Information Technology Governance, Risk, and Compliance in Healthcare

cloud security alliance®

The permanent and official location for the Health Information Management Working Group research is: https://cloudsecurityalliance.org/research/working-groups/health-information-management/

Acknowledgments

Lead Author:

Dr. James Angle

Contributors:

Michael Roza

CSA Global Staff:

Vince Campitelli
Alex Kaluza
Claire Lehnert (Design)
AnnMarie Ulskey (Cover)

The CSA's Health Information Management Working Group aims to directly influence how health information service providers deliver secure cloud solutions (services, transport, applications, and storage) to their clients, and foster cloud awareness within all aspects of healthcare and related industries. The working group research was and will continue to be freely available for use without license fees or restrictions by the CSA.

Table of Contents

Abstract

Information Technology (IT) Governance, Risk, and Compliance (GRC) are three words that significantly impact organizations. While each term seems straightforward, putting them together creates a concept that is difficult to understand and even harder to implement. Essentially, GRC includes policies and procedures to manage organizational processes that align management and control of information with business objectives, organizational risk tolerance, and guidance for complying with regulations and managing risk. Highlighting each GRC term and integrating them into a singular GRC program provides a structured process to ensure IT supports business objectives while managing risk and compliance. This paper will convey how to create a program for each GRC component and integrate them into one cohesive plan.

Introduction

Healthcare Delivery Organizations (HDOs) are in the grip of a digital revolution. This trend started years ago when HDOs began digitizing health records, and it continued with increasing demand for business and health data. Additionally, the recent COVID-19 pandemic escalated demand for data and accelerated telehealth development. HDOs ability to manage this data and associated processes is essential. Developing and implementing an IT Governance, Risk, and Compliance program underscores an HDOs commitment to managing information and risk while complying with applicable laws and regulations. The following figure shows the GRC process:

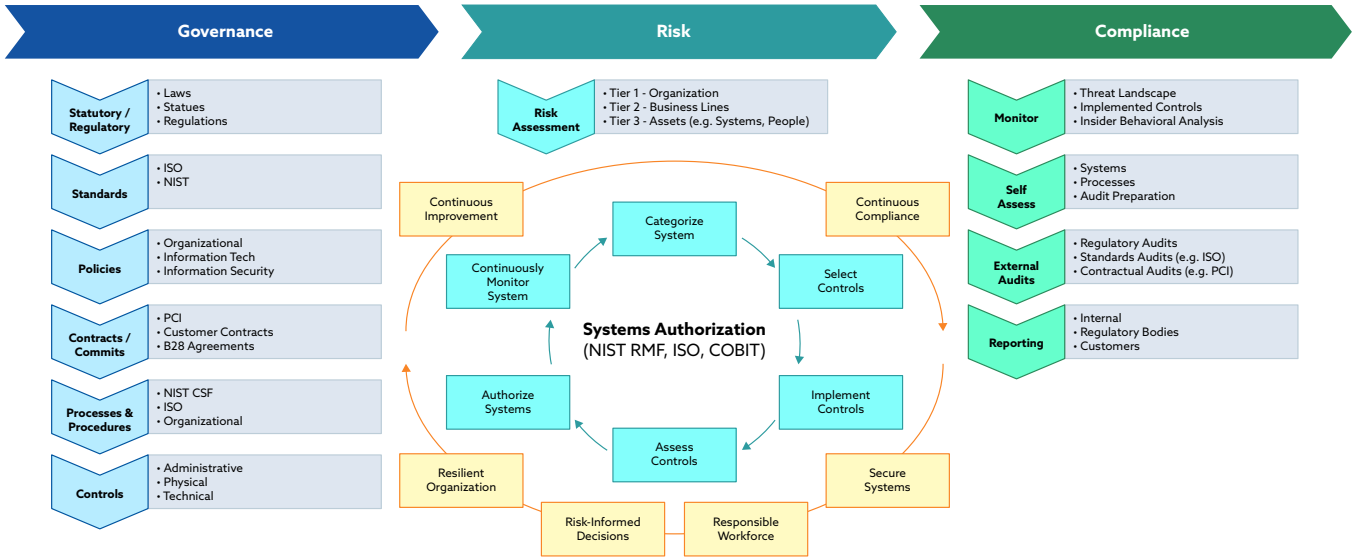

Figure 1 GRC Process

A good GRC program will provide the following benefits:

- Improve patient quality of care.
- Improve data quality, resulting in improved public health.
- Increases operational efficiency and effectiveness.
- Allows HDOs to make risk-based decisions and manage their risk (American Health Information Management Association, 2014).

Governance, risk, and compliance management allow organizations to gather vital risk data, manage risks while ensuring and validating compliance, and report results to management. This data enables management to set budgets, make risk-based decisions, and manage compliance. Additionally, a GRC program illuminates an HDO's risk and compliance postures—empowering leadership to make prudent risk-based decisions regarding resource allocation and risk mitigation throughout the data lifecycle.

Healthcare delivery organizations have a wide range of data types that must be managed. For example, HDOs collect, store, and process Personally Identifiable Information (PII), Payment Card Industry (PCI) data, and Protected Health Information (PHI)—all of which have different regulatory requirements.

An effective GRC program allows HDOs to integrate risk and compliance with business processes.

- Governance is the management approach through which executives direct and control the entire organization, using a combination of management information and hierarchical management control structures.
- Risk Management is the set of processes used to identify, analyze, and (where necessary) respond to risks that might affect the realization of the organization›s core business functions.
- Compliance means conforming to stated requirements, as defined by laws, regulations, standards, contracts, strategies, and policies (Secure Digital Solutions, 2014).

During the current COVID-19 pandemic, the rules governing telehealth have changed dramatically. Healthcare delivery organizations hoping to track and comply with these changes require an effective GRC program. The need for an effective GRC program is essential for HDOs navigating through the pandemic recovery period—especially considering rapidly evolving demands and regulatory requirements for big data analytics and telehealth. An established GRC process can ensure seamless adherence to new requirements while maintaining the current risk posture. This paper will examine governance, risk, and compliance separately and then explain how to integrate them into a cohesive GRC program. While a complete GRC program covers the entire HDO and all its business processes, this paper focuses on GRC as it relates to information technology.

Governance

Information governance defines the structure, policies, procedures, laws, and regulations to which HDOs must adhere. Information governance seeks to extract value from information and how it is managed throughout the data lifecycle. Data lifecycle management is critical because, over time, the data value may decline; however, data storage costs and exposure risks do not. When reviewing data lifecycles, it is useful to use terms defined in cloud computing. Standard data lifecycle[1] terms include:

1. Create: When new data is created or when existing data is modified.
2. Store: Data is committed to a storage repository.
3. Use: When data is processed, viewed, or used in any activity.
4. Share: Data or information made accessible to others.
5. Archive: Data placed in long-term storage.
6. Destruction: When data is no longer required, it is physically destroyed.

Create

The data lifecycle's first phase is creation or modification. Healthcare delivery organizations create and collect various data regarding numerous topics, such as financial, supply chain, human resources, and patient care. The critical governance factors in this stage include a consideration of the following questions:

1. How is the data created, collected, or modified? Is the data produced by an external source (i.e., a new patient or employee entering the initial data)? Is it created by compiling data for other data sources? Is it collected by keyboard entry, mobile application, or combining data? The HDO must know the origins of all data.
2. What will the data be used for? This query is essential for HDOs, as PII and PHI laws require HDOs to inform data subjects of the reasons for data collection.
3. Who can create or collect the data? Identifying who can produce or collect data is particularly essential when data contains PHI. The "who" in this equation reflects on the integrity of the data.
4. What is the data classification and categorization? Data classification relates to confidentiality requirements for data types. For example, data may be designated for internal use only, business-sensitive, or PHI-sensitive. "Categorization" defined in Federal Information Processing Standards (FIPS) 199 establishes three potential levels of impact: "low," "moderate," and "high." These levels are relevant to information security and information systems for each of three stated security objectives: "confidentiality," "integrity," and "availability" (Stine, Kissel, Barker, Fahlsing, and Gulick, 2008).

Understanding data sources will enable organizations to build a solid governance foundation.

[1] https://cloudsecurityalliance.org/artifacts/telehealth-risk-management/

Store

Healthcare delivery organization storage management policies should enable HDOs to manage storage resources effectively while complying with applicable laws and regulations. However, before HDOs can determine storage requirements, they must understand how much and what type of data they are storing. The following questions can help start the conversation regarding storage:

1. Where will the data be stored? Will it be in the cloud, an enterprise data center, locally stored, or on removable media? Each has different requirements, and HDOs should consider the implications for each type of storage.
2. For cloud-based data, where is it stored? It is vital to know where data is stored (both primary and backup information). Is the data stored offshore? The regulatory requirements may be different depending on the storage locations.
3. How long will the data be required? Retention requirements may determine storage methods.
4. Is there a requirement for encrypting data at rest? Due to data sensitivity needs, there may be a regulatory or business requirement for encryption.

Knowing what data is being stored, where it is stored, and how long it is required will enable HDOs to create appropriate policies and procedures for data storage.

Use

As data collection increases in speed and scale, the analytic techniques used to process these datasets become more sophisticated, and the data usage becomes more varied. Big data analytics will continue to expand health data usage—including considerable potential for application in health research. However, proper care must be taken to prevent data loss or misuse. Data governance in healthcare strives to enable positive outcomes and prevent negative consequences. Additionally, transparency presents a complex challenge for healthcare data governance. Healthcare delivery organizations must be transparent in how they use data while maintaining privacy and security.

The first step to using data is to understand the data and how it will be used. Healthcare delivery organizations must know the answers to the following questions:

1. Who is the user of the data?
2. What is the purpose of the data, and how will it be used?
3. Is that use appropriate (based on data type and regulatory requirements)?
4. How will the data be used in the future?

To answer these questions, HDOs must classify and categorize data. Gaining a complete understanding of the data and its users will aid in implementing controls that efficiently and effectively protect it. Additionally, HDOs must understand how data will be used.

Share

For years, HDOs built "stovepipe" data repositories where data was confined and isolated. The use of these stovepipe systems encouraged data duplication (rather than sharing). Good data governance can provide the processes required to share data effectively. Healthcare delivery organizations cannot be confident that shared data and information is current, correct, relevant, and secure without effective data governance. Data governance will enable HDOs to develop policies and procedures that define what data can and should be shared. Additionally, governance should clearly articulate who the data can be shared with, the reasons for sharing data, the methodology for sharing data (email, internet, cloud, etc.), and the process requirements for securing data that is to be shared.

Archive

Data no longer in active use can and should be destroyed or archived, depending on future needs and regulatory requirements. It is critical to understand whether data requires long-term data archiving, as this step carries considerable financial and technical hurdles. Healthcare delivery organizations create highly regulated data with requirements to maintain data for several years. As stated, data storage is expensive. Archiving data reduces storage costs, and long-term storage is cheaper than short-term. While HDOs cannot control data growth rates, they can plan for efficient archiving solutions that provide for future access needs and cost savings.

A thorough data governance strategy that includes an archiving solution can aid in regulatory compliance endeavors and enable data access and retrieval. However, archiving data requires an approach that allows for different retention periods (DataArchiva, 2018). Therefore, HDOs must learn data retention requirements, as they may range from a few years to 25-plus years.

Destruction

Laws and regulations—such as the Health Insurance Portability and Accountability Act (HIPAA)—demonstrate the need for effective planning to manage the robust data volumes that HDOs create, process, and store. As a result, HDOs must implement information governance policies that minimize liabilities, improve operations, and reduce expenses.

Often, one overlooked aspect of information governance is data destruction. The need for clear, concise policies and procedures regarding data destruction of outdated, restricted information is greater than ever—especially with the exponential growth of data collection (particularly with cloud-based information).

Addressing these problems requires effective and defensible data destruction policies, including answers to the following queries:

> - Who is responsible for data destruction?
> - How can you minimize and streamline repositories for information to help avoid searching multiple locations for the same data?
> - How often should you scan for space-depleting items for potential deletion?

- What destruction measures are in place to ensure data is truly gone and unrecoverable?
- Are data in litigation-hold maintained in that state until the conclusion of the hold (Crosbie, 2020)?

Then there is the question of how to ensure cloud data is destroyed? Cloud data can be stored in a multi-tenant environment, so media cannot be eliminated without destroying the other tenant›s data. The most effective way to ensure data destruction is to encrypt the data. Then, when the data is no longer required, destroy the keys. While the data is still physically in the cloud, it can never be used (Gillin, 2019). Regarding this method: the HDO must ensure that each tenant has different keys for encryption through contractual obligations.

An additional aspect of data destruction is asset disposal. When an asset is no longer required, is the data on the asset properly destroyed? Has the physical storage capability been removed, and the data destroyed? Part of the destruction policy must identify the procedures for ensuring all sensitive data are destroyed.

Risk Management

Before moving to cybersecurity risks, it is necessary to first define what "risk" means. Instead of defining risk in technical terms, cybersecurity professionals—when speaking to executives—can adopt the definition of risk used by almost every business manager and board of directors: the potential for monetary loss. In this context, "risk" is the possibility that an event will lead to reduced profitability. Therefore, a cyber event causing damage to an HDO's brand or reputation can be quantified. As a result, the crucial question is: how much does a cyber event ultimately cost the HDO (Gundert, 2020)?

Cybersecurity risk is a subset of "business risks" and, as such, should be talked about in business terms. As a result, HDOs should view "information risks" in the context of "organizational risks." When HDOs implement information security controls, their goal is to reduce risk. Since no information system is 100 percent secure, the control aims to minimize risk to an acceptable level (as defined by HDO leadership). This concept is often expressed as the organization›s risk appetite and risk tolerance.

Risk Appetite

Risk appetite is the tolerance level organizations have for risk. One aspect of this is understanding how much risk an organization is willing to tolerate, while another is thinking about how much an organization is willing to invest or spend to manage the risk.

Risk Tolerance

Risk tolerance is the level of risk or degree of uncertainty acceptable to organizations and is a vital element of organizational risk frames. An organization's risk tolerance level is the amount of data and systems that can be risked to an acceptable level. Having a defined risk tolerance level means

the security program understands the degree that management requires the organization to be protected against confidentiality, integrity, or availability compromises.

To build a sound cyber defense, HDOs must understand their appetite and tolerance for risk. Cybersecurity risk is derived from threats and vulnerabilities, and how its effects are evaluated and measured likelihood, and impact then summarized and reported in a risk profile.

Threats

A threat is any circumstance or event with the potential to adversely impact organizational operations, assets, individuals, or other organizations through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

When threats are identified, threats can be modeled, developed, and analyzed. Threat events for cyber or physical attacks are characterized by the tactics, techniques, and procedures employed. Understanding threat events gives HDOs insights into the capabilities associated with specific threat sources. Additionally, knowing the intent and targeting aspects of a potential attack helps HDOs narrow the set of the most relevant threat events (National Institute of Standards and Technology, 2012).

Cybersecurity professionals should never take action on a threat before understanding whether it represents a risk to an HDO. When HDOs address threats that do not pose a genuine risk (or are only minor risks), they expend unnecessary resources and may miss opportunities to address serious threats (Gundert, 2020).

Vulnerability

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation exploitable by a threat source (National Institute of Standards and Technology, 2012). A vulnerability does not mean an attacker will use it; it simply means there is a risk. Without an exploit, a vulnerability is a potential problem (Haber and Hibbert, 2018). Vulnerabilities within information systems can be found in organizational governance structures, environments, and external relationships.

Examples of different vulnerabilities include:

1. Physical: unlocked rooms containing switches
2. Environmental: flooding
3. External relationships: telecommunications outage

Risks occur when threat events take advantage of vulnerabilities. Therefore, healthcare delivery organizations should use threat models to show how exploiting a vulnerability by a threat source can result in a monetary loss to an HDO. For example, an employee (insider threat) can download sensitive data (vulnerability, weak control) and provide the data to a competitor.

Likelihood

Simply stated, likelihood is the probability an event will happen, while probability measures the likelihood or chance of an uncertain event. The assignment of numbers to represent the probability of an event is based on the work of the Russian mathematician Andrey Kolmogorov.

The first probability axiom is $0 \leq P(E_i) \leq 1$ The probability that an event (E_i) will happen is assigned a number between 0 and 1 inclusive, with "0" representing absolute certainty the event will not occur and "1" representing complete certainty the event will occur. The second axion is $\sum P(E_i) = 1$ The sum of the probabilities assigned to any set of mutually exclusive and collectively exhaustive events is "1". For example, if the probability in a fair die toss is .17 of hitting a specific number, then the probability of not hitting that number is .83 (the two probabilities .17+.83 =1.)

In a risk analysis, determining the likelihood of a threat exploiting a vulnerability considers multiple factors. The risk analyst reviews threat intelligence to understand threat capabilities, motivations, exploitability, and implemented controls and uses this information when determining the likelihood of occurrence. The analyst must ask and answer the following questions to estimate the likelihood of occurrence:

1. Is there an exploit available?
    a. What are the technical skills required to execute the exploit? Can someone execute it without technical knowledge, or does it require advanced skills?
    b. Can the exploit be executed remotely?
2. What is the motive?
    a. Is the threat from an activist?
    b. Is the exploit for profit?
3. Are there controls in place to mitigate the vulnerability?

The answer to these questions gives the analyst an understanding of the probability of an exploit.

Since the answers lead to qualitative analysis, the analyst can use something (like the table below) to add values to the assessment.

Probability Table		
Likelihood of Occurrence		
Relative	**Numeric**	**Description**
Very Low	0.1	Highly Unlikely
Low	0.3	Unlikely
Moderate	0.5	Somewhat Likely
High	0.7	Highly Likely
Very High	0.9	Almost Certain

Table 1 Probability Values

Impact

In addition to likelihood, a relevant factor is impact. Impact helps categorize and prioritize risk. Some risks have a high impact but infrequently occur, while others may have a moderate impact but occur with greater frequency (Thorhallsdottir, 2018). The impact of a threat is the magnitude of the harm that can occur if the threat is realized.

Healthcare delivery organizations should explicitly define how they are impacted by potential adverse activities, such as a breach. The HDOs should determine impact based on the data affected, as this may cause HDOs to experience different impacts with the same event. For example, the impact on a system containing public releasable information is much less than the impact on a system containing sensitive information.

Risk Profile

The information risk profile should include a current-state analysis of identified information risk factors that have a reasonably high probability of occurrence and would represent a material impact on HDO operations if realized. Risk descriptions should be brief and expressed in language that is recognized and understood by both business and technology leaders.

The current-state representation should also include the HDO's risk management views, expectations, and requirements. This representation should consist of identification and analysis of the opinions of business leaders and stakeholders, their views on information risks and security, a description of current business conditions, current threat and vulnerability analysis outcomes, and expectations of external parties (i.e., customers, partners, vendors, and regulators).

Healthcare delivery organizations have numerous business processes but also limited resources and bandwidth to protect them. Therefore, it is vital to identify the most critical business processes and capabilities within the information risk profile—those that (if impacted negatively) could cause a material impact on HDO operations.

Information values are often misunderstood and based on subjective perceptions of data owners or evaluators instead of meaningful analysis and calculation. A fundamental principle of information risk management is that the cost to protect information should not exceed its value. The information risk profile does not need to quantify the exact value of data assets but must establish a general representation of value to allow for the definition of appropriate levels of classification and control.

To simplify information management, it is essential to classify data into easily understood containers associated with control objectives and mandates that identify data-handling requirements. This classification schema should be as simple for it to be helpful to the information risk profile and general HDO activities. The information risk profile should include an HDO data classification schema and a summary of the control requirements and associated objectives.

Level	Designation
4	PHI Confidential
3	Confidential
2	Internal
1	Unclassified

Table 2 Data Classification

Risk levels and categories provide a framework that can be used to organize and communicate information risk in an easily recognizable format. In addition, risk levels offer a scale to represent the level of material business impact if a risk were realized. The categories help to define the type of impact that would likely materialize (NIST, 2003).

The following are examples of information risk levels:

- **High**—Severe material compliance, legal and/or financial consequences; significant material impact on critical business processes and/or business operations; loss of customer trust and/or damage to brand reputation.
- **Medium**—Significant material compliance, legal or financial consequences; substantial material impact on key business processes and/or business operations; weakened customer trust and/or brand reputation.
- **Low**—Negligible to no material compliance, legal and/or financial consequences; minimal material impact on key business processes and/or operations; insignificant change in customer trust and/or brand reputation.

The following are examples of information risk categories:

- **Confidentiality**—The disclosure of sensitive information to unauthorized individuals or systems.
- **Integrity**—The impact on the accuracy and consistency of data and information.
- **Availability**—The effect on the ability to access capabilities and associated data and information.

Using this method of level setting and categorization, essential business processes can be presented in a heat map to visualize the associated information risk levels.

The following table is an example of a heat map:

Key Business Process	Confidentiality	Integrity	Availability
Electronic Health Records	High	High	High
Finance	High	High	Medium
Human Resources	High	High	Low
Supply Chain	Moderate	Moderate	Low

Table 3 Information Risk Heat Map

Material business impact considerations are a key element of any information risk profile. These considerations are equivalent to the pain charts commonly used in healthcare environments. Healthcare providers often use a pain chart (typically a numerical or graphical scale) to understand the level of pain and discomfort a patient is experiencing. This feedback allows providers to respond with appropriate levels of care. Likewise, in information risk profiles, material business impact considerations identify the impacts of an incident or loss in easily understood, recognizable terms for HDOs.

The following shows three types of charts that can be used:

- Financial: An immediate and unplanned loss equal to (or greater than) the following list would represent a material business impact on an HDO

Material Business Impact	Financial Loss Amount
Catastrophic	$50,000,000 and above
Major	$5,000,000 to 50,000,000
Moderate	$1,000,000 to 4,999,999
Minor	$100,000 to 999,999
Negligible	Less than $100,000

Table 4 Financial Impact

- Productivity: An immediate and unplanned loss of employee productivity equal to (or greater than) the following list would represent a material business impact on an HDO.

Material Business Impact	Employee Productivity Loss
Catastrophic	80% and above
Major	40 - 79%
Moderate	20 - 39%
Minor	10 - 19%
Negligible	1 - 9%

Table 5 Productivity Impact

- Availability: An immediate complete or partial lack of availability of one or more critical business processes and associated information assets and supporting systems would represent a material business impact on an HDO.

Material Business Impact	System Down Time
Catastrophic	Beyond 1 week
Major	73 - 1 week
Moderate	9 - 72 hours
Minor	2 - 8 hours
Negligible	Less than 2 hours

Table 6 System Downtime

For the information risk profile to be meaningful to an HDO, its leadership and stakeholders must endorse it. Once the risk profile is completed, HDOs will understand what defines an acceptable risk and what needs to be done to mitigate risks to a tolerable level.

Compliance

Healthcare compliance is the ongoing process of meeting—or exceeding—all legal, ethical, and professional standards applicable to an organization or provider. Every HDO deals with confidential health information (Smith, 2019). Consequently, HDOs must integrate policies compliant with HIPAA (and state and local laws and regulations) into compliance programs. Furthermore, healthcare delivery organizations that use cloud computing and store any data in the European Union (EU) or treat EU data subjects must adhere to the General Data Protection Regulation (GDPR). Healthcare delivery organizations must also adhere to the laws and regulations for any other jurisdiction where their data may reside.

As regulations applicable to HDOs evolve, so must compliance programs. For example, due to the COVID-19 pandemic, the current guidance from the Centers for Medicare and Medicaid Services (CMS) has broadened access to Medicare telehealth services so that patients can receive more services from their doctors without having to travel to a healthcare facility. These benefits are part of the broader effort by CMS and the White House Task Force to ensure that all Americans are aware of easy-to-use, accessible benefits that can help keep them healthy while also containing community spread of the virus (CMS, 2020). Therefore, any HDO policies and procedures should reflect this change.

Regardless of the technology used, all HDOs are required to assess their systems and have policies enacted to ensure adherence to HIPAA and other federal, state, and local laws and regulations (Interwork, 2018). With a well-designed and implemented compliance program, HDOs can avoid issues where they comply with one requirement (i.e., HIPAA) but fail to comply with others (i.e., PCI). Additionally, HDOs must understand that compliance is not the same as security.

The following table provides some of the drivers for laws and regulations.

PCI	
Goals	**Requirements**
Build and Maintain a Secure Network and Systems	1: Install and maintain a firewall configuration to protect cardholder data. 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3: Protect stored cardholder data. 4: Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5: Protect all systems against malware and regularly update anti-virus software or programs. 6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures	7: Restrict access to cardholder data by business need to know. 8: Identify and authenticate access to system components. 9: Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10: Track and monitor all access to network resources and cardholder data. 11: Regularly test security systems and processes.
Maintain an Information Security Policy	12: Maintain a policy that addresses information security for all personnel.
HIPAA	
Conduct a Risk Assessment	1: Conduct a project risk assessment. 2: Identify HIPAA data that will be processed, stored, or transmitted. 3: Identify vulnerabilities, threats, and risks.
Encryption	4: If keeping PHI for any period, encrypt it.
System Configuration	5: Any system with PHI access must be hardened before use.
Software Development Process	6: When developing in-house applications, use stringent development processes and secure coding guidelines.
Secure User Access	7: Ensure all access requires unique account information. 8: Ensure software implements access control. 9: Ensure multi-factor authentication is used for all remote access.
Software Testing	10: Conduct vulnerability scanning. 11: Conduct penetration testing.
PII	
Compliance Requirements	1: Identify all requirements for processing, storing, and handling PII. 2: Implement processes to ensure compliance.
Risk Assessments	3: Ensure a PII risk assessment has been conducted.
Access Controls	4: Ensure access control enforcement is incorporated into the software.

Table 7 Compliance Drivers

While this is not an all-inclusive list, it should provide insight into the complexities of compliance.

Measurement

As with any business process, measurement is paramount. Compliance reports illuminate areas within HDOs where compliance initiatives are met effectively and areas where HDOs do not meet regulatory or internal controls. Compliance metrics and key performance indicators (KPIs) measure a HDO's ability to align with organizational policies (both internal and external) and government regulations. Typical compliance functions include internal audits, compliance training, policy enforcement, and risk management. Compliance KPIs are meaningful, leading indicators of potential risk. Knowing this allows an HDO's leadership to make effective decisions about resource allocation, risk management, and strategic planning for the future.

Monitoring and Reporting

At a fundamental level, monitoring ensures an organization's operations are working as they should. Additionally, monitoring can identify areas of noncompliance. Monitoring is an essential first step to enhance compliance performance or other processes, and understanding the current state of compliance is a vital starting point. Organizations can only be confident they've identified all gaps in their approaches after implementing a robust monitoring and reporting system.

Reporting methods may include using the Cybersecurity Framework (CSF) and the Privacy Framework (PF) to identify an HDO's current privacy and security posture. These processes allow HDOs to compare current postures to future state postures. Furthermore, the framework supplies a common language for understanding and managing cybersecurity. The framework core supplies activities to achieve cybersecurity outcomes, and functions organize cybersecurity activities. Both frameworks will aid HDOs in aligning and prioritizing privacy and security activities with business requirements, risk tolerances, and resources. Additionally, these frameworks provide a common structure for approaching privacy and security by assembling standards, guidelines, and effective practices (NIST, 2018). As a result, this provides a standard reporting method for HDO leadership.

Governance, Risk, and Compliance

To ensure GRC policies are effective, HDOs should first understand applicable laws and regulations. Starting with compliance ensures that HDOs build a program with a solid foundation. The second step is conducting a comprehensive risk assessment and gap analysis. The risk analysis will show if HDOs: (1) meet compliance requirements and (2) provide adequate security. *Remember, compliance does not equal security.* Once the risk and compliance gaps are fully acknowledged, HDOs should ensure organizational policies and procedures address the shortcomings. This paper uses the National Institute of Standards and Technology security controls found in *SP 800-53 Rev 4* as examples.

Example 1 HIPAA Rule

HIPAA rule 164.312(a)(2)(i) Unique User Identification (R) Assign a unique name and/or number for identifying and tracking user identity (NIST, 2008).

This HIPAA requirement maps to National Institute of Standards and Technology (NIST) security control IA-2 Identification and Authentication (Organizational Users) which states:

Control: The information system uniquely identifies and authenticates organizational users or processes acting on behalf of organizational users (NIST, 2013).

Looking at the HIPAA requirement and the NIST security control the HDO can write the policy statement for user identification.

User Identification and Authorization
All Users of HDO Information Systems shall:

1. Obtain Manager or Sponsor authorization for the use of Information Systems.
2. Complete access requests and approvals for individual systems that are appropriate to the business purpose and do not compromise segregation of duties (SOD's).
3. Be issued a unique User ID that identifies only one User.
    a. User ID's shall be provisioned using the approved Identity Management (IDM) Solution. The account name will be the users first and last name, the user ID will be a randomly generated 4X4 account. That is four letters and four numbers, (3856kige).
    b. User ID's shall not be reassigned to a different User.
    c. User ID's shall be required to access all Information Systems.
    d. All User ID's shall have a designated Manager or Sponsor.

Example 2 GDPR Rule

GDPR Article 32, paragraph 2 states:
In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed (European Union, 2018).

This GDPR requirement maps to NIST security control RA-3 Risk Assessment which states:
Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in risk assessment report;
c. Reviews risk assessment results;

> d. Disseminates risk assessment results; and
> e. Updates the risk assessment annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system (NIST, 2013).

In addition to the security control NIST provides privacy controls.
Privacy Impact and Risk Assessment:
Control: The organization:

> a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and
> b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Looking at the GDPR requirement and the NIST security control the HDO can write the policy statement for risk assessments.

Performing Risk Assessments

> 1. HDO Security shall perform Risk Assessments on all Information Systems that create, receive, store, transmit, or view Confidential or PHI Confidential information or assets that are connected to the HDO network.
> 2. Risk Assessments must be documented in a central repository and include the qualitative and quantitative analysis of the impact and likelihood of threats and/or vulnerabilities.
> 3. HDO Security shall be responsible to update the Risk Assessments as appropriate following each Security Incident and Security Event.

The HDO would follow a similar process to write the privacy policy that relates to this control.
In this process you have a compliance requirement, a security control that both provides security and compliance, and a policy for implementing the control. The final step in the process is to ensure the policies are in alignment with the business mission. In today›s competitive healthcare environment, the alignment of IT operations with the business strategies and management of IT risks are imperative. IT governance is a way to accomplish IT-mission alignment.

Conclusion

Information technology GRC is critical for organizations because it helps align IT operations, business strategies, and compliance requirements. The overall purpose of GRC is to enact a structured process that supports business requirements, reduces risks, and ensures compliance. Governance, risk, and compliance is a business strategy that requires cooperation between business units to achieve results that meet internal guidelines and processes. Governance, risk, and compliance aren't about adding complexity and effort to existing over-complicated processes that already require tremendous work effort. Instead, its enactment can coordinate efforts while condensing and clarifying processes to reduce duplication and labor.

Healthcare delivery organizations can complete a risk assessment and highlight the controls required to protect their systems by identifying and classifying assets. Once an HDO has completed this process, they can pinpoint the compliance needs and determine if their controls meet those requirements. In addition to ensuring the controls meet the compliance requirements, HDOs should then assess them to ensure they provide security. At this juncture, HDOs can write policies that support compliance and security. The policies provide the governance, the controls address the risk—and both ensure compliance.

Healthcare delivery organizations rely on IT systems for day-to-day work, and security is essential. As HDOs implement GRC, they must ensure their IT governance programs include cloud computing considerations. An effective GRC program incorporating on-premise and cloud computing concerns will enhance security and compliance. By identifying risks and compliance requirements, HDOs can determine security controls that satisfy security and compliance. An HDO can then produce policies and procedures required to implement the security controls. Once controls are in place, HDOs can test them to ensure effectiveness. At this stage, HDOs have a well-established foundation for a solid GRC program. However, HDOs are well-served to remember that compliance does not equal security—but a sound, effective GRC program does provide security and compliance.

References

American Health Information Management Association. (2014). *Information Governance Principles for Healthcare*. Retrieved from https://library.ahima.org/doc?oid=107468

Armor. (2016). *Security vs Compliance*. Retrieved from https://www.healthcareitnews.com/sponsored-content/security-vs-compliance

Crosbie, D. (2020). *Why Data Destruction is Essential to Information Governance*, Complete Discovery Source. Retrieved from https://cdslegal.com/insights/why-data-destruction-is-essential-to-information-governance/

DataArchiva. (2018). *The rising importance of data governance and archiving in healthcare*. Retrieved from https://www.dataarchiva.com/the-rising-importance-of-data-governance-and-archiving-in-healthcare/

European Union. (2018). *General Data Protection Regulation (GDPR)*. Retrieved from https://gdpr-info.eu/

National Institute of Standards and Technology. (2003). *Federal Information Processing Standards Publication 199 Standards for Security Categorization of Federal Information and Information Systems*, National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Gillin, P. (2019). *Data Destruction in the Cloud: It's Complicated*. Retrieved from https://www.ironmountain.com/blogs/2019/data-destruction-in-the-cloud-its-complicated

Gundert, L. (2020). *The Risk Business: What CISOs Need to Know About Risk-Based Cybersecurity*, CyberEdge Group.

Haber, M. J. and Hibbert, B. (2018). *Asset Attack Vectors: Building Effective Vulnerability Management Strategies to Protect Organizations*, Apress

Interwork. (2018). *How to Achieve & Maintain Regulatory Compliance in Healthcare*. Retrieved from https://interwork.com/regulatory-compliance-in-healthcare/

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology. (2012). *Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments*, National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (2018). *Special Publication 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

National Institute of Standards and Technology. (2013). *Special Publication 800-53 Rev 4 Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-53r4

National Institute of Standards and Technology. (2008). *NIST Special Publication 800-66 Rev 1 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf

Secure Digital Solutions. (2014). *Governance, Risk, and Compliance*. Retrieved from https://trustsds.com/downloads/white-papers/Governance-Risk-Compliance.pdf

Smith, M. L. (2019). *Healthcare Compliance: An overview of the basics for organizations and providers*. Retrieved from https://www.thehealthlawfirm.com/resources/health-law-articles-and-documents/healthcare-compliance.html

Stine, K., Kissel, R., Barker, W. C., Fahlsing, J., and Gulick, J. (2008). *Special Publication 800-60 Volume I Revision 1: Guide for Mapping Types of Information and Information System to Security Categories*, National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final

Thorhallsdottir, K. (2018). *Impact and Probability in Risk Assessment*. Retrieved from http://apppm.man.dtu.dk/index.php/Impact_and_Probability_in_Risk_Assessment

U.S. Department of Health & Human Services, Center for Medicare and Medicaid Services. (2020). *Medicare Telemedicine Health Care Provider Fact Sheet*. Retrieved from https://www.hhs.gov/about/news/2020/03/17/ocr-announces-notification-of-enforcement-discretion-for-telehealth-remote-communications-during-the-covid-19.html

Cloud Security Alliance. (2021). *Telehealth Risk Management*. Retrieved from https://cloudsecurityalliance.org/artifacts/telehealth-risk-management/