HIMSS Analytics® INFRAM

The HIMSS Analytics Infrastructure Adoption Model (INFRAM) helps healthcare organizations improve care delivery, reduce cyber and infrastructure risk, and create a pathway for infrastructure development tied to business and clinical outcomes.

STAGE	HIMSS Analytics® INFRAM Infrastructure Adoption Model Cumulative Capabilities
7	Adaptive and flexible network control with software defined networking; home-based tele-monitoring; internet/TV on demand
6	Software defined network automated validation of experience; on-premise enterprise/hybrid cloud application and infrastructure automation
5	Video on mobile devices; location-based messaging; firewall with advanced malware protection; real-time scanning of hyperlinks in email messages
4	Multiparty video capabilities; wireless coverage throughout most premises; active/active high availability; remote access VPN
3	Advanced intrusion prevention system; rack/tower/blade server-based compute architecture; end-to-end QoS; defined public and private cloud strategy
2	Intrusion detection/prevention; informal security policy; disparate systems centrally managed by multiple network management systems
1	Static network configurations; fixed switch platform; active/standby failover; LWAP-only single wireless controller; ad-hoc local storage networking; no data center automation
0	No VPN, intrusion detection/prevention, security policy, data center or compute architecture

The stages of the model are as follows:

Stage 7

The organization's data, voice, and location grade exceeds 81 percent for all internal areas, and has achieved data, voice and location grade for all specified external on-campus areas. 802.11x passive and active wireless surveys have been conducted for all internal locations and specified external on-campus location-grade areas. A high-availability wireless identity and access management solution and a high-availability wireless enterprise mobile management solution are implemented on-premise and in the cloud. The organization has well-defined bring-your-own-device network access policies for both staff-owned and guest-owned devices that are managed through the enterprise mobile management solution with software defined network policy enforcement. Identity, access, and mobile device management solutions integration use the software defined networking controller to provide advanced security and automated access policy enforcement.

Stage 6

The organization has implemented a campus software defined networking access capability using a campus software defined controller that supports API integration with provisioning. There is also a software defined network with automated validation of experience based on defined policies. Traffic loads are manipulated dynamically based on policy compliance monitoring. There is end-to-end visibility of service delivery in real-time. There is on-premise enterprise-wide hybrid cloud application and infrastructure automation that is API driven using an automation tool on virtualized and non-virtualized platforms (application, network, compute or storage). There is also a self-service portal for IT use-cases.

Stage 5

The organization's network infrastructure using micro virtual segmentation in the campus infrastructure is now based on virtual extensible local area network. The organization is defining its network quality of service policies based on its quality of experience requirements. The local and wide area networks are advanced with quality of service performance monitoring for policy compliance using a software defined network controller for end-to-end quality of service policies across platforms. Its software defined networking is based on a single physically-centralized controller design with a static architecture based on unchangeable links and controller positions logically centralized with either a flat or hierarchical architecture. In addition to its dual on-premise wireless controllers, an on-premise wireless controller is now reserved for software defined networking access in a mixed mode.

Stage 4

The organization's network infrastructure uses macro virtual segmentation based on virtual local area network trunking protocol propagation and virtual routing and forwarding. There is a well-defined and automated configuration of access port policy in place utilizing automated configuration tools. However, campus software defined networking access has not yet been implemented. The campus network and the wide area network is fully redundant and designed to recover very quickly with no or limited downtime. The dual on-premise wireless controllers with access point and client stateful switchover now supports lightweight access points with cloud-capable redundancy groups.

HIMSS Analytics® INFRAM

The HIMSS Analytics Infrastructure Adoption Model (INFRAM) helps healthcare organizations improve care delivery, reduce cyber and infrastructure risk, and create a pathway for infrastructure development tied to business and clinical outcomes.

STAGE	HIMSS Analytics® INFRAM Infrastructure Adoption Model Cumulative Capabilities
7	Adaptive and flexible network control with software defined networking; home-based tele-monitoring; internet/TV on demand
6	Software defined network automated validation of experience; on-premise enterprise/hybrid cloud application and infrastructure automation
5	Video on mobile devices; location-based messaging; firewall with advanced malware protection; real-time scanning of hyperlinks in email messages
4	Multiparty video capabilities; wireless coverage throughout most premises; active/active high availability; remote access VPN
3	Advanced intrusion prevention system; rack/tower/blade server-based compute architecture; end-to-end QoS; defined public and private cloud strategy
2	Intrusion detection/prevention; informal security policy; disparate systems centrally managed by multiple network management systems
1	Static network configurations; fixed switch platform; active/standby failover; LWAP-only single wireless controller; ad-hoc local storage networking; no data center automation
0	No VPN, intrusion detection/prevention, security policy, data center or compute architecture

Stage 3

The organization has decreased the number of devices at the end of their support to less than 3 percent for core and distribution layer technologies and less than 10 percent for its access layer technologies. It has increased its modular and scalable network design to between 41 and 70 percent of network switches. It has also implemented an active/active failover procedure for its network core and distribution layer and the network is fully redundant and designed to recover very quickly with no or limited downtime. The network design includes dual on-premise wireless controllers with access point and client stateful switchover but supporting only lightweight access points. It has implemented a predominantly IP Telephony environment with IP Telephony exceeding 90 percent of the network and an analog/digital PBX used for less than 10 percent.

Stage 2

The organization begins to demonstrate a well-defined, but manually-configured access port policy. It has implemented a modular and scalable network design, but only for less than 40 percent of network switches. The organization has reduced to 20 percent the number of access layer technologies that have reached an end of support status. The network is fully redundant, but retains an active/standby configuration that may introduce system delays in network failure recovery. Data and voice grade exceeds 80 percent and location grade for specific areas, but the data and voice grade for other areas is less than 80 percent with no location grade. The organization has completed an 802.11x passive wireless survey for entire location and an 802.11x active wireless survey internally. Location grade is specified for certain areas only. Network design is based on a single on-premise wireless controller that only supports lightweight access points. The organization has implemented a hybrid IP telephony and analog/digital PBX environment. The organization has implemented some basic information assurance capabilities such as role-based access control, inventory/fault management, and basic voice reporting.

Stage 1

The organization has only static virtual segmentation for its infrastructure and has a limited access port policy definition which is also manually configured. Less than 5 percent of the organization's core infrastructure and distribution layer technologies and less than 30 percent of access layer technologies have reached an end of support status. Its network design is not modular, cannot be scaled, and operates on a fixed switch platform. The organization has implemented an active/standby failover procedure it uses for the core and distribution layer of the network, but it has single points of failure. There are redundant components available, but for less than 5 percent of its wireless controller infrastructure and less than 30 percent of its wireless access point infrastructure. The network design is based on a single on-premise wireless controller with a combination of lightweight and autonomous access points. The organization has implemented an analog/digital PBX.

Stage 0

The organization has not implemented VPN support, but may have some level of access control and related policy. It has not implemented or configured any quality of service settings or policy definitions, and has not implemented an intrusion detection and prevention system. There are no formal security policies implemented or enforced, no dedicated data center network, and no structured compute architecture in place.

For more information visit: www.himssanalytics.org/benchmarks