CYGNA LABS

Applying ITIL® Best Practice Principles to DDI

By Timothy Rooney

About Cygna Labs

Cygna Labs is a software developer and one of the top three global DDI vendors. Many Fortune 100 customers rely on Cygna Labs' DDI products and services, in addition to its industry-leading security and compliance solutions to detect and proactively mitigate data security threats, affordably pass compliance audits, and increase the productivity of their IT departments. For more information, visit https://cygnalabs.com.

Introduction

The discipline of network management affords innumerable technical and business benefits to organizations via the centralization of control, monitoring, and provisioning of distributed network elements such as routers and application or services databases. These benefits include holistic management of the entire network from a centralized point where appropriate resources and expertise can be leveraged for troubleshooting, resolution, and escalation. This pan-network approach lends itself well to supporting structured network change control procedures and is even more crucial today with enterprise networks expanding into clouds, IoT subnetworks, and mobile networks.

Because IP addresses and associated DHCP and DNS functions are foundational to IT services and applications running over an IP network, these functions must be prudently managed, much as other critical network infrastructure elements are managed. The most commonly applied network management approach is that of the FCAPS model from a functional perspective and ITIL® from a service management perspective. This white paper highlights key ITIL areas as applied to IP address management (IPAM), and the benefits that can be realized by using this management framework.

The FCAPS Legacy

To fully understand and appreciate ITIL, let's start first with a quick review of the International Telecommunications Union (ITU) network management standard FCAPS, which is an acronym for the five major management functions: Fault, Configuration, Accounting, Performance and Security. These five functions should be considered when implementing a network management architecture, whether it's for a service provider or enterprise environment. FCAPS is specified in the ITU's M.3400-series, which deals with telecommunications network management.

- **Fault management** deals with alarming and detection of faults within the various elements of the network and the localization or identification of the root cause of those faults, as well as the correction, repair, testing and trouble-reporting of faults.
- **Configuration management** involves planning, installing and provisioning of a new network element, as well as adding in customer related data. Provisioning of a new customer, for example, on a telecommunications-type service would impact the configuration management function.
- **Accounting management** addresses the collection of information that can be used, perhaps by a billing or usage management system. As such, the accounting management function measures the use of the network and associated resource utilization, which can be used to generate goals for evolving and improve network services.
- **Performance managemen**t encompasses the evaluation and reporting of the behavior and effectiveness of network equipment. This includes measurement of capacity and quality of transmissions, usage of network elements and CPU utilization. In a nutshell, it helps make sure the network is running on all cylinders.
- **Security management** deals with the prevention, detection and containment of any security issues or concerns related to your network, computing and applications infrastructure. It also includes an audit logging capability in order to troubleshoot or analyze any violations or to detect security violations.

ITIL Overview

FCAPS was developed as a standard for management of telecommunications service providers' networks. ITIL, formerly known as the Information Technology Infrastructure Library, is a documented set of best practices for use by an IT organization desiring to manage, monitor, and continually improve IT services provided to the enterprise organization. ITIL was originally developed by the U.K. Office of Government and Commerce, and is now managed by Axelos, a joint venture company created by the Cabinet Office of Her Majesty's Government in the UK and Capita, plc. Its IT-service oriented approach has been deployed by a number of organizations. The most common drivers for ITIL implementation include:

- Cost reduction of IT services delivery to the organization
- IT service level consistency and improvements
- Risk management through disciplined planning and evaluation of potential service-affecting changes
- Efficiencies in utilizing documented processes and continual improvement

ITIL 4, the latest version, was launched in February, 2019 as an evolution of version 3. There are many similarities between the two versions, but the major changes introduced in ITIL 4 include the following:

- The service value chain concept, depicted in Figure 1, has replaced the ITIL 3 service lifecycle in order to loosen the implication of an ordered serial process and to more accurately reflect the use of service value chain activities alone or in conjunction with others in no specific order to provide value.

- The concept of how value is created has evolved from that of being created by IT alone (service provider) to that of being jointly created by the service provider and the service consumer, which in turn comprises the customer or services definer, user of the service and sponsor or budget authorizer.
- The concept of "process" has been broadened to that of "practice", which defines a broader perspective and accounts for people, partners, technology and processes.

The demand or opportunity component of the Service Value Chain, depicted on the left side of Figure 1, denotes the recognition of a business need that can be addressed jointly with IT and other teams within the organization. The Engage activity consists of collaboration among cross-functional team members to define solutions to the identified need or opportunity.

The design and transition activity serves to design products and services that continually meet stakeholder expectations for function, quality, cost and time to market, including transition of new or updated products and services. The obtain/build activity identifies implementation alternatives that meet stakeholder requirements, often involving analysis of "make or buy" alternatives in full or in part. Deliver and support activities ensure products and services adhere to product and services specifications and are support in accordance with service level agreements.

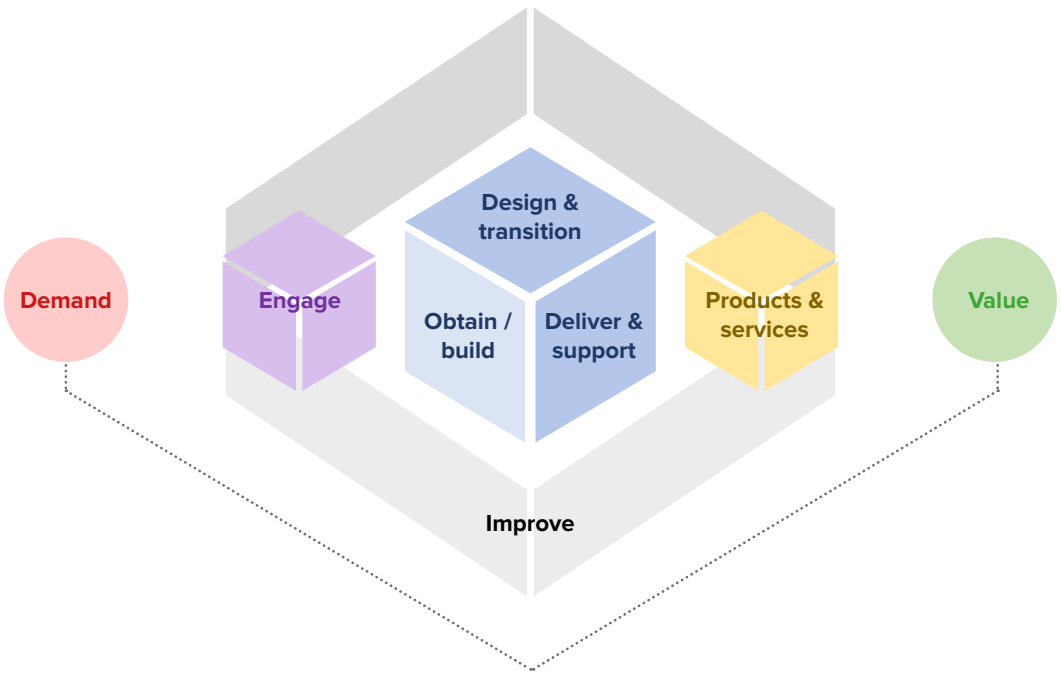

Figure 1: ITIL 4 Service Value Chain (source: Axelos)

The products and services activity involves the lifecycle management of those defined and delivered within the product and service catalogue which ultimately are intent to provide or exceed the anticipated value for the organization. As circumstances evolve, new demands may arise which feeds back to the beginning of the service value chain.

Enveloping the service value chain is an overall plan activity, which seeks to anchor the chain with a cohesive vision for the current status, future direction and improvement direction of the service chain, and the improve activity which affords continual improvement of products and services.

ITIL Business benefits

ITIL is focused on providing value to your organization, particularly the business of value creation for customers, efficiency gains for internal operations and cost management for IT and affiliated stakeholders. The key business benefits include:

- Reducing the cost of delivery of IT services.
- Improving IT service levels and consistency—for instance, consistently allocating a new address for a user within two hours.
- Managing risk through the identification of risks up front and developing backup plans.

- Maximizing efficiency by documenting processes, executing them the same way every time and by honing them over time through the continuous feedback cycle.
- Meeting regulatory and compliance requirements (may be industry specific).

FCAPS and ITIL

A basic comparison between FCAPS and ITIL is shown in Table 1. FCAPS, as previously mentioned, is an ITU standard with a primary focus on telecommunications. ITIL is explicitly focused on enterprises, though with an "IT as a service provider" perspective.

Table 1: FCAPS/ITIL Comparison

	FCAPS	ITIL
STANDARD GOVERNANCE	ITU	Axelos
FOCUS	Telecom	Enterprise
COVERAGE	Narrow – implementation	Broad – strategy, implementation, continual improvement
ORIENTATION	Functional	Service Value
ADVOCATES PROCESS	Yes	Yes
PROVEN, REPEATABLE, DISCIPLINED	Yes	Yes
BEST PRACTICES FRAMEWORK	Yes	Yes

FCAPS is narrow in scope with its focus on operations and the nuts and bolts of implementation, e.g., what to do when you get an alarm. ITIL has a much broader scope, encompassing strategy stakeholders and continual improvement along with implementation. ITIL considers how IT can help the business—not only executing tasks from a brute-force methodology, but also folding IT into the overall strategy to provide the best service possible.

From an orientation perspective, FCAPS is functional and task-oriented, whereas ITIL is service-oriented. Both FCAPS and ITIL advocate documented processes and proven and repeatable disciplines that can be executed by anyone, with the expectation of achieving similar results each time. And both form the foundation of best practices frameworks for their respective focus areas.

IPAM Fundamentals

Before we discuss how ITIL, as well as FCAPS, applies to IP address management, let's start with an overview of the key functions IP address management performs.

IPAM is comprised of three key functions:

- IP address inventory of address blocks, subnets and individual IP addresses
- Dynamic Host Configuration Protocol (DHCP) server management
- Domain Name Server (DNS) server and security management

IP address inventory entails rigorously tracking your IPv4 and IPv6 address space across your LAN, WAN, SD-WAN, cloud, IoT, wireless, Internet access and partner networks. This includes allocation of address blocks and subnets and inventorying individual IP address assignments, whether they are static addresses for routers or servers, or those within an address pool. For address pools within subnets, the configuration of DHCP servers must be performed in accordance with the address plan such that end users accessing the network may automatically obtain IP addresses from the proper pools using the DHCP protocol.

Likewise, for static addresses in the address plan, you're going to have routers and servers, cloud virtual machines and other devices that are statically configured, hence their denoting as static addresses. Once configured, you can reach these devices by the corresponding IP address. But you might want to reach them by name as opposed to remembering each device's IP address. Fortunately, DNS provides a way to map a device name to an IP address so I can type in my router's name, which my browser looks up in DNS, to find the corresponding IP address and connect to it. DNS provides that hostname to IP address mapping, and a lot more. DNS security adds to overall network security and is a crucial layer of a defense-in-depth strategy.

To summarize, the IP address plan component of IPAM minimizes the chance of errors in assigning the same address to one or more static addressed devices, let alone to portions of an address pool configured on a DHCP server. The use of DHCP itself automates address assignment; once configured in accordance with the address plan, a DHCP server dispenses addresses from its pools to laptops, printers and other devices as needed to access the IP network without manual intervention. Likewise, DNS works behind the scenes to resolve host names into IP addresses so computers can communicate and people can use them. IPAM helps IP network administrators cohesively manage these three core components—IP inventory, DHCP and DNS—to provide users easy access to and use of the IP network. Like other aspects of network management, IP address management should follow a rigorous and disciplined approach.

Applying FCAPS to IPAM

FCAPS defines a disciplined network management approach for managing network elements. IP addressing, DHCP and DNS certainly qualify, so application of a disciplined FCAPS framework is appropriate:

- **Fault management** deals with the detection of DHCP and DNS server faults and cloud IP addressing faults. This includes troubleshooting, isolating and resolving the faults through a monitoring and alerting process.
- **Configuration management** encompasses the accurate configuration of DHCP and DNS servers so that the DHCP address pools are consistent with the address plan and DNS-hostname-to-IP-address mappings are likewise consistent. Configuration support or validation of router subnets and cloud virtual machine IP addresses also falls within this area. Having a consistent and accurate address plan using a centralized inventory can help assure the accuracy and proper configuration of the DHCP and DNS services and IP address occupants across your diverse network.
- **Accounting management** can be applied to IPAM with respect to tracking the usage of IP addresses. Being able to track what IP addresses an employee used over a specific time period is very helpful from an accounting management perspective.
- **Performance management** monitors resource utilization of the DNCP and DNS services and IP address space in general. It enables network administrators to know if they have enough addresses in their address pools and if the servers are running at full capacity from a processor and memory perspective.
- **Security management** supports IPAM and overall network security policy defnition and enforcement. This includes network access monitoring, administrator access control, secure server deployments, denial of service mitigations, DNS tunneling detection, malware detection via DNS firewalls and DNS security extensions (DNSSEC). Audit logging for spot checking, troubleshooting and just for general auditing purposes also falls under security management.

Clearly, FCAPS principles can be applied to IPAM, and hopefully the IPAM solution you choose gives you the key functional areas needed from an FCAPS perspective without having to purchase additional tools.

Applying ITIL Practices to IPAM

ITIL practices are split into three areas: general, service and technical management. General management practices focus on broad business and management areas. Service management practices relate to IT services management, while technical management deals with IT software development and infrastructure management. A brief summary of the practices that fall within each ITIL practice area and their relevance to IPAM follows.

General management practices

- **Architecture management** entails inventorying all of the elements that comprise the organization and the interrelationships among them. Identification of such assets including people, technology and processes enables an organzation to manage complex change in an agile and controlled manner.

IPAM Impact: Tracking and managing IPAM assets including physical and virtual IPAM servers, IP address blocks, IP assignments, DHCP servers, pools and leases, and DNS servers, domains and resource records fall under this area. An IPAM system that tracks the dynamics of this information is indispensible for accurate identification of assets that need to be redeployed for example to address a business need.

- **Continual improvement** focuses on identifying the current state of IT services, the desired state, and an assessment of how to progress from the current to the desired state possibly through a number of steps. As business needs evolve and change, the desired state likely changes as well, ergo the use of the “continual” moniker.

IPAM Impact: An IPAM system can provide an accurate perspective on the current and predicted future state of IP address space, DHCP pool capacity and DNS server performance for example. Each of these items and others may require improvements to better meet the demands of the business, and understanding the current state helps to define incremental steps required to attain the desired state. Some IPAM systems such as IPControl from Cygna Labs support modeling of the desired future state to facililtate planning and continual improvement.

- **Information security management** comprises securing the information that the organization requires to conduct operations. This includes identifying risks, assessing the likelihood and cost of addressing each risk, and defining a plan to prevent, detect and correct situations where such risks are exploited.

IPAM Impact: Beyond inventorying IPAM related assets, an IPAM system should support secure deployment and communications among its components. It should also facilitate configuration of security features such as access control lists, rate limiting controls, authentication and encryption, among others. In addition, configuration and support of DNS security measures such as DNS firewalls and DNS tunnel detection broadens your overall network security. Please contact us to receive our NIST Cybersecurity Framework Core applied to the practice of securing DNS for key considerations when securing your DNS in accordance with the NIST de facto security standard.

- **Knowledge management** consists of assuring appropriate access to information and knowledge within the organization to improve efficiencies and decision making. This practice implies providing simple access to information for those requiring such information without exposing it beyond the need to know in keeping with the security principle of least privilege.

IPAM Impact: Your IPAM system should support administrator controls to constrain access by certain users to particular information for which they are responsible.

- **Measurement and reporting** is critical to supplying the information necessary to detect fault or security incidents and to assure services availability and performance. You can’t manage what you can’t see. Monitoring IP address usage, DNS and DHCP server states and performance metrics for example provides valuable input to assess service availability and assure *operation*.

IPAM Impact: IPAM systems should enable monitoring and reporting of administrator activity for auditing, deployed DHCP and DNS server status and availability, as well as DHCP and DNS transaction loads, trends and forensics.

- **Organization change management** deals with managing organizational changes smoothly including managing human aspects of such changes as appropriate.

IPAM Impact: Any changes affecting IPAM responsibilities of particular personnel should be reflected in system access permissions coincident with such changes.

- **Portfolio management** practices are intent on assuring the organization is supporting a solid mix of IT services, products and solutions to meet its overall business objectives. As the scope of an organization's requirements for IT services expands to incorporate newer technologies such as IoT, cloud, artificial intelligence, etc., this practice would be responsible for managing IT services evolution to incorporate these requirements.

IPAM Impact: As the diversity and span of your network expands, your IPAM system needs to keep pace, given the foundational role IPAM serves in IP networks.

- **Project management** comprises the practice of efficiently planning, executing and completing projects within time and budget constraints.

IPAM Impact: Your IPAM system should allow planning of alternative approaches, e.g., to IPv6 allocations, server deployments, cloud virtualized network functions, etc.

- **Relationship mnangement** focuses on the organization's stakeholders and manages these relationships with respect to maximizing stakeholder satisfaction through the understanding of stakeholder requirements, prioritization of IT projects, and effective delivery of products and services delivery accordingly.

IPAM Impact: Offering IPAM system read-only visibility to organizational stakeholders may provide a vehicle for transparency and collaboration.

- **Risk management** is broader than information security management discussed above, in considering all of the risks and vulnerabilities to an organization, including risks to facilities, people, and business operations.

IPAM Impact: Your security and risk mitigation plans including business continuity, pandemic response, and disaster recovery plans should consider and address IPAM components and systems.

- **Service financial** management naturally includes accounting, similar to accounting management in the FCAPS model, though the financial management area addresses actual dollars and cents as well. This process area also deals with any chargebacks or cost allocations for certain departments under an IT funding or cost allocation model.

IPAM Impact: Some firms do implement cost chargebacks for IP address usage. In such a scenario, the financial management processes would need to account for tracking of IP address usage along with the corresponding user and chargeable entity (e.g., department). Depending on the billing or chargeback cycle, this IP address usage information will need to be stored for the current cycle and beyond to enable archiving or dispute resolution. Audits and history data in your IPAM system can be a big help with cost allocation.

- **Strategy management** comprises the enumeration of the goals of the organization and the allocation and management of resources necessary to achieve said goals. Each goal is distilled in terms of impacts on constituent organizations including IT, which must manage its resources to fulfill its role in meeting organizational goals.

IPAM Impact: Every IT initative involving networking likely impacts IPAM in some manner. Planning and scenario analysis capabilities can be useful in considering IPAM impacts of potential strategies.

- **Supplier management** involves supplier contract management and the continual measuring of each supplier's performance with respect to meeting the objectives established upon contracting with each. Collaboration with key suppliers can facilitate improved value creation through joint enhancements or solutions.

IPAM Impact: Use of multiple vendor DHCP and DNS products, IoT suppliers, and private and public cloud providers can impact corresponding supplier relationships and should be considered within this practice area.

- **Workforce and talent** management practices involve assuring people resources are properly aligned with the organization's goals with respect to staffing and recruiting of people with appropriate skill sets for each job role, training and development and succession planning.

IPAM Impact: Periodic auditing of IPAM administrator system activities can be helpful input to assessing administrator proficiency and/or training needs.

Services Management Practices

- **Availability management** is a practice focused on making sure IT services are available to end users. High availability, a common goal for applications including cloud, DHCP and DNS, requires deployment of redundant configurations and the ability to leverage these configurations to provide continuous service in the face of a component outage.

IPAM Impact: Deployment of redundant DHCP and DNS server clusters, e.g. virtual or physical appliances, can provide localized clustering, while implementation of DHCP failover or split-scopes and multi-master DNS deployments provides an additional layer of redundancy. Redundant IPAM database deployments through LDAP, sharded clusters, or replicated relational databases with automated failover can also assure availability of the IPAM application for managing IP space. Monitoring of the availability of each of these redundant components enables proactive detection of outages to facilitate rapid outage resolution while redundant components shoulder the load.

- **Business analysis** is a key practice in understanding business requirements and fermenting these into IT requirements for technology, training, and operations processes needed to meet stated business goals.

IPAM Impact: IPAM components cost money, so optimizing component deployments to provide desired performance, availability and security is key. Monitoring and measuring such aspects provides valuable input into assuring maximum cost efficiency.

- **Capacity and performance** management simply involves assuring adequate IT resources of the proper type are available for the business to conduct its work.

IPAM Impact: Considering the application of this concept to IPAM, certainly IP address capacity management springs to mind, but one should also consider DHCP and DNS server load capacity. In the former case, capacity management requires monitoring of addresses and address pools to provide enough IP addresses for employees to get an address and access the network. Monitoring for trends is helpful, and enabling alerting for low pools is also recommneded for tightly allocated networks. Of course, given the magnitude of IPv6 address space, this will likely not be an issue for IPv6 space for most enterprise networks but tracking of address occupancy is crtical for auditing and forensics activities.

With respect to server capacity management, monitoring each physical and virtual server's network, memory and CPU utilization over time can provide insights into its load and performance. Such performance tasks may in fact be required as a linkage to service level management in terms of percentage of transaction completion (lease or resolution) as well as response times. Regardless, excessive loads on servers can have detrimental impacts on the availability of DNS and DHCP services, so server monitoring and perhaps even probe-like transactional monitoring can provide effective measures of service levels and capacity.

- **Change control** provides controls on the implementation of changes in the IT infrastructure. This involves assuring that all affected parties are in agreement with respect to the scope and implementation timing of the proposed change.

IPAM Impact: The scope of change management commonly affects IPAM components, such as the addition of an address pool, deployment of a new DHCP/DNS server in the network, deployment of cloud subnets or virtualized functions, or upgrading a server to a new software version. And some IPAM changes require network changes, such as subnet provisioning or updating relay agent router configurations. Basically, anything affecting any part of the infrastructure, whether it's physical, virtual or software or even underlying appliance operating systems, falls under the change management process, which seeks to assure all appropriate approvals are in place and corresponding back-out plans are available.

- **Incident management** is a practice area which involves tracking and resolving incidents to restore normal services as efficiently as possible. Through incident management, IT can also detect and troubleshoot network issues proactively.

IPAM Impact: Regardless of the means of detection for a given incident, access to IP inventory data is indispensible to troubleshooting and incident resolution. In addition, monitoring of server states with thresholds, alerts, logging information and audits can provide a head start to incident detection and verification of incident resolution.

- **IT asset management** entails managing the lifecycle of IT assets from purchasing decisions, allocation of assets as required, reuse, retirement and disposal within the context of meeting organizational, contractual,regulatory and envionmental requirements while maximizing value, controlling costs and managing risks.

IPAM Impact: From an IPAM perspective, this practice must assure proper sizing of IPAM, DHCP and DNS servers, trading off budget availability with performance requirements, among other criteria. Refreshes of hardware is also a critical component of this practice to assure hardware reliability.

- **Monitoring and event management** involves surveilling all or at least core network components to verify appropriate performance and to detect state changes or events that may arise as they inevitably do. The goal is to identify events that could indicate potential or pending incidents or faults.

IPAM Impact: We recommend you monitor your IPAM, DHCP and DNS services to identify performance degradation, communications errors, or other issues that could herald a server or service outage. This practice calls for initiating proactive measures to restore hampered servers while relying on redundant servers to compensate prior to and in an effort to prevent a full service outage.

- **Problem management** calls for the tracking of known problems and resolutions in a problem forensics database. If someone calls into the service desk with an incident, for example, it could get bumped over to problem management to identify whether this incident has been reported and addressed in the past. If so, the defined resolution path can be followed to quickly troubleshoot and resolve the issue.

IPAM Impact: While IPAM systems traditionally don't store problem histories with resolution annotations, some can provide a database of problem information through logging history, as well as inventory change audits. Some vendors enable access to general knowledge databases, available as part of their support services. Network management system integration through APIs can provide a holistic view of problem history by providing IPAM data through the API to a trouble ticketing system for example. IPAM is a key part of the overall network or IT service management approach, but it's not comprehensive; no system is. Having that integration is a key to garnering a holistic view of the problem management scope.

- **Release management** is a practice area which provides controls on deployed releases for hardware and software versions, not only for operating systems, but also for applications and appliances. This process area is responsible for making those versions available and accessible on the IT network and assuring there's an authorized set of releases and versions available that can be deployed appropriately.

IPAM Impact: Release planning, release management, dealing with upgrades and patch management for DHCP and DNS services at remote sites and in the cloud from a central location can be a big timesaver. The alternative, requiring on-site upgrades of operating system, patches, and application software is costly and time-consuming. Release management of the IPAM system also falls within this category.

- **Service catalogue management** consists of maintaining a centralized repository of all services, solutions, products and service components supported by IT for the organization. Such a catalogue documents the suite of IT products and services available to the user (customer) community as well as technical and organizational steps required for implementation of each to enable efficient and consistent service delivery.

IPAM Impact: IPAM components certainly comprise critical ingredients for IT services and associated impacts must be catalogued, e.g., a new type of network device that requires a unique set of DHCP options for example.

- **Service configuration management** is similar to the FCAPS configuration management functionality in terms of identifying, recording and controlling configuration items (CI's) affecting IT services.

IPAM Impact: Configuration management functions are core to IPAM, from configuring new address pools from a DHCP perspective, zones and resource records in DNS, to IP addresses for subnets on routers, IoT devices, or cloud systems, etc. The IPAM database can be considered a configuration management database (CMDB) component of an IT's confederation of CMDBs for network configuration inventory.

Administrator controls need to be considered for organizations with more than one IPAM administrator to ensure that changes to DHCP and DNS configurations are performed within the appropriate scope and permissions. For instance, you may want administrators to be able to make changes, but not actually deploy them on the DHCP and DNS servers – restricting that function to a higher level of administrator. On the back end, audit information if key for accountability tracking and reporting.

Possessing accurate IP configuration information is necessary to provide a solid foundation on which future configuration changes can be planned. A corollary requirement leads to the necessity of validating that inventory against network actual data. IP inventory tracked on a spreadsheet is great, but requires constant manual updating. The ability to collect information from the network and compare it with the plan is crucial to automation and IP inventory assurance. Audits go hand in hand with inventory information collection. Arming the service desk with this information can provide a solid first line for addressing calls immediately, or to at least moving them through the process more quickly.

- **Service continuity management** is related to availability management in that it deals with providing continuous services. For example, in the event of a disaster, this process area would require a disaster recovery plan be in place.

IPAM Impact: A variety of deployment strategies are available based on the criticality, cost and scope requirements of the organization for particular DHCP/DNS servers and IPAM systems.

- **Service Design** is the practice area where technology solutions and products are integrated for the purpose of delivering a given IT service to the organization. This practice requires creative skills for identifying service components, and associated suppliers, and potentially stitching together two or more components in a "service chain" to provide the overall desired

service. Supplier management skills are required for the evaluation and testing of products as fit for purpose as well as integration capabilities in accordance with service requirements.

IPAM Impact: DHCP or virtual machine cloud API-based device initialization is commonly required for new services in particular as is specific DNS resolution requirements. IP addressing, and DNS security impacts must also be considered.

- **Service Desk** serves as the interface to the user community, the Service Desk filters input to the IT organization for incident reporting, change requests and even new service requests. It serves to qualify and direct user requests or problems to any one of the other ITIL areas, providing end users with a helpdesk function.

The policies and culture of the organization will drive whether the Service Desk performs traditional "level 1" support only by logging troubles with subsequent follow-up, or higher support levels, performing a thorough diagnosis. In the case of level 1 support, little more is needed than a ticketing system with the ability to assign tickets to those responsible for other process areas depending on the caller's issue. A service desk staffed to perform some trouble diagnosis will require access to status monitoring tools to try to "see what the caller sees" with respect to the issue.

IPAM Impact: For IP address or name resolution related calls, providing service desk personnel access to IP inventory information may prove beneficial. For instance, if a person located in the Headquarters office is not able to get an IP address, the service desk needs to know the address plan for Headquarters in order to focus the problem and trouble resolution process on that particular subnet, associated routers, cloud platforms or DHCP/DNS servers.

The service desk is the interface not only for trouble reports, but for change requests, such as IP subnet or address assignments. Providing service desk personnel with basic access to the IPAM system to request such changes, or better yet, enable end users themselves to register such service requests to an automated IT portal can increase end users' satisfaction with IT services through rapid fulfillment. Sch a portal interface with linkages to your IPAM system can streamline the service request process.

- **Service level management** is a delivery and support practice area which encompasses the specification of service levels for various services provided by the IT organization. This is akin to a service level agreement (SLA). An example metric is the time frame within which an IP address will be assigned or a DNS resolution provisioned. Service level management includes measurement of service delivery against these specifications to monitor adherence and measure the level of service that IT provides.

IPAM Impact: From an IPAM perspective, service level management involves definition and measurement of the levels of service provided to those requesting IPAM related services, whether it be end users requesting an IP address or the business needing to open a new office. Treating end users of the business as customers, this process seeks to gauge whether service delivery is meeting defined service levels, such as timeliness of completion of these requests. Automating IPAM related service delivery, whether solely IPAM-impacting or involving IPAM as a component of a broader IT service such as VoIP deployment, facilitates timely and accurate services delivery.

- **Service request management** comprises the handling of user requests for defined IT services, e.g., from the services catalogue. Establishment and measurement of SLAs for service requests enables the IT organization to provide a reliable service enabled in a timely manner.

IPAM Impact: Measuring DHCP and DNS response time and that of relevant automation workflows is important to fully appreciate the overall stakeholder experience to assure service performance.

- **Service validation and testing** seeks to ensure the implementation of a new or modified IT service meets requirements set forth by the organization when commencing and deploying new development or modification of a service.

IPAM Impact: New or modified IT services may likely impact IPAM configurations, so foundational IPAM components must be included in all such validation and testing practices.

Technical management practices

- **Deployment management** ultimately involves the "putting into production" new, updated or modified software, hardware, processes, documentation, and operations related practices. Prior to production rollout, this practice also entails lab testing and staging as warranted to improve the likelihood of a successful deployment.

IPAM Impact: As foundational to IT services and general IP networking, IPAM components must be included in lab testing and staging of new or updated products and services.

- **Infrastructure and platform management** consists of monitoring IT infrastructure and platform components with respect to industry offerings and solutions and how they could benefit the organization in terms of enhancing current services or otherwise improve the organization's operations. Such forward looking activities are required to maintain parity if not leadership with industry initiatives and trends.

IPAM Impact: IPAM components are common across all IT services that require IP network initialization and/or DNS navigation, whether on private or public networks or clouds.

- **Software development and management** deals with design, specification, development, testing, delivery and feedback/fixes/enhancements for software developed within the organization. Many IT organizations employ a DevOps approach given a well-scoped user community in general which can provide input and iterative feedback as software enhancements and fixes are released.

IPAM Impact: Rapid and agile services development necessitates flexible and agile IPAM systems including DHCP/DNS services and cloud automation workflows to facilitate tweaking and testing of software and services updates.

Conclusion

Designed as an evolutionary change, ITIL 4 seeks to broaden the perspective of IT services management to broader organizational goals and constituents, while building upon most of the foundational concepts and processes specified in prior ITIL versions. ITIL best practices serve as an industry benchmark against which you can measure the effectiveness of your IT practices and plan for improvements.

Whether you're comfortable with the legacy FCAPS model or the enterprise-focused ITIL service management approach, the institution of a disciplined and documented approach to performing IT functions can help save time and money. Performing service delivery functions in a consistent, repeatable manner yields predictable and measurable service levels. These service levels can then provide a measure of IT service expectations for the end user community and enable IT to meet or exceed such expectations regularly, maximizing efficiency and productivity.

As IT services increasingly require IP-based applications and services, the reliance on an effectively managed IP network grows. It follows that IP address management functions should be on the forefront when implementing a disciplined IT management scheme. The IPControl™ Sapphire product line from Cygna Labs Diamond IP addresses many of the IPAM impacts discussed in this white paper and can provide a key ingredient in implementing FCAPS and/or ITIL.

Toll Free: **(844) 442-9462**
International: **+1 (305) 501-2430**
Fax: **+1 (305) 501-2370**

Sales: **sales@cygnalabs.com**
Support: **support@cygnalabs.com**
Billing: **finance@cygnalabs.com**

cygnalabs.com

CYGNA LABS