IT Service Management and Infosec: Collaborate for Mutual Success

Kevin Geil

IT Service Management and Infosec: Collaborate for Mutual Success

GIAC GCCC Gold Certification

Author: Kevin T. Geil, Info@placidsecurity.com
Advisor: Clay Risenhoover

Accepted: June 8, 2021

Abstract

Collaboration between information security and IT is critical to the success of both teams. Information security frameworks and IT service management methodologies share a foundation in asset management, configuration management, and change management. This research describes the nexus between information security and IT service management by mapping ITIL version 4 management practices to the CIS Critical Security Controls. It shows that in many cases, information security controls and IT service management practices can be implemented and audited using the same steps.

1. Introduction

Businesses and users often view information security measures as a burden necessary to protect the organization's assets. In contrast, Information Technology Service Management (ITSM) methodologies are considered to be management strategies that enhance the company's performance. In reality, the foundation of both disciplines is essentially the same. When approached this way, ITSM methodologies and information security programs create synergy that greatly enhances both practices. This paper outlines the close relationships between IT service management methodologies and information security frameworks by discussing the congruencies between the Center for Internet Security (CIS) Critical Security Controls version 8.0 (CIS Controls) and the Information Technology Infrastructure Library version 4 (ITIL).

Information security is often described as the application of controls to balance confidentiality, integrity, and availability of information to keep risk within documented, acceptable thresholds. ITSM is defined as the development and application of a set of practices to information systems to maximize business value ("*What is IT Service Management*?," n.d). Both disciplines attain their objectives by achieving detailed documentation of Information Technology (IT) assets, along with their configurations and interactions with one another. After establishing this baseline, changes to assets and configurations are managed. In plain terms, ITSM and information security are based on three principles: 1) Knowing what you have, 2) Knowing how your assets are configured, and 3) Managing change to those configurations. This foundation enables practitioners to monitor systems for anomalies, which is a powerful method for ensuring that services are provided efficiently and reliably and reducing security risk to the organization.

The DevOps movement revolutionized software development methods. Before its inception in 2009, companies developing software faced difficulties navigating organizational silos between software developers and operations teams responsible for building the infrastructure on which development work is done. DevOps achieves its success and popularity by merging these silos and creating a shared mindset between

developers and operations teams with a shared set of principles. Recommendations from *The DevOps Handbook* (2016) include integrating information security (Infosec) as early as possible in the development lifecycle and providing the opportunity to incorporate information security requirements into projects from the beginning. Accomplishing this allows for the adoption of guidance from Infosec "in the earliest stages of the project when there is the most amount of time and freedom to make corrections" (Kim et al., 2015). The incorporation of infosec into DevOps is sometimes called DevSecOps. When applied to companies not focused on software development, the term used is SecOps, or the merging of Infosec and IT operations. This nexus between security and operations is the focus of this paper. A well-executed SecOps implementation manifests itself in a set of shared principles and operating procedures which enhance both ITSM and information security. This research will present a foundation for such principles and operating procedures.

The ITIL framework was selected because of its broad applicability across various organization types and sizes. ITIL began as a project in 1987 within the United Kingdom government's Central Computer and Telecommunications Agency (CCTA), collaborating with IBM to standardize approaches to IT infrastructure management. The first product was a library of books outlining best practices ("*How ITIL started*," 2013). ITIL is now the most commonly used ITSM framework worldwide (Watts, 2021). ITIL was updated in 2019 and 2020 (to version 4) and incorporated concepts from other ITSM methodologies, including Lean, DevOps, and Agile. ITIL prescribes a set of thirty-four "management practices," which are a specific set of activities intended to ensure the efficient delivery of IT services with a focus on creating value for the organization. Major guiding principles of ITIL are progressive iteration, feedback loops, and continuous improvement (Rae, 2020).

The Center for Internet Security (CIS) Controls were chosen because CIS drafts the controls collaboratively, achieving consensus from experts in a broad range of roles from multiple organization types worldwide. This consensus approach makes the CIS controls an effective basis for cyber-defense across a wide range of organizations. CIS introduced the concept of "implementation groups" with version 7.1 of the Critical

Security Controls. The three implementation groups are based on organization size, risk appetite, and security program maturity. This use of implementation groups broadens the utility of the CIS controls to organizations of any size. There are eighteen high-level Critical Security Controls, each with a set of specific sub-controls. Sub-controls are associated with implementation groups that assist the prioritization of control applications. CIS designs the controls to fulfill the requirements of regulatory and compliance frameworks (CIS Controls, 2021). The approach used by CIS in development of the Controls: consensus-driven control design, specific guidance on prioritization, and applicability to a wide array of control frameworks makes the CIS controls suitable for almost any organization.

A search of the CIS website for the word "mapping" will produce links to multiple documents which map the CIS controls to compliance and regulatory frameworks. Enclave Security maintains a "master mapping" document that maps the CIS controls to more than forty frameworks (Enclave Security, 2020). As of this writing (April 2021), a mapping document for ITIL Version 4 is unavailable. This paper provides evidence from both ITIL and CIS controls to create such a mapping document. ITIL lists "Information security management" as one of its management practices that broadly addresses information security as part of its methodology. Still, other ITIL practices provide rich opportunities for mapping to CIS controls. Section 2.0 below describes these mappings. Section 3.0 provides systems documentation examples and auditing examples that effectively assess compliance with CIS controls and ITIL management practices.

2. Mapping CIS Controls to ITIL Management practices

Section 2 of this paper maps CIS controls to several ITIL management practices. A table for this mapping is included in each sub-section. Appendix A combines the tables from section 2, outlining all of the relationships discussed in this document. Appendix B presents a table from the reverse perspective: CIS controls mapped to related ITIL management practices.

2.1. ITIL 5.1.1: Architecture management

The goal of ITIL's architecture management practice is to establish a documented architecture of the business, describing relationships among the information assets, tools, and technology critical to business operations. (*ITIL Foundation*, 2019). The combination of ITIL's architecture management practice and the three CIS controls listed in table 1 below creates positive feedback loops between IT service managers and the infosec team.

ITIL 5.1.1: Architecture management	CIS Control 1: Inventory and Control of Enterprise Assets CIS Control 2: Inventory and Control of Software Assets CIS Control 4: Secure Configuration of Enterprise Assets and Software

Table 1. ITIL's Architecture management with its associated CIS Controls

The definition of enterprise architecture from the NIST Computer Security Resource Center glossary effectively summarizes the components of ITIL's architecture management practice:

> The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated

> to support the enterprise mission, and how they contribute to the enterprise's overall security posture. (2004)

Asset management, a significant component of architecture management, is critical to both ITSM and information security. Managing or securing assets without awareness of their existence is difficult. Application of CIS Control 1 and 2, (Inventory and Control of Enterprise and Software assets) supports the ITIL Enterprise Architecture management practice by helping organizations identify all hardware and software assets owned by the organization. Information obtained through the application of ITIL's Architecture management practice enables successful application of CIS control 4: Secure Configuration of Enterprise Assets and Software. Through the application of architecture management principles, practitioners gain awareness of hardware and software assets and how they connect, building a robust foundation for both ITSM and Information security.

2.2. ITIL 5.2.1. Availability Management

Availability management is a substantial component of both ITSM and information security. Among the recommendations of ITIL's availability management practice are:

- "*ensuring that services and components are able to collect the data required to measure availability*" (*ITIL Foundations*, 2019).
- *"Monitoring, analyzing, and reporting on availability"* (ITIL Foundations, 2019).
- Ensuring an appropriate Mean Time Between Failure (MTBF) or Mean Time To Restore Services (MTRS). (*ITIL Foundations*, 2019)

Table 2 below shows the two CIS controls which support ITIL's Availability Management practice.

ITIL 5.2.1. Availability Management	CIS Control 8: Audit Log Management CIS Control 11: Data Recovery

Table 2. ITIL's Availability Management with its associated CIS Controls

CIS Control 8, Audit Log Management, establishes the foundation for availability monitoring. In the SANS SEC 566 coursebooks, Enclave Security considers a log management/Security Information and Event Management (SIEM) system to be a "minimum control sensor" (2021). With properly configured audit policies, Host Intrusion Detection (HIDS) agents and Endpoint Detection and Response (EDR) agents are capable of recording service events, such as start, stop, and failure. A log management solution can parse these events and generate alerts and statistics such as MTBF to measure progress toward availability goals.

The underpinning of data availability assurance is a thorough and regularly tested disaster recovery plan. The ever-increasing number of ransomware attacks in the daily news reinforces the critical nature of disaster recovery planning and testing. CIS Control 11, Data Recovery directly maps to the recommendations in ITIL 5.2.1 regarding the establishment and monitoring of MTRS. The sub-controls of CIS Control 11 recommend a data recovery process which is automated and regularly tested. Whether it's a security incident, flood, fire, or pestilence, both IT service managers and information security practitioners have a significant interest in well-documented and regularly tested recovery plans.

2.2 ITIL 5.2.4: Change Control

The ITIL change control practice aims to maximize the number of successful system changes while minimizing disruption. It does so by recommending a system for assessing the risk of a proposed change and requiring authorization for changes, which are made according to a change schedule (*ITIL Foundations*, 2019). In Gene Kim's *Visible Ops Handbook: Implementing ITIL in 4 Practical and Auditable Steps*, Kim references a culture of change management as a key success factor common to "high performing IT organizations." (Behr, Kim, Spafford, 2013). Table 3 below lists ITIL's change control practice and its associated CIS controls.

ITIL 5.2.4: Change Control	CIS Control 1: Inventory and control of Enterprise assets CIS Control 2: Inventory and control of software assets CIS Control 4: Secure Configuration of Enterprise Assets and Software

Table 3. ITIL's Change Control practice and its associated CIS Controls

ITIL recognizes three change types: Standard Changes (low-risk, pre-authorized, and recorded), Normal Changes (requiring authorization), and Emergency Changes (expedited and often approved by "senior managers who understand the business involved") (*ITIL Foundations*, 2019).

Change control is fundamental to the application of several CIS Controls. The examples below are not an exhaustive list but rather some highlights. CIS Controls 1 and 2, Inventory and Control of Enterprise assets (hardware and software), are required for an effective change control program. Without a baseline inventory of hardware and software assets, organizations cannot determine whether the existence of an asset on the corporate network was authorized, which presents an obstacle to effective systems management. CIS control 4, Secure Configuration of Enterprise Assets and Software recommends that configuration updates are "tracked and approved through configuration management workflow process" for compliance, auditing, and incident response. The detection of system changes, and subsequent determination as to whether or not a change was intentional, is intrinsic to multiple controls. New accounts, system services, and other configuration changes all should be traceable back to a valid request for change.

2.3 ITIL 5.2.5 Incident Management:

Incident management is recommended by both ITIL and the CIS Controls, as shown in table 4 below.

ITIL 5.2.5: Incident Management	CIS Control 17: Incident Response Management

Table 4. ITIL's Incident management practice with its associated CIS Control

ITIL's definition of an incident is "*an unplanned interruption to a service, or the reduction in the quality of a service*" (*ITIL Foundations*, 2019). The recent Colonial Pipeline outage and other news articles describing security incidents affecting broad ranges of organization services are commonplace ("*Ransomware*," n.d.). This onslaught of ransomware attacks makes it imperative that both IT operations staff and security staff prepare for incident response. ITIL's incident management practice recommends the classification and logging of every incident, as well as using a "suitable tool" for storing information about incidents. ITIL recommends that such a tool records several pieces of information, including affected configuration items, known problems, and related incidents. This information, recorded by a well-trained service desk staff, provides an efficient hand-off to the security team when such escalation is needed.

Both ITIL and the CIS controls recommend prioritization of incidents based on impact to the organization. ITIL recommends using an "agreed classification" of incidents to assist with prioritization. CIS Control 19 recommends an "Incident scoring and prioritization schema based on known or potential impact to your organization" (CIS Controls, 2019). Because both ITIL and the CIS controls require documentation of contact information and escalation procedures, development of an incident classification and prioritization schema is an exceptional opportunity for collaboration between IT operations and the security team.

2.4 ITIL 5.2.6 Asset management:

Asset management is critical to both IT service management and information security controls. Table 5 below show ITIL's Asset Management practice with its related CIS Controls.

ITIL 5.2.6: Asset Management:	CIS Control 1: Inventory And Control of Enterprise Assets CIS Control 2: Inventory and Control of Software Assets

Table 5. ITIL's Asset Management practice with its related CIS Controls

The ITIL definition of an IT asset is "any financially valuable component that can contribute to the delivery of an IT product or service (*ITIL Foundations*, 2019)". ITIL uses "IT Asset Management" (ITAM) to include *hardware, software, networking, cloud services, and client devices*… and operational technology, like building monitoring systems and industrial control systems (*ITIL Foundations, 2019*). ITIL advises practitioners to keep an accurate asset register, populated and updated when an asset undergoes a status change, including when it is purchased, put into service, upgraded, or decommissioned. ITIL also suggests integrating the asset database and the Configuration Management Database (CMDB) (*ITIL Foundations*, 2019). CIS Control 1.1 similarly recommends maintaining an accurate inventory of all technology assets. CIS control 2 clearly states that "complete software inventory is critical for preventing attacks" (*CIS Controls*, 2021). Close coordination between the asset management team and the security team provides significant mutual benefit. For example, the asset management team can significantly increase the accuracy of the ITAM database by incorporating information from the CIS Controls 1 and 2, including active/passive asset discovery tools, DHCP log monitoring, and software inventory tools. Alternatively, data from the asset management team, such as a list of newly purchased client machines, facilitates the information security team in differentiating between authorized and unauthorized devices. In cases where triage is necessary, asset management details equip information security staff to make better assumptions about assets than they would without this information.

2.5 ITIL 5.2.7 Monitoring and Event Management

ITIL's Monitoring and Event Management is another practice with a directly related CIS control, as shown in table 6 below.

ITIL 5.2.7: Monitoring and Event Management	CIS Control 8: Audit Log Management

Table 6. ITIL's Monitoring and Event Management practice with its associated CIS Control

Monitoring system logs prepares the IT service management team and the security team for both proactive and reactive activities. Many events of interest are important to both teams. Log collection, management, and alerting is a practice that can add value to the activities in other functional groups, such as the asset management team, identity, and access management team, and the IT service management team. The security team, generally the owner of a Security Information and Event Management (SIEM) or log management system, is equipped to spearhead this collaboration. The ITIL Monitoring and event management practice and CIS Control 8 (Audit Log Management) are almost identical in their application. At a high level, both the CIS Controls and ITIL advise achieving a baseline for logs, as well as configuring alerts for events of particular interest (ITIL Foundations, 2019, and Enclave Security, 2021).

2.6 ITIL 5.2.10 Service Catalog Management:

A service catalog with an associated service configuration document is a powerful enabler of several CIS Controls. In turn, multiple CIS controls support ITIL's Service Catalog and Service Configuration Management practices, as shown in table 7 below.

ITIL 5.2.10 Service Catalog Management and 5.2.11: Service Configuration Management	CIS Controls 1 and 2: Inventory and control of Enterprise and Software assets CIS Control 4: Secure Configuration of Enterprise Assets and Software CIS Control 12: Network Infrastructure Management

Table 7. ITIL's Service Catalog Management and Service Configuration Management practices, and their associated CIS Controls

The ITIL service catalog integrates multiple management practices. A well-drafted provides "a single source of consistent information on all services and service offerings" (*ITIL Foundations*, 2019). ITIL recommends creating the service catalog so that different stakeholder groups can view the information in different ways. For example, a new user seeking to get her Fitbit connected to her company-issued phone has a much different need than a database administrator seeking information on services running on a public-facing web API server. The service catalog is built upon ITIL's service configuration management practice. This practice intends to ensure that "accurate and reliable information about the configuration of services, and configuration items that support them is available when, and where it is needed" (*ITIL Foundations*, 2019).

A service catalog, combined with its service configuration management document, describes a service and then each configuration item that is a dependency for that service. In turn, practitioners document configuration information required for the service in question to run. Figure 1 below is a screenshot from iTop (2021), a free, open-source IT service management software solution. Figure 1 below from the iTop demo site is an example of how a dependency chart might look.

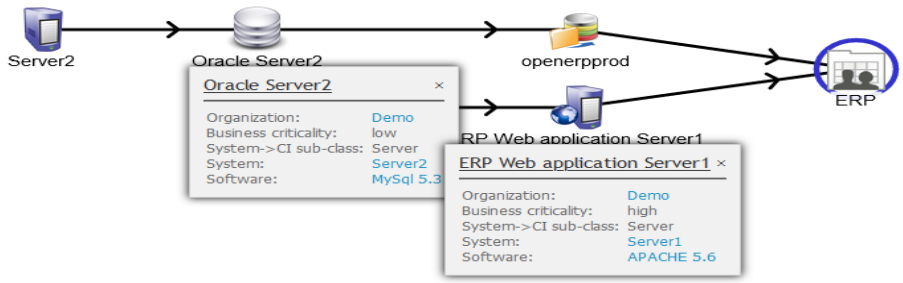

Figure 1. Visualization of service catalog dependencies

The diagram in Figure 1 represents a high-level view of a system. Each dependency should have information regarding network ports, protocols, configuration files, and other pertinent information. As indicated by the reference to multiple CIS controls in table 7 above, Information security teams can utilize this information to make hypotheses about which services and network traffic patterns are expected and which ones are not. Reaching out to the IT operations team to test these hypotheses is an opportunity for fruitful collaboration.

3. Systems documentation and auditing

This paper uses two tools to demonstrate systems documentation and auditing methods: iTop ITSM software and an instance of Elastic SIEM. A comprehensive demonstration of the capabilities of ITSM software or SIEM systems for supporting ITIL and the CIS controls is beyond the scope of this paper. There are, however, examples in the following sections which demonstrate the benefit of using such systems.

iTop is free and open-source ITIL-focused service management software. It is well-documented, and operators can create a systems documentation framework in a short period of time. After this high-level skeleton is in place, stakeholders such as project managers, system owners, and IT staff can add configuration items and documentation to attain the level of desired detail needed. Future iterations of

documentation provide opportunities for continual improvement of IT service management effectiveness and information systems resilience.

Elastic, also known as "ELK," is a popular data analysis platform proven to be a capable SIEM system. "ELK" is an acronym for the names of the three major technologies making up the platform: Elasticsearch, Logstash, and Kibana. Justin Henderson's SANS course SEC 555: SIEM with Tactical Analysis leverages an Elastic SIEM for its demonstrations. Demonstrations in section 3 employ concepts from SEC 555 and the virtual machine provided as part of the course.

3.1 Business systems documentation

iTop provides the capability to document the ITIL management practices and CIS controls outlined in this paper. Demonstrating business architecture documentation highlights the utility of ITSM software for supporting both ITSM and security controls implementation. Existing controls can be entered as configuration items, and any new controls can be entered as change management items. The example below demonstrates documentation of ITIL's architecture management practice using iTop:

iTop (2021) uses the term "Business Process" to describe top-level configuration items. In Figure 2 below, "Revenue and reporting" is the highest-level configuration item. Once a business process is defined, a hierarchy of configuration items and dependencies is underneath. Practitioners can link an unlimited number of documents or sub-items to each node in the diagram below.

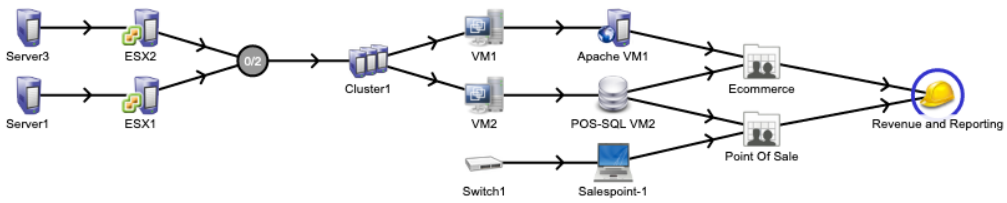

Figure 2. iTop's "Depends On" view for the Revenue and Reporting node

As practitioners add assets to iTop, they can identify and document dependencies and services. In Figure 2 above, both "Ecommerce" and "Point Of Sale" are "application solutions" in iTop. These nodes typically include high-level documents such as requests for proposals, contracts, and system owner information. To the left of application solutions in this diagram are either servers, databases, networking equipment, or points of sale. As technicians add software and hardware assets into iTop, they are visible in charts such as this one. Each node in the diagram is clickable, which provides a higher level of detail. When change management tickets or incident tickets are entered into iTop, the visualization changes, presenting clickable links to the asset and associated incidents, problems, or change requests. The tooltip shown in figure 3 below contains links to the asset, Incident I-000003, and other related items.

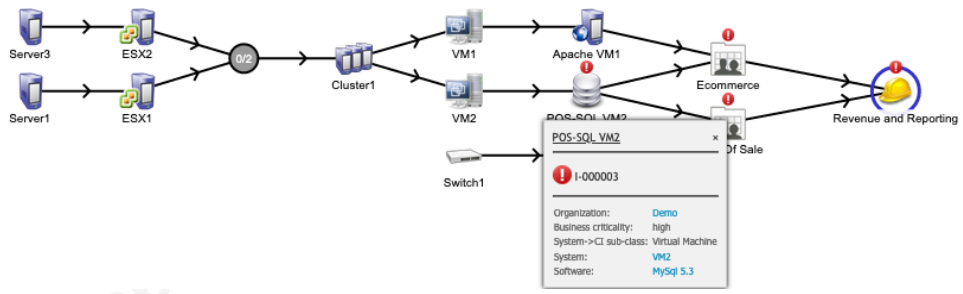

Figure 3. The dependency chart view affected by an incident.

The diagrams above represent a "first pass" at documenting a single piece of business architecture and its associated systems. As hardware and software assets are added to the database, a more detailed picture is created, providing valuable information for executive management, security teams, IT operations. Likely configuration items for a "second pass" through this business architecture would be network switches and firewalls, which each contain configuration documentation.

3.2 Auditing

Auditing examples in this section support a broad range of ITIL management practices and CIS Controls. Auditing concepts and a sample view will be provided, with details of management practices and CIS Controls that the information supports listed afterward.

3.2.1: Dynamic Host Configuration Protocol (DHCP) logs

DHCP logs help infosec and IT staff discover assets as they are added to the network. Being easy to ingest into a SIEM and easy to understand, DHCP logs are an accessible item to monitor for anomalies in either hostnames or mac address fields. In figure 4 below, it is easy to see that "Gamer17.sec555.com" has a hostname that doesn't appear to fit with the organizational naming convention and that the Organizationally Unique Identifier (OUI) portion of the mac address differs from the other hosts in the table. These two factors indicate that Gamer17 is likely not a system configured by the sec555.com organization.

Hostname	Mac address	IP address	Count
GAMER17.sec555.com	842B2B509FB9	192.168.4.54	7
IT01.sec555.com	000C29864EFC	192.168.1.81	2
IT02.sec555.com	000C2929DF23	192.168.1.50	2
IT03.sec555.com	000C29128B03	192.168.1.51	3
deathstar.sec555.com	000C296AD09D	192.168.1.52	1
doc01.sec555.com	000C296F5161	192.168.4.50	4
doc02.sec555.com	000C298892DE	192.168.4.51	4
doc03.sec555.com	000C2977CD80	192.168.4.52	4

Figure 4. Dhcp logs from Sec555, Lab 4

Because "deathstar.sec555.com" has a hostname that doesn't fit either the ITxx.sec555.com or docxx.sec555.com naming convention, it might also be a system worth investigating. IT and infosec staff who require DHCP reservations for all hosts

will benefit from receiving alerts when a host is assigned an address from the DHCP pool without a reservation. A sample script for this purpose is included in Appendix 3.

The examples detailed above provide the opportunity for three responses: If the host in question is foreign to the organization, staff should open a security incident so that the host can be removed from the network, and its activities can be analyzed. If the host in question is simply misconfigured, the misconfiguration can be fixed, and the host can be added to the asset database. If the host in question represents a new naming convention or new Organizationally Unique Identifier OUI for the organization, systems documentation can be updated to reflect the changes. These actions support the ITIL Architecture management practice, Asset Management practice, and CIS Control 1: Inventory and control of hardware assets.

3.2.2 Nagios logs

Nagios is a popular free and open-source monitoring solution ("industry standard in IT infrastructure monitoring," n.d.). It is commonly used to monitor availability of systems. The pie chart below represents the distribution of all available Nagios states for an asset group for a period of time. It provides a snapshot of the overall availability for the group of assets. Nagios provides a wealth of information for availability management. Visualizations such as the one in Figure 5 below are helpful for auditing both ITIL's availability management practice and ensuring that the data recovery testing recommended by CIS control 11: Data Recovery is being performed.

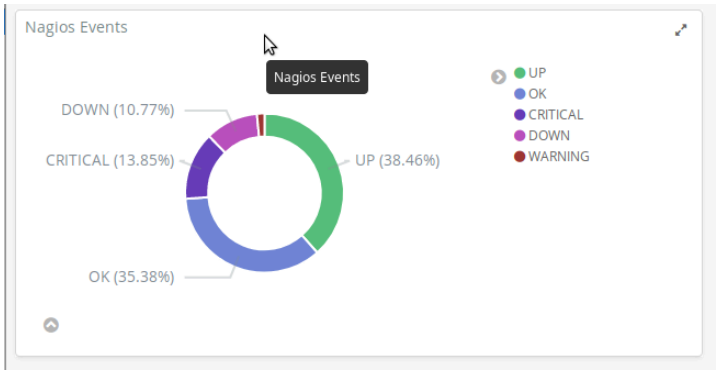

Figure 5. Availability visualization using Nagios logs

3.2.3: Network device logs

Network device logs generally contain information regarding changes to the device. In figures 6 and 7 below, examples of such changes can be seen.

Time	id	usr	msg
April 13th 2021, 20:53:10.258	firewall	Administrator	Configuration changed: Member in Address Group by user Administrator
April 13th 2021, 20:53:10.258	firewall	Administrator	Configuration changed: Address Object in Group by user Administrator
April 13th 2021, 20:53:10.257	firewall	Administrator	Configuration changed: Local User To Group Object Dependency by user Administrator

Figure 6. configuration changes recorded in a firewall log

Time	id	usr	msg	m	note
April 13th 2021, 20:53:10.245	firewall	FWAdmin	Access rule added	440	Allow 'Any' from 'LAN Subnets' to 'Corp Lan'
April 13th 2021, 20:53:10.245	firewall	FWAdmin	Access rule modified	441	Allow 'Any' from '(GMS) CorpLAN (VPN)' to 'LAN Subnets'
April 13th 2021, 20:53:10.245	firewall	FWAdmin	Access rule added	440	Allow 'Any' from 'Corp Lan' to 'LAN Subnets'
April 13th 2021, 20:53:10.245	firewall	FWAdmin	Access rule modified	441	Allow 'Any' from 'LAN Subnets' to '(GMS) CorpLAN (VPN)'
April 13th 2021, 20:53:10.244	firewall	FWAdmin	Access rule added	440	Allow 'Any' from 'Scanning Subnets' to 'SecureSvrsGrp (VPN)'
April 13th 2021, 20:53:10.244	firewall	FWAdmin	Access rule added	440	Allow 'Any' from 'FinanceServers' to 'Secure Subnets'

Figure 7. Access control list modification logs

Both Figures 6 and 7 above indicate changes to permitted network traffic. To audit these configuration changes, the actions detailed above should be compared to change requests to ensure that they are approved changes. If they do not represent approved changes, operational staff can investigate the change in question, and reverse it if it is not appropriate for the environment.

Auditing events such as those described above and comparing them to change requests is applicable to many of the CIS Controls and ITIL management practices outlined in this paper. A change in permitted network traffic without an associated change request and update to systems documentation might represent an undocumented architecture change, emergency change for troubleshooting purposes, or malicious intent. This auditing example supports ITIL's architecture management, service management, and change management practices, and maps directly to CIS Controls 4: Secure Configuration of Enterprise Assets and Software, and 12: Network Infrastructure Management.

3.2.4 AppLocker logs

AppLocker is Microsoft's built-in application allowlisting offering. Because configuring an allowlisting solution to block unapproved applications from running can be a large undertaking, many organizations elect to leave AppLocker in audit mode and send logs to a SIEM. Figure 8 below demonstrates multiple pieces of software that would have been prohibited if AppLocker was running in block mode.

Time	hostname	appname	msg
June 5th 2021, 07:36:07.117	PC0002.corp.viamonstra.com	%SYSTEM32%\NOTEPAD.EXE	was allowed to run but would have been prevented from running if the AppLocker policy were enforced.
June 5th 2021, 07:36:07.115	PC0002.corp.viamonstra.com	%SYSTEM32%\DLLHOST.EXE	was allowed to run but would have been prevented from running if the AppLocker policy were enforced.
June 5th 2021, 07:36:07.113	PC0002.corp.viamonstra.com	%OSDRIVE%\USERS\ADMINISTRATOR.VIAMONSTRA\DESKTOP\ADKSETUP(1).EXE	was allowed to run but would have been prevented from running if the AppLocker policy were enforced.
June 5th 2021, 07:36:07.113	PC0002.corp.viamonstra.com	%SYSTEM32%\DLLHOST.EXE	was allowed to run but would have been prevented from running if the AppLocker policy were enforced.
June 5th 2021, 07:36:07.112	PC0002.corp.viamonstra.com	%SYSTEM32%\MMC.EXE	was allowed to run but would have been prevented from running if the AppLocker policy were enforced.

Figure 8. AppLocker log in Kibana

Information obtained from AppLocker logs such as this is invaluable for both IT operations and security staff. This auditing information supports ITIL's asset management practice, as well as CIS Control 2: Inventory and control of software assets.

As seen in the auditing examples in section 3, several auditing techniques are applicable to assessing compliance with ITIL practices, and the CIS Controls. The examples above are a small subset of the possible auditing procedures which can provide value for both IT operations and security specialists. For several of the events highlighted in this paper's auditing recommendations, there is ambiguity about whether the events in question represent business as usual, rogue administrative activity, or malicious intent. The most effective way to differentiate among these is to view them in the context of systems documentation consisting of asset management, configuration management, and change control.

4. Conclusion

IT service managers and information security practitioners rely on shared principles: Asset identification, configuration standards, and change management. These shared principles compel administrators to build well-defined standard operating procedures and follow them at every point in a system's lifecycle. Developing procedures from shared principles creates a "True North" vision which accelerates accomplishment for both security and IT operations teams. The concept of "True North" vision, popularized by Stephen Covey in *The 7 Habits Of Highly Effective People* (1989) is often cited as a primary indicator of organizational success. When security and operations teams understand a shared a set of principles in this way, they can build procedures which enable the organization to be adaptable and resilient.

Two tables are included as appendices to this paper. Appendix A lists mappings of ITIL practices and CIS controls from the ITIL perspective. Appendix B lists mappings from the CIS Controls perspective. Although the CIS controls are a suitable fit for mapping to ITIL controls, there are myriad opportunities to create synergy between the application of ITIL practices and any security framework. Such endeavors help organizations manage information systems in secure, resilient ways. These mapping exercises can help blend security and operations so that all stakeholders involved recognize that there is little difference between carefully and meticulously managed IT systems and securely managed IT systems. This collaboration leads to a more gratifying, secure, and sustainable workplace.

Kevin T. Geil, info@placidsecurity.com

References

Axelos. (2019). ITIL Foundation. Stationery Office Books (TSO).

Behr, K., Kim, G., & Spafford, G. (2005). The visible ops handbook: Implementing ITIL in 4 practical and Auditable steps. Information Technology Process inst.

Center for Internet Security. (2021, May). CIS Controls Version 8.

Covey, S. R. (1997). The seven habits of highly effective people: Restoring the character ethic. Macmillan Reference USA.

Enclave Security, LLC. (March, 2021). SEC566 | Implementing and Auditing the Critical Security Controls In Depth. SANS Institute.

Henderson, J. (2020, November). SIEM training | SIEM with tactical analysis | SANS SEC555. Cyber Security Training | SANS Courses, Certifications & Research. https://www.sans.org/cyber-security-courses/siem-with-tactical-analytics/

How ITIL started. (2013, February 11). IBPI http://www.ibpi.org. https://internationalbestpracticeinstitute.wordpress.com/2013/02/11/how-itil-started/

The industry standard in IT infrastructure monitoring. (n.d.). Nagios. https://www.nagios.org/

iTop documentation. (2020, April 8). iTop Hub is the ITSM & CMDB open source community toolset. https://www.itophub.io/wiki/page

Kim, G., Humble, J., Debois, P., & Willis, J. (2016). The DevOps handbook:: How to create world-class agility, reliability, and security in technology organizations. IT Revolution.

Rae, B.https://documents.bmc.com/products/documents/22/04/522204/522204.pdf

Ransomware. (n.d.). WIRED. https://www.wired.com/tag/ransomware/

Watts, S. (2021, March 22). ITSM frameworks explained: Which are most popular? CompTIA. https://www.comptia.org/blog/itsm-frameworks-explained-which-are-most-popular

Kevin T. Geil, info@placidsecurity.com

What is IT service management? | ITIL | AXELOS. (n.d.). Global Best Practice Solutions | AXELOS. https://www.axelos.com/best-practice-solutions/itil/what-is-it-service-management

Appendix A:
ITIL Management Practices and Associated CIS Controls

ITIL 5.1.1: Architecture management	CIS Control 1: Inventory and Control of Enterprise Assets CIS Control 2: Inventory and Control of Software Assets CIS Control 4: Secure Configuration of Enterprise Assets and Software
ITIL 5.2.1. Availability Management	CIS Control 8: Audit Log Management CIS Control 11: Data Recovery
ITIL 5.2.4: Change Control	CIS Control 1: Inventory and control of Enterprise assets CIS Control 2: Inventory and control of software assets CIS Control 4: Secure Configuration of Enterprise Assets and Software
ITIL 5.2.5: Incident Management	CIS Control 17: Incident Response Management
ITIL 5.2.6: Asset Management:	CIS Control 1: Inventory And Control of Enterprise Assets CIS Control 2: Inventory and Control of Software Assets
ITIL 5.2.7: Monitoring and Event Management	CIS Control 8: Audit Log Management
ITIL 5.2.10 Service Catalog Management and **ITIL 5.2.11**: Service Configuration Management	CIS Controls 1 and 2: Inventory and control of Enterprise and Software assets CIS Control 4: Secure Configuration of Enterprise Assets and Software

Kevin T. Geil, info@placidsecurity.com

	CIS Control 12: Network Infrastructure Management

Appendix B:
CIS Controls and Associated ITIL Management Practices

CIS Control 1: Inventory and Control of Enterprise Assets	ITIL 5.1.1: Architecture management ITIL 5.2.10 Service Catalog Management ITIL 5.2.11: Service Configuration Management ITIL 5.2.4: Change Control ITIL 5.2.6: Asset Management:
CIS Control 2: Inventory and Control of Software Assets	ITIL 5.1.1: Architecture management ITIL 5.2.4: Change Control ITIL 5.2.6: Asset Management:
CIS Control 3: Data Protection	
CIS Control 4: Secure Configuration of Enterprise Assets and Software	ITIL 5.1.1: Architecture management ITIL 5.2.10 Service Catalog Management ITIL 5.2.11: Service Configuration Management ITIL 5.2.4: Change Control
CIS Control 5: Account Management	
CIS Control 6: Access Control Management	
CIS Control 7: Continuous Vulnerability Management	
CIS Control 8: Audit Log Management	ITIL 5.2.1. Availability Management ITIL 5.2.7: Monitoring and Event Management
CIS Control 9: Email and Web Browser Protections	
CIS Control 10: Malware Defenses	
CIS Control 11: Data Recovery	
CIS Control 12: Network Infrastructure Management	ITIL 5.2.10 Service Catalog Management ITIL 5.2.11: Service Configuration Management
CIS Control 13: Network Monitoring and Defense	
CIS Control 14: Security Awareness and Skills Training	
CIS Control 15: Service Provider Management	
CIS Control 16: Application Software Security	
CIS Control 17: Incident Response Management	ITIL 5.2.5: Incident Management
CSI Control 18: Penetration Testing	

Appendix C:
Send-DHCPAlert DHCP Monitoring Script

```
<#
    .SYNOPSIS
      Sends alerts when a DHCP lease has been issued without a reservation.
The user that runs the script needs to be a member of the AD DHCP Users group.
    .Example
      DHCPEmail -DhcpServer MyDHCPServer -scope 10.50.0.0 -SMTPServer
MySMTPServer -FromEmail monitoring@example.org -ToEmail
admin1@example.org,admin2@example.org

#>

param($DhcpServer,$scope, $SMTPServer,$FromEmail,$ToEmail,$LogFilePath)

function Send-DhcpAlert ($DhcpServer, $scope, $SMTPServer, $FromEmail,
$ToEmail, $LogFilePath) {
$Header = @"
<style>
TABLE {border-width: 1px; border-style: solid; border-color: black; border-
collapse: collapse;}
TH {border-width: 1px; padding: 3px; border-style: solid; border-color: black;}
TD {border-width: 1px; padding: 3px; border-style: solid; border-color: black;}
</style>
"@
  $datetime= Get-Date #| Out-String
  $LeaseInfo = Get-DhcpServerv4Lease -scopeID $scope -ComputerName $DhcpServer
| select -Property ClientID, Hostname, AddressState | where {$_.AddressState -
eq "Active"}
  $LeaseInfo.ClientID = $LeaseInfo.ClientID -replace '-',''
  $Body = $LeaseInfo | ConvertTo-Html -Head $Header
  IF (!$LogFilePath) {$LogFilePath = (Get-Item -Path ".\").FullName}
      IF ($LeaseInfo)
      {
          Send-MailMessage  -SmtpServer $SMTPServer -From $FromEmail -To
$ToEmail -Subject "DHCP Lease without Reservation Detected" -BodyAsHtml "$Body"
              ForEach($_ in $leaseinfo)
                  {"$datetime DHCP Lease without Reservation Detected $_" |
Out-File -Append -FilePath $LogFilePath\dhcpscript.log}
      }
      Else
      {
```

Kevin T. Geil, info@placidsecurity.com

```
        "$datetime  No non-reserved dhcp leases detected for $dhcpserver for
scope $scope" | Out-File -Append -FilePath $LogFilePath\dhcpscript.log
      }
}

Send-DhcpAlert -DhcpServer $DhcpServer -scope $scope -SMTPServer $SMTPServer -
FromEmail $FromEmail -ToEmail $ToEmail -LogFilePath $LogFilePath
```

Kevin T. Geil, info@placidsecurity.com

Kevin T. Geil, info@placidsecurity.com