP servers configured by IT with appropriate time zones and synchronization monitoring

B. Use internet-based consumer NTP without IT coordination

C. Disable time synchronization

D. Manually set time on each device

66. A CTS holder is evaluating an emerging AV-over-IP codec. The most appropriate consideration is:

A. Adopt the codec immediately without evaluation

B. Research the codec's maturity, ecosystem support, interoperability, and long-term adoption prospects

C. Reject all emerging technologies

D. Use only legacy codecs

67. A client is integrating a cloud-based AI transcription service with their conferencing system. The most appropriate consideration is:

A. Deploy without privacy review

B. Enable the service unconditionally

C. Use consumer-grade transcription

D. Evaluate privacy, data residency, and regulatory implications; ensure compliance with applicable requirements

68. A CTS holder is reviewing a proposed cloud-based AV management platform deployment. The most important consideration is:

A. The platform's data residency, security posture, SLAs, integration capabilities, and long-term commitments

B. The platform's marketing

C. The platform's office location

D. The platform's CEO personality

69. A CTS holder is troubleshooting a Teams Room deployment where meetings occasionally fail to start. The Teams service is operational. The most likely cause is:

A. The Teams service has failed

B. Endpoint-specific issues with certified hardware, authentication, network, or local configuration

C. All endpoints globally have failed

D. The display has failed

70. An AV-over-IP encoder has firmware that was recently updated. Since the update, it has become unreliable. The most appropriate response is:

A. Continue using the unreliable firmware

B. Replace the encoder hardware

C. Review the firmware update notes, consider rollback or subsequent update, and coordinate with the manufacturer

D. Accept the unreliability as a characteristic

71. A client has asked about modern videoconferencing interoperability. The most accurate response is:

A. Modern systems typically use either proprietary platforms or standards-based systems (SIP, H.323), with varying interoperability

B. All videoconferencing systems are identical

C. Videoconferencing does not require interoperability

D. Interoperability is only a consumer feature

72. A CTS holder is implementing log collection from AV devices. The most appropriate approach is:

A. Configure log collection per retention policy, secure transport, appropriate access controls, and integration with the client's SIEM if applicable

B. Store logs on each device only

C. Disable logging

D. Share logs publicly

73. A CTS holder has been asked about the relevance of SMPTE 2110 to professional AV. The most accurate response is:

A. SMPTE 2110 is consumer-only

B. SMPTE 2110 is irrelevant to modern AV

C. SMPTE 2110 defines IP-based video, audio, and ancillary data transport, relevant to broadcast and emerging professional AV

D. SMPTE 2110 is a consumer streaming format

74. A CTS holder is deploying a new AV installation with emphasis on manageability. The most appropriate consideration is:

A. The aesthetic manageability of the installation

B. A comprehensive management strategy including monitoring, updates, backup, access control, and incident response

C. Disable all management

D. Use only verbal coordination

75. A cloud-based conferencing platform has changed its endpoint certification requirements. The most appropriate response is:

A. Ignore the changes

B. Immediately replace all endpoints

C. Review the changes and plan appropriate updates to equipment or configurations per the new requirements

D. Disable the platform

76. A CTS holder is evaluating a wireless BYOD presentation system. The most important security consideration is:

A. The system's aesthetic

B. The system's color

C. The system's prestige

D. Authentication, encryption, and network isolation to prevent unauthorized access or interference

77. A CTS holder is reviewing a proposed AV installation for disaster recovery. The most important consideration is:

A. Ignore DR

B. Understand the client's business continuity requirements and design backup procedures, failover capabilities, and documentation aligned with those requirements

C. Use lowest-cost equipment

D. Use only a single manufacturer

78. A CTS holder is configuring API-based integration with a client's enterprise application. The most appropriate approach is:

A. Use the vendor's published API with appropriate authentication, error handling, and ongoing monitoring

B. Reverse-engineer the API

C. Use undocumented methods

D. Abandon the integration

79. A CTS holder has received a vulnerability disclosure from an AV equipment manufacturer. The most appropriate response is:

A. Ignore the disclosure

B. Share the vulnerability publicly

C. Review the specific vulnerability, assess impact on the installation, apply the recommended patches or mitigations in coordination with client security

D. Delay response indefinitely

80. A client has asked about the relationship between AV-over-IP and traditional SDI. The most accurate response is:

A. SDI and AV-over-IP are identical

B. AV-over-IP has replaced SDI entirely

C. SDI is obsolete

D. SDI is an established broadcast interface; AV-over-IP is a network-based alternative with different infrastructure requirements and tradeoffs

81. A CTS holder is deploying a system with cloud-based meeting room scheduling. The most appropriate consideration is:

A. The scheduling platform's mascot

B. The scheduling platform's integration with the client's calendar system, reliability, and synchronization characteristics

C. The scheduling platform's aesthetic

D. The scheduling platform's location

82. A CTS holder is troubleshooting a Microsoft Teams Room where camera framing automation has failed. The room is currently working without the automation. The most appropriate response is:

A. Investigate the automation configuration and sensor functionality, coordinate with manufacturer if needed, and plan remediation

B. Accept the manual operation indefinitely

C. Replace the entire Teams Room

D. Disable all automation permanently

83. A client has deployed remote worker endpoints that integrate with the office AV system. The most important deployment consideration is:

A. Consumer-grade security

B. Default credentials

C. No authentication

D. Remote worker endpoint security, authentication, and integration with the client's enterprise security policies

84. A CTS holder is evaluating an emerging real-time collaboration platform. The most appropriate approach is:

A. Deploy without evaluation

B. Ignore emerging platforms entirely

C. Research the platform's maturity, security, integration options, support, and alignment with the client's requirements

D. Use only a single-vendor approach

85. A CTS holder is integrating with a client's cloud-based phone system. The most appropriate consideration is:

A. Use only on-premises phone systems

B. Coordinate with the cloud phone system vendor and client for appropriate endpoint certification, configuration, and integration

C. Bypass the phone system

D. Use consumer VoIP

86. A CTS holder is reviewing a proposed deployment with heavy cloud service dependency. The most important consideration is:

A. Cloud services are always more reliable

B. Cloud services are always less reliable

C. All cloud services are identical

D. Understand cloud SLAs, failure modes, network dependency, and design appropriate fallback capabilities for mission-critical applications

87. A CTS holder is reviewing security controls for a new AV deployment. The most appropriate approach is:

A. Apply a layered security model including network, device, identity, and operational controls aligned with the client's security posture

B. Use only network security

C. Rely only on default manufacturer settings

D. Disable security

88. A client is integrating AV with an enterprise resource planning (ERP) system for operational data flow. The most appropriate approach is:

A. Develop the integration without ERP team involvement

B. Use a consumer-grade workaround

C. Coordinate with the ERP vendor and client ERP team to use supported integration methods, authentication, and appropriate data flow

D. Bypass ERP integration

89. A CTS holder is implementing a new AV-over-IP architecture. The most important switch capability beyond basic Ethernet is:

A. Consumer-grade switches without management

B. Managed switches with IGMP snooping, Quality of Service, appropriate bandwidth, and PoE where required

C. Unmanaged switches only

D. Wireless switches

90. A CTS holder has been asked about zero-day vulnerabilities in AV equipment. The most appropriate response is:

A. Ignore vulnerabilities

B. Deny vulnerabilities exist

C. Maintain awareness of vendor disclosures, monitor for patches, apply timely updates, and maintain defense-in-depth security practices

D. Share vulnerabilities publicly

91. A CTS holder is deploying a cloud-managed device monitoring platform. The most important configuration consideration is:

A. Maximum verbosity

B. No monitoring

C. Appropriate monitoring scope, privacy alignment, secure data transport, and actionable alert configuration

D. Monitoring without alerts

92. A client has asked about NDI for video over IP. The most accurate description is:

A. NDI is identical to SDI

B. NDI (Network Device Interface) is a protocol for video over IP primarily used in broadcast and production, with specific network requirements

C. NDI is only for consumer applications

D. NDI is a cable standard

93. A CTS holder is reviewing a proposed cloud-based conferencing deployment with specific data residency requirements. The most appropriate response is:

A. Ignore the requirement

B. Use any cloud provider

C. Deploy without coordination

D. Coordinate with the conferencing platform and client to confirm data residency, regional routing, and compliance with applicable regulations

94. A CTS holder is integrating with a client's existing single sign-on (SSO) environment. The most appropriate approach is:

A. Bypass SSO with local credentials

B. Implement SSO using the client's supported protocols and coordinate with identity management

C. Use shared passwords across devices

D. Disable authentication

95. A CTS holder is troubleshooting a Zoom Rooms deployment where sign-in has failed. The most likely cause is:

A. The room has lost power

B. Authentication issues, account configuration, or network access to Zoom sign-in services

C. The room's ceiling has shifted

D. The display has failed

96. An AV-over-IP stream experiences banding at specific color transitions in the video. The most likely cause is:

A. Insufficient compression bit depth or color space conversion

B. The display has failed

C. The amplifier has degraded

D. The DSP has reached end-of-life

97. A CTS holder has been asked about the differences between Zoom, Microsoft Teams, and Google Meet for AV integration. The most accurate response is:

A. All three are identical in AV integration

B. The platforms have similar goals but differ significantly in endpoint certification, integration APIs, room management, and admin capabilities

C. Only Microsoft Teams has professional features

D. Only Zoom is used in AV installations

98. A CTS holder is implementing remote troubleshooting capabilities for an installed system. The most appropriate approach is:

A. Use consumer remote-access tools bypassing enterprise security

B. Disable all remote access

C. Use default credentials

D. Implement remote troubleshooting through the client's approved VPN and authentication methods with appropriate logging

99. A CTS holder is asked to evaluate an emerging spatial audio technology for a conference room. The most appropriate approach is:

A. Adopt the technology without evaluation

B. Reject all emerging technologies

C. Research the technology's maturity, compatibility, integration requirements, and actual benefit for the client's use case

D. Use only legacy audio

100. A CTS holder is evaluating a cloud-based AV analytics platform. The most important consideration is:

A. The platform's branding

B. The platform's employee count

C. The platform's security practices, data privacy, integration capabilities, and actionable insight quality

D. The platform's CEO personality

SIMULATION EXAM 11 — ANSWER KEY AND FULL EXPLANATIONS

1. D — Microsoft's official Teams Rooms certification documentation is authoritative and current for certified hardware, deployment requirements, and admin portal configuration. AVIXA materials, manufacturer marketing, and online forums lack the platform-specific authority that Microsoft's own documentation provides. Relying on the vendor's source ensures the integration meets current certification requirements.

2. C — Visually lossless compressed 4K at approximately 800 Mbps. A 1 GbE network cannot support uncompressed 4K60 4:4:4 (12 Gbps) or 8K bandwidth, but easily accommodates visually lossless compressed 4K streams in the 800 Mbps range. Matching stream bandwidth to network capacity is fundamental to reliable AV-over-IP deployment.

3. B — Zoom Rooms is a cloud-based meeting service with certified in-room devices. The meeting intelligence and routing occur in Zoom's cloud infrastructure, while certified room hardware connects to it. Understanding this architecture is essential for deployment, network planning, and troubleshooting.

4. A — Change all default administrative passwords to strong, unique credentials. Default credentials are the most common attack vector for networked AV devices, as they're publicly documented by manufacturers. Unique strong passwords per device are the foundational cybersecurity baseline.

5. D — IPMX is an open standards-based framework built on SMPTE 2110 technologies. It's designed to bring broadcast-quality IP transport to professional AV applications, with an alliance of industry players supporting open adoption. Understanding its architectural basis distinguishes it from proprietary alternatives.

6. B — SDVoE is an alliance-defined AV-over-IP technology using 10 Gigabit Ethernet for uncompressed transport. The 10 GbE infrastructure enables uncompressed 4K with ultra-low latency, suitable for applications where compression artifacts are unacceptable. This bandwidth requirement is a key differentiator from 1 GbE compressed solutions.

7. A — In-room camera, microphone, and loudspeaker connectable to user devices via USB-C. Modern BYOD architecture keeps the conferencing software with the user's device while providing professional-grade in-room peripherals through a single USB-C connection. This balances user flexibility with in-room audio/video quality.

8. C — The control system's reliability, authentication, API stability, and support commitments. Cloud-based control systems introduce dependencies on vendor infrastructure and policies,

making these ongoing service considerations critical. Aesthetic, marketing, and prestige are not substantive selection criteria.

9. B — Dante is a proprietary audio-over-IP protocol from Audinate; AES67 is an open interoperability standard that enables communication between different audio-over-IP systems. Dante can be AES67-compliant, allowing interoperability. This distinction matters for multi-vendor deployments.

10. D — The software's reliability, update cadence, security practices, and support availability. Software-based DSPs run on general-purpose hardware, so the software vendor's practices directly determine long-term reliability and security. Aesthetic and marketing considerations are irrelevant to operational outcomes.

11. A — Verify that all AV devices support TLS 1.2+ before deployment and coordinate with IT for implementation. TLS 1.2+ is the current enterprise security minimum; older versions have known vulnerabilities. Verification before deployment prevents post-installation retrofits or non-compliance findings.

12. C — Client-side network, firewall, or authentication changes are affecting the specific installation. When the cloud platform reports normal operations but the installation has issues, the fault is on the client side — the service is working for everyone else, so the difference must be local. This diagnostic logic is fundamental for cloud-integrated systems.

13. D — Gigabit Ethernet-based multicast with appropriate QoS and IGMP snooping. Visually lossless compressed 4K at approximately 800 Mbps is the typical profile for 1 GbE-based AV-over-IP systems. QoS and IGMP snooping are essential for reliable multicast delivery on shared networks.

14. A — Use unique credentials managed through a centralized credential management platform. Centralized management enables rotation, revocation, audit, and enforcement of credential policies. Hard-coded, shared, or plaintext credentials all fail enterprise security standards.

15. C — Review codec compatibility and adjust DSP or codec settings to accommodate the new platform behavior. Platform-side audio codec changes often require endpoint configuration adjustments to maintain optimal performance. Hardware replacement or platform avoidance are disproportionate responses.

16. B — Implement SSO or SAML integration per the identity management system's supported protocols. Enterprise identity management integration uses established protocols like SAML 2.0 or OAuth 2.0, matched to what the client's system supports. Shared passwords and local-only authentication violate enterprise security standards.

17. B — Cables certified for USB-C with power, video, and data at the required specifications. USB-C cables vary significantly in capabilities; BYOD applications require cables certified for full power delivery, video transport, and data simultaneously. Uncertified cables produce unreliable behavior at modern bandwidths.

18. D — The platform's security practices, uptime SLAs, integration options, and long-term support commitment. Cloud platform selection involves operational dependencies that persist for years, requiring due diligence on security, reliability, and vendor longevity. Branding factors are not substantive.

19. A — Latency varies by compression, network configuration, and codec; typical uncompressed systems have very low latency, while compressed systems have higher but still acceptable levels. Understanding the tradeoff between compression and latency guides architecture decisions for specific use cases. Categorical statements about latency misrepresent the technology's characteristics.

20. C — *Correction noted:* The keyed answer C ("Disable network security for AV") does not reflect current professional practice. The correct answer based on content is **B — Use VLAN segmentation with appropriate QoS configuration, coordinated with IT**. VLAN-based segmentation with QoS is the professional approach that balances AV performance requirements with enterprise security. This should be corrected in editorial review before publication.

21. B — The installed endpoints must be certified and configured for the client's Teams Direct Routing environment. Direct Routing has specific requirements for SBC integration, endpoint certification, and admin configuration. Consumer-grade VoIP or bypass approaches fail the certification requirements.

22. A — HDMI 2.0 supports up to 18 Gbps; HDMI 2.1 supports up to 48 Gbps, enabling 8K60 and higher refresh rates. The bandwidth jump between versions is significant, driving cable selection and display compatibility decisions. Understanding these limits is essential for 4K and 8K deployments.

23. D — Security policy updates are disrupting authentication tokens or blocking required ports. When disconnections correlate with IT security policy timing, the policy changes are the disruption source. Firmware, cabling, and display issues don't correlate with security policy events.

24. C — The platform's API documentation, authentication methods, and webhook capabilities for integration. Cloud booking platform integration depends on technical capabilities exposed through APIs and webhooks. Marketing materials and organizational trivia don't enable integration.

25. B — *Correction noted:* The keyed answer B ("On-premises is always better than cloud") is too absolute and doesn't reflect professional nuance. The correct answer based on content is **D — The choice depends on the client's security posture, operational model, and data residency requirements**. Professional practice evaluates specific client requirements rather than making categorical statements. This should be corrected in editorial review before publication.

26. B — Ensure telemetry collection aligns with the client's privacy and data protection policies. Telemetry can include sensitive operational data; collection must comply with the client's

governance policies. Maximum or covert collection violates privacy principles; disabled telemetry eliminates valuable operational insight.

27. A — OAuth is a delegated authentication framework where the device can access calendar data without storing user credentials directly. This token-based approach is more secure than credential storage and is standard across modern cloud integrations. Understanding OAuth is essential for calendar-integrated conferencing devices.

28. D — Implement certificates issued through the client's certificate authority with appropriate lifecycle management. Enterprise certificate deployment uses the client's CA with proper enrollment, renewal, and revocation processes. Self-signed, shared, or disabled validation approaches fail enterprise security requirements.

29. C — Coordinate with IT to open the specific ports required while maintaining security posture. Service-specific port requirements should be opened precisely, not wholesale. Ignoring or bypassing firewall requirements violates IT governance and creates security gaps.

30. B — Patch management, secure configuration baselines, authentication practices, and network segmentation. Networked AV equipment cybersecurity requires multiple dimensions working together — no single control is sufficient. Price, aesthetic, and manufacturer tier don't reflect security posture.

31. A — Codec-internal video processing is producing latency. When the network is verified stable but video latency persists, the issue is in the codec's processing pipeline itself — encoding, scaling, or compression stages. Microphones, display age, and cable length don't produce this pattern.

32. D — Feature sets, certified devices, admin capabilities, SLAs, and integration options. Platform selection is multi-dimensional, balancing technical capabilities, operational support, and integration. Logo, founding date, and billing cycle are not substantive selection criteria.

33. C — Implement appropriate audit logging with retention policy aligned with compliance requirements. Compliance-driven logging has specific scope, retention, and storage requirements. Disabled logging fails compliance; maximum verbosity creates management burden; local-only storage fails audit requirements.

34. B — Evaluate the specific use case, required bandwidth (typically 48+ Gbps uncompressed), display availability, and content considerations. 8K deployment is context-dependent — appropriate for specific high-detail applications, excessive for many others. Blanket deployment or rejection both fail the professional evaluation standard.

35. A — Coordinate with IT security to implement remote access using approved methods including VPN and multi-factor authentication. Remote management must operate within the client's security framework. Consumer tools, categorical refusal, or default credentials all fail one or both of the operational and security requirements.

36. C — Network switch backplane or uplink is approaching saturation. When switch configuration appears correct but encoders drop from multicast streams, bandwidth saturation at the switch's backplane or uplink is a common cause. Individual device failures produce different patterns.

37. D — IGMP snooping and appropriate QoS on a managed switch. Multicast AV-over-IP requires IGMP snooping to prevent multicast flooding, plus QoS to prioritize time-sensitive traffic. Wireless, consumer switches, or fiber-direct approaches miss these requirements.

38. A — Develop a replacement plan with the client including timeline, budget, and replacement equipment selection. End-of-support is a predictable transition requiring proactive planning rather than indefinite continuation, immediate removal, or unauthorized support arrangements.

39. B — Design for reliable remote access with secure VPN, appropriate monitoring, and tools for remote troubleshooting. Remote worker integration requires designing for distributed access with appropriate security. Physical-only security, ignoring remote workers, or requiring on-site presence all fail modern hybrid work requirements.

40. D — IoT integration uses MQTT, REST APIs, or similar protocols with appropriate security controls. Modern IoT relies on well-defined protocols with authentication, encryption, and authorization. Wireless-only or co-location requirements misrepresent current IoT capabilities.

41. C — The choice depends on latency requirements, network reliability, security, and the specific use case. Cloud DSPs and hardware DSPs each have strengths — cloud offers flexibility and centralized updates, hardware offers deterministic latency. Professional evaluation matches technology to use case.

42. A — Ensure the monitoring configuration aligns with the client's privacy and data governance policies. Monitoring data may include sensitive information requiring governance alignment. Maximum collection without policy consideration or covert collection violate privacy principles.

43. B — Research the AI camera's capabilities, integration options, security controls, and operational lifecycle, then plan accordingly. Emerging AI-enabled equipment requires professional due diligence rather than blind deployment, categorical rejection, or treating as equivalent to legacy equipment.

44. D — *Correction noted:* The keyed answer D ("Good network infrastructure") describes a state, not a cause of failures. The correct answer based on content is **C — Device firmware issues, network switch backplane saturation, or endpoint-specific faults**. When network QoS is verified but streams fail intermittently, the fault is elsewhere in the ecosystem. This should be corrected in editorial review before publication.

45. C — Certified hardware selection, network configuration, and proper account and room setup in the Zoom admin portal. Zoom Rooms deployment requires certified hardware integrated with Zoom's admin portal for room creation and management. Aesthetic and branding considerations don't drive functional outcomes.

46. A — Cloud platforms typically provide redundant data center architecture; the client's redundancy strategy should address network path diversity and failover procedures. Platform providers handle infrastructure redundancy; client-side redundancy addresses the last-mile connectivity. Categorical statements about cloud reliability misrepresent the architecture.

47. C — The endpoint's codec compatibility, encoding quality, latency, and manufacturer support. AV-over-IP endpoint evaluation is multi-dimensional — technical capabilities, performance, and long-term support. Color, brand prestige, or price alone miss critical dimensions.

48. B — Coordinate with the client on a firmware management strategy that balances security updates with operational stability, with appropriate testing and staging. Automatic updates without governance create risk; disabled updates create security gaps. The professional approach balances both concerns through managed processes.

49. D — Enterprise SSO enables users to authenticate to AV services using their existing enterprise credentials, typically via SAML or OAuth. This eliminates separate AV credentials while maintaining enterprise security controls. Limiting SSO to desktop or consumer use misrepresents its enterprise application.

50. A — Configure monitoring for proactive alerting on critical issues, with appropriate granularity of monitored metrics and alert routing. Effective centralized monitoring detects issues before users report them, with appropriate metrics and routing. Disabled alerts eliminate the value; single-room monitoring doesn't serve multi-room deployments.

51. A — A comprehensive approach including patch management, secure configuration, authentication, network segmentation, and incident response. Cybersecurity requires multiple mutually reinforcing controls; no single dimension is sufficient. Appearance, age, and price don't reflect security posture.

52. D — Plan and execute migration to the new API version before the deprecation date. API versioning requires proactive migration to maintain integration continuity. Ignoring, replacing hardware, or disabling integration are disproportionate or failure-creating responses.

53. B — LDAP or similar directory protocols that support enterprise directory integration. Enterprise directory integration uses established protocols like LDAP, Active Directory, or related standards. File access and consumer alternatives don't meet enterprise authentication requirements.

54. C — Modern authentication refers to current authentication practices like OAuth 2.0, SAML, and multi-factor authentication. This terminology distinguishes current secure practices from legacy authentication like basic password over unencrypted transport. Understanding the term is essential for enterprise integration discussions.

55. A — The platform's certifications (SOC 2, ISO 27001) and specific compliance with applicable regulations like HIPAA, GDPR, PCI. Regulated industries require specific platform compliance

evidence, documented through certifications and regulatory attestations. Logo, location, and leadership are not compliance evidence.

56. D — Implement proper token management including secure storage, rotation, and revocation. OAuth 2.0 tokens require appropriate lifecycle management to maintain security. Hard-coded, shared, or non-expiring tokens all violate security principles.

57. B — Work with IT to design AV integration that aligns with zero-trust principles including identity verification, network segmentation, and continuous authentication. Zero-trust architecture applies to all networked devices including AV. Bypassing, default credentials, or isolated legacy approaches all violate the zero-trust framework.

58. A — QoS is not configured to prioritize Dante traffic. Clicks during general network traffic indicate time-sensitive audio packets being delayed by other traffic. QoS configuration prioritizes audio over general traffic on shared networks.

59. C — Equipment, installation, network infrastructure, cloud subscriptions, maintenance, support, and lifecycle replacement. TCO for modern AV includes ongoing cloud subscriptions and lifecycle replacement costs that weren't major factors in legacy systems. Single-category cost analysis misses critical lifecycle dimensions.

60. D — Implement comprehensive audit logging with appropriate retention and secure storage. Administrative action logging requires comprehensive capture, defined retention, and secure storage to serve compliance and audit needs. Disabled, local-only, or failure-only logging don't meet these requirements.

61. A — Review the vendor's security certifications, incident history, vulnerability disclosure process, and product security practices. Vendor security evaluation examines multiple dimensions of security posture. Pricing, brand recognition, and marketing claims don't reflect security practices.

62. A — Client-side network, authentication, or configuration issues affecting the specific installation. When the cloud service reports normal operations, the issue is local. This diagnostic principle applies to all cloud-integrated systems and avoids misdirected troubleshooting effort.

63. C — Select certified devices and configure them per Google Meet's deployment requirements, including Google Workspace admin integration. Google Meet has specific certification requirements and integration with Workspace admin. Bypassing or using alternative platforms fails the client's specified environment.

64. B — Coordinate with the MDM administrator to ensure any AV-integrated mobile devices or tablets comply with the MDM policies. Enterprise MDM governs mobile device configuration across the organization; AV-integrated devices must comply. Bypassing MDM controls violates enterprise governance.

65. A — Use enterprise NTP servers configured by IT with appropriate time zones and synchronization monitoring. Enterprise NTP ensures consistent, authenticated time sources across the organization. Consumer NTP, disabled synchronization, or manual time-setting all create time drift and coordination problems.

66. B — Research the codec's maturity, ecosystem support, interoperability, and long-term adoption prospects. Emerging codec evaluation requires professional due diligence considering both current capabilities and future viability. Immediate adoption or categorical rejection both fail the evaluation standard.

67. D — Evaluate privacy, data residency, and regulatory implications; ensure compliance with applicable requirements. AI transcription processes sensitive conversation content with significant privacy implications. Unconditional enablement or consumer-grade alternatives fail the compliance requirements.

68. A — The platform's data residency, security posture, SLAs, integration capabilities, and long-term commitments. Cloud platform deployment decisions have long-term operational and compliance implications requiring thorough evaluation. Marketing and leadership are not substantive criteria.

69. B — Endpoint-specific issues with certified hardware, authentication, network, or local configuration. When the Teams service operates normally, failure at a specific endpoint is localized to that endpoint's environment. Global service or categorical failures would produce different patterns.

70. C — Review the firmware update notes, consider rollback or subsequent update, and coordinate with the manufacturer. Post-update reliability issues are addressed through structured response — review, potential rollback, manufacturer coordination. Continuing unreliable operation or wholesale hardware replacement are disproportionate.

71. A — Modern systems typically use either proprietary platforms or standards-based systems (SIP, H.323), with varying interoperability. Understanding this landscape guides integration decisions for mixed environments. Categorical statements misrepresent the diversity of current systems.

72. D — *Correction noted:* The keyed answer D ("Share logs publicly") violates security principles and is clearly incorrect. The correct answer based on content is **A — Configure log collection per retention policy, secure transport, appropriate access controls, and integration with the client's SIEM if applicable**. Log management requires appropriate governance and security controls. This should be corrected in editorial review before publication.

73. C — SMPTE 2110 defines IP-based video, audio, and ancillary data transport, relevant to broadcast and emerging professional AV. The standard underlies IPMX and similar emerging frameworks. Dismissing it as consumer or irrelevant misrepresents its growing importance in professional AV.

74. B — A comprehensive management strategy including monitoring, updates, backup, access control, and incident response. Modern AV manageability requires systematic approach across multiple dimensions. Disabling management or relying on verbal coordination fails the scale and complexity of modern deployments.

75. C — Review the changes and plan appropriate updates to equipment or configurations per the new requirements. Platform certification changes require structured response balancing compliance with operational impact. Ignoring changes creates future compliance gaps; immediate replacement is disproportionate.

76. D — Authentication, encryption, and network isolation to prevent unauthorized access or interference. Wireless BYOD security requires multiple layers — authentication for device identity, encryption for content protection, and network isolation to limit lateral movement. Aesthetic and branding considerations don't provide security.

77. B — Understand the client's business continuity requirements and design backup procedures, failover capabilities, and documentation aligned with those requirements. DR design is client-specific, matching capabilities to business needs. Ignoring DR or using default equipment doesn't address specific continuity requirements.

78. A — Use the vendor's published API with appropriate authentication, error handling, and ongoing monitoring. Published APIs are supported integration paths with defined contracts and security models. Reverse-engineering or undocumented methods create fragile integrations.

79. C — Review the specific vulnerability, assess impact on the installation, apply the recommended patches or mitigations in coordination with client security. Vulnerability disclosures require structured response — assessment, coordination, and remediation. Ignoring, public disclosure, or indefinite delay all fail the professional response.

80. D — SDI is an established broadcast interface; AV-over-IP is a network-based alternative with different infrastructure requirements and tradeoffs. Both have ongoing roles in their respective applications; neither is obsolete. Understanding the tradeoffs guides appropriate selection for specific use cases.

81. B — The scheduling platform's integration with the client's calendar system, reliability, and synchronization characteristics. Room scheduling value depends on accurate calendar integration and reliable synchronization. Branding, aesthetic, and location are not operational criteria.

82. A — Investigate the automation configuration and sensor functionality, coordinate with manufacturer if needed, and plan remediation. Automation failures require structured diagnostic response — config review, sensor check, manufacturer engagement. Accepting the failure or wholesale replacement are disproportionate responses.

83. D — Remote worker endpoint security, authentication, and integration with the client's enterprise security policies. Remote endpoints extend the enterprise security boundary and must comply with

enterprise policies. Consumer-grade security, default credentials, or no authentication all create vulnerabilities.

84. C — Research the platform's maturity, security, integration options, support, and alignment with the client's requirements. Emerging platform evaluation requires professional due diligence matching platform capabilities to client needs. Immediate deployment, categorical rejection, or single-vendor approaches all fail the evaluation standard.

85. B — Coordinate with the cloud phone system vendor and client for appropriate endpoint certification, configuration, and integration. Cloud phone integration requires coordination with the platform vendor for certified endpoints and proper configuration. On-premises-only or consumer alternatives don't meet the client's specified architecture.

86. D — Understand cloud SLAs, failure modes, network dependency, and design appropriate fallback capabilities for mission-critical applications. Heavy cloud dependency creates specific risk profiles requiring appropriate mitigation for critical applications. Categorical reliability statements misrepresent the varied reality.

87. A — Apply a layered security model including network, device, identity, and operational controls aligned with the client's security posture. Defense-in-depth is the foundational security architecture principle, with multiple controls working together. Single-dimension security or defaults leave gaps; disabled security is untenable.

88. C — Coordinate with the ERP vendor and client ERP team to use supported integration methods, authentication, and appropriate data flow. ERP integration requires coordination with the ERP team and use of supported integration paths. Bypassing or consumer-grade workarounds create unsustainable integrations.

89. D — Managed switches with IGMP snooping, Quality of Service, appropriate bandwidth, and PoE where required. AV-over-IP architecture requires switch capabilities beyond basic Ethernet — multicast handling, traffic prioritization, and power delivery. Consumer or unmanaged switches lack the necessary capabilities.

90. A — *Correction noted:* The keyed answer A ("Ignore vulnerabilities") is professionally unsound and clearly incorrect. The correct answer based on content is **C — Maintain awareness of vendor disclosures, monitor for patches, apply timely updates, and maintain defense-in-depth security practices**. Zero-day vulnerabilities require active awareness and layered defenses. This should be corrected in editorial review before publication.

91. C — Appropriate monitoring scope, privacy alignment, secure data transport, and actionable alert configuration. Cloud monitoring platforms require balanced configuration that serves operational needs while respecting governance. Maximum verbosity, no monitoring, or alerts-less monitoring all fail the professional standard.

92. B — NDI (Network Device Interface) is a protocol for video over IP primarily used in broadcast and production, with specific network requirements. Understanding NDI's scope helps guide deployment decisions for live production applications. Consumer or cable-standard characterizations misrepresent its technical role.

93. D — Coordinate with the conferencing platform and client to confirm data residency, regional routing, and compliance with applicable regulations. Data residency requirements drive platform selection, regional deployment, and compliance documentation. Ignoring the requirement or deploying without coordination creates compliance exposure.

94. A — *Correction noted:* The keyed answer A ("Bypass SSO with local credentials") violates enterprise security principles. The correct answer based on content is **B — Implement SSO using the client's supported protocols and coordinate with identity management**. Enterprise SSO integration should align with the client's identity management infrastructure. This should be corrected in editorial review before publication.

95. B — Authentication issues, account configuration, or network access to Zoom sign-in services. Zoom Rooms sign-in failures localize to authentication or network access to Zoom's sign-in infrastructure. Power, physical environment, or display issues produce different symptom patterns.

96. C — Insufficient compression bit depth or color space conversion. Banding in AV-over-IP streams typically originates in the encoding pipeline — insufficient bit depth or poor color space handling. Display, amplifier, and DSP issues produce different symptom patterns.

97. B — The platforms have similar goals but differ significantly in endpoint certification, integration APIs, room management, and admin capabilities. Understanding these differences guides platform-specific deployment decisions. Categorical equivalence or exclusion misrepresents the distinct platforms.

98. D — Implement remote troubleshooting through the client's approved VPN and authentication methods with appropriate logging. Remote troubleshooting must operate within enterprise security frameworks with appropriate auditability. Consumer tools, disabled access, or default credentials all fail enterprise standards.

99. C — Research the technology's maturity, compatibility, integration requirements, and actual benefit for the client's use case. Emerging technology evaluation requires professional due diligence matching capabilities to client needs. Immediate adoption or categorical rejection both fail the evaluation standard.

100. C — The platform's security practices, data privacy, integration capabilities, and actionable insight quality. Cloud analytics platform evaluation is multi-dimensional, with security and actionable insight being the most important factors. Branding, organizational size, and leadership personality are not substantive criteria.