INST726 : Fundamentals of Information Governance

Assignment: Creating IG “Drilled-Down” Policies, Frameworks & Solutions for UMGC

Instructor: Professor Jason R Baron

Student : Ushasri Bhogaraju

Date : 04/18/2024

SECTIONS

1. INTRODUCTION
2. INFORMATION GOVERNANCE PRINCIPLES AND PRACTICES
3. THE CLIENT, UMGC
4. AUDIT FINDINGS

A. MAPPING AUDIT FINDINGS TO UMGC POLICIES

B. DISCUSSION OF GAPS AND BEST PRACTICES

C. PROPOSED CHANGES IN EXISTING IG POLICIES

1. CONCLUSION
2. CITATIONS

I.A.INFORMATION GOVERNANCE PRINCIPLES AND PRACTICES

Information Governance is an evolving field, the principles, and practices of which are being constantly examined for strength and being expanded with recommendations by industry expert bodies such as the Sedona Conference Commentary on IG, authors such as Robert F Smallwood, and practicing experts such as Professor Jason R Baron, Ms. Susan Bennet and Ms. Sandra Serkes, Mrs. Amy Marcos, and implementation experts like Mr. David Marcos.

The size of information available to an organization is humongous now, because of evolution in networking, storage, and analytical capabilities. Because of this size, frequent examination through manual interventions by supervisors is not possible, and there must be policies put in place that employees can follow, on all the aspects that govern information handled by an organization. As challenges emerge, more and more aspects of information management are being brought under the protection of robust information governance programs.

That the field is ever evolving with new problems and solutions is evident from industry expert Ms. Susan Bennet’s initial IG model from few years ago, having only 7 areas such as Privacy and Data Protection, Records & Information Management, Data Governance, Legal eDiscovery, Data Analytics, Risk& compliance and Cyber security, and the latest model, reorganizing the initial IG model and also adding technology integration, automation and AI, Business Intelligence, Information life cycle management and archiving and long term preservation to the IG umbrella.

The procedures for implementing the policies created for effective information governance can be laid out clearly for manual implementation, or the process can be automated with readymade solutions available in the industry marketplace. There are innovative approaches to achieve the same, such as the privacy-by-design approach, or implementing software solutions such as auto-classification of records and version control software solutions to address important aspects of information governance. Auto-classification of documents in real-time is an important enabler as it makes it easier to manage vast amounts of information that is generated effectively and also makes it easy to comply with ethical and regulatory requirements. However, creating awareness about the whole challenge regarding information, its uses and safety and the need for adherence to the information governance policy guidelines by all employees are paramount to achieving the goal of safeguarding and using information efficiently for business needs.

I.B. THE CLIENT, UNIVERSITY OF MARYLAND GLOBAL CAMPUS

The University of Maryland Global Campus is an accredited institution that conducts courses online and awards globally recognized degrees to students. The University has a well-designed [information governance policy website](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology), that provides the links to the laid down information governance policy documents which comprise of details such as policy category, policy owner, policy version effective date and review cycle, most importantly, policy contact along with the purpose, scope, definitions and policy statements themselves . The obvious aim of this enterprise is to serve as guidance to staff and faculty, in order that they may conduct the University’s business relevant to their area of operation, securely and smoothly. As a member of the [public university system of Maryland,](https://www.usmd.edu/regents/bylaws/SectionX/X100.html) UMGC must be subject to regular internal and external audits. A Gap analysis created from one such (fictitious) audit is the basis of the present report. This report comprises of a review of selected policies that were mapped to findings in the Gap analysis report, and recommendations for changes in the said policies that will bridge the perceived gaps.

As presented in my summary on IG principles and Best practices learned from industry experts and the textbook, information governance policies of an enterprise are the central resource that informs the staff and executives, the information creators, consumers, stakeholders, and legal representatives of the enterprise, on the University’s information governance program. In the text of the documents, the procedures that are to be followed to conduct the business of the enterprise securely and responsibly are provided. A well-developed information governance policy framework, frequently reviewed and developed, is an imperative for the modern enterprise, as besides providing transparency, it lays down procedures to ensure data security, avoid legal hassles and delivers business value by treating information as an important asset. Forums like the Sedona Conference are important bodies that shape the information governance landscape, as they bring together experts in various fields, by providing a platform for exchange of knowledge, best practices, and solutions for IG problems.

Therefore, their formal recommendation of ‘a top-down, overarching framework, guided by the requirements and goals of all stakeholders that enables an organization to make decisions about information for the good of the overall organization and consistent with senior management’s strategic decisions.’ (Sedona Conference, 2019, p.97) to form the basis of the information governance policy framework of an enterprise, is recommended for organizations like UMGC.

The nature of the business conducted by UMGC involves providing education on online platforms, fostering research and exchange of data between researchers and faculty, and handling employee requirements and payments. The University is subject to ethical and regulatory compliances along with membership compliances, being a member of the University of Maryland system. Some of the main elements of the University’s information governance policy framework should be,

1. Data Management: UMGC is expected to hold PII data pertaining to staff, faculty and students, student academic records, academic research and publications which may be subject to intellectual property rights. Data generated as part of various forms of communication, through the use of web applications, mobile device applications, by way of more formal means such as documents and records, must all be carefully dealt-with and guidelines for management of the same should be incorporated into the IG policy framework of UMGC. Since the University acquires smaller educational institutions, policies and procedures to manage information inflow should be laid down. A suitable version control software implementation is required to manage Official documents generated by the University staff.
2. Regulatory body compliances : UMGC must comply with FERPA for student records and as a member of the University system of Maryland, also with the applicable compliances required by the system. By adopting suitable solutions such as auto-classification of records which can not only handle risk categorization, eDiscovery requirements and privacy requirements, but also handle archiving and destruction of records by generating prompts at predetermined times, UMGC can ensure compliance.
3. Data life cycle and retention periods: UMGC IG policy framework must clearly have policies and procedures to be followed regarding retention of data and records as prescribed for educational institutions. Any ambiguity in the policy framework may lead to huge piles of archives. In this context, the importance of staff awareness and training in record classification, storage and destruction policies of the organization cannot be understated.
4. Clear policies on information sharing and collaboration: Since educational institutions support information sharing and collaboration among researchers, faculty, and students, the UMGC IG principles must be clear in prescribing rules in this regard.
5. Since the University accepts payments via cards, all the procedures for processing, storage and transmission of card information must be compliant with PCI SSC standards.
6. Information security : The University IG policy framework should adequately cater to the mitigation of external and internal threats to its information resources.
7. Employee training: Since employee awareness and training are critical to the success of an IG program, the University must have an ongoing IG training program.

On examination of the Policies under Administration section of the University Governance structure, we find that, to a large extent the University IG policy framework is well developed. But as is true for all organizations, constant review and enhancement of existing policies is an important undertaking and audits serve as the stimulus for such reviews and corrections.

II. AUDIT FINDINGS

**A1.1 (IG Management, Processes and Policies, No.1 )**

**Statement:**

‘The Executive IG Council referenced in UMGC X-1.01 does not know who to report to other than the President of the University. There is not a clear line of communication with the Board of Trustees.’

1. MAPPING TO UMGC POLICIES

Referenced UMGC Policy Name: [Information Governance](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/information-governance) Policy No. UMGC X-1.01

Policy is categorized under Information Governance, Security & Technology and therefore the reporting structure for the Information Governance team must ideally be part of the policy. To an extent, the policy in its existing state serves that requirement in its purpose statement and policy statements.

The purpose of the policy is to establish an enterprise-wide oversight framework to support effective Information Governance across the University and facilitate the integration of a set of standards and attributes listed therein.

1. DISCUSSION OF GAPS AND BEST PRACTICES

Smallwood textbook pins down the responsibility of ‘Board of Directors’ in the implementation of various aspects of information governance such as oversight on compliance with Privacy Policies, IT Governance, Record management, and other areas, making it necessary that the information governance council have regular contact with the board. In the case of UMGC, which is a non-profit, the same rules apply for the relationship between the information governance council mentioned in the aforesaid policy and the Board of Trustees.

To understand further if the duties of the Board of Trustees are different from those of the Board of Directors, I investigated and found this [Investopedia article](https://www.investopedia.com/terms/b/boardoftrustees.asp#:~:text=A%20board%20of%20trustees%20is,all%20types%20of%20management%20decisions.) that says, ‘A board of trustees is an appointed or elected group of individuals that has overall responsibility for the management of an organization. The board of trustees is typically the governing body of an organization and seeks to ensure the best interest of [stakeholders](https://www.investopedia.com/terms/s/stakeholder.asp) in all types of management decisions’, which sealed my understanding of the role of Board of Trustees at UMGC.

To find out who the Board of Trustees are at UMGC, I explored this link, [UMGC’s Boards and Committees](https://www.umgc.edu/administration/leadership-and-governance/boards-and-committees) and found that there is no mention of the Board of Trustees on its website. The [Leadership and Governance](https://www.umgc.edu/administration/leadership-and-governance/boards-and-committees) structure lists SVPs in charge of distinct operational vertices, with the UMGC president, Gregory Fowler as the Head. The [Policies and reporting](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/information-governance) structure states that UMGC follows a shared governance policy, by providing separate governance bodies for the three stakeholder groups viz, the Student Advisory Council, the Academic Advisory Board and the Global Staff Advisory Council. Nowhere in the reporting structure is a mention of the Board of Trustees.

The Smallwood book recommends that the board of directors be involved in every aspect of governance of an organization from policy making to implementation. The Board of Trustees at UMGC therefore, must provide strategic direction to the IG team, collaborate to set and manage information governance policies, understand information governance risks and ensure compliance with legal and ethical standards. Therefore, the Board of Trustees must ideally be accessible to the information governance council and the [Information Governance](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/information-governance) Policy No. UMGC X-1.01 must be updated to this effect.

1. PROPOSED CHANGES IN IG POLICY IMPLEMENTATION IN IDENTIFIED AREAS
2. In the Boards and Committees section, along with the Senior Executive team, introduce the Board of Trustees and provide their contact information.
3. Under Administration>Policies & Reporting > Policies>[Information governance, security & technology](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/information-governance) , the present policy statement has 3 main policy statements with sub-statements. The following policy statement may be included as item D. under Section IV. Policy Statements.

D. ‘ The information governance council will prepare and submit a comprehensive report on all matters dealt with by the council during the month. The report shall include a status report on the University’s position with regard to ethical and regulatory compliance standards. In addition to submitting a monthly report, an exigency report seeking direction may be submitted to the board, whenever the Board’s direction is needed on a strategic matter. Members of the information governance council may contact the Board of Directors via any official channel for this purpose.’

**Audit Finding reference : B.5. (Communication Technologies, No.5 )**

**Statement:**

‘Email is a huge pain point for staff. Employees routinely reach their inbox limit and that is what prompts them to take action. Staff do not have time to keep up with the incoming email volume. Some employees also find that emails they want to follow up on get “lost in the morass.” Staff are indiscriminately dumping email into an archive without assessing whether the information needs to be saved, resulting in an email archive running into the millions of documents. Some staff do not understand that email is covered by the University records management policies.’

1. MAPPING TO UMGC POLICIES

Referenced UMGC Policy No. UMGC X-1.26

Policy link : [ELECTRONIC MAIL](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/electronic-mail)

Existing Policy details:

The purpose of the policy is comprehensive and does not need change. It states,

‘The purpose of this policy is to establish information security standards and related University policies for electronic mail (“e-mail”) use and e-mail processes relevant to University of Maryland Global Campus ("UMGC" or "University") Information Technology Resources.

The scope of the policy is also comprehensive and does not require change.

*The current policy statements deal with all aspects of email usage, but do not address the concerns raised by the auditors in the findings. There are 4 related policies listed under the existing policy, none of which provide guidance to staff on the matter.*

1. DISCUSSION OF GAPS AND BEST PRACTICES

What does the textbook offer by way of solution to the problem that surfaced in the audit on email communications? Smallwood identifies solving the email problem as one of the 10 main reasons why IG makes business sense. (Smallwood,2020,p.10). Further under the section Smallwood IG Principles in the textbook, in the 4th principle regarding information organization and classification, he aptly regards emails as business information. I reproduce the text instead of paraphrasing it here, because he says it best.

‘It also means creating a records retention schedule (RRS) that spells out how long the PII/PCI/PHI as well as business information (e.g., e-mail, e-documents, spreadsheets, reports) should be retained and how it is to be disposed of or archived (disposition). Further, it means developing departmental file plans that are logical and help end users to conduct more complete and accurate searches for information.’(Smallwood,2020, p.31)

Further in Principle 8 on Information governance monitoring and auditing, he says,

‘To guard against claims of legal spoliation, the use of e-mail, social media, cloud computing, and report generation should be logged (recorded or archived) in real time and maintained as an audit record. Technology tools such as document analytics can track how many documents users access and print and how long they spend doing so.’ (Smallwood, 2020, p.33)

The author also recommends storing email in a compressed and indexed format to reduce storage requirements and allow for rapid, complex searches. He says that archiving real-time applications like email can only be deemed reliable with record integrity if it is performed immediately in real time.(Smallwood, 2020, Glossary) .This can easily be achieved using modern auto classification software.

I believe that UMGC’s email problem can be solved by implementing the above ideas.

1. PROPOSED CHANGES IN EXISING POLICIES

Incorporating the above recommendations, we can add the following policy statements to the existing email policy referred to above. Under Section IV. Specific use of electronic mail the present policy statements’ list ends with L.

M. Email Archiving and Retention: Emails containing official records or business-critical information must be retained according to the University records retention schedule. The email archives must be reviewed at least once a month, to avoid unnecessary accumulation. In case a specific matter needs longer retentions and direction, the policy contact may be approached for the same.

N. Email usage and inbox management: Employees are advised to be mindful of incoming volume of emails and prioritize responses based on urgency and relevance. Employees are required to avoid indiscriminate archiving. All employees receiving emails in the course of duty are required to assess and mark those to be deleted, based on the University records management policies. The supervisor of the employee is authorized to delete the emails, upon on verification.

O. Training : A self-paced training tutorial on email policy implementation for all University employees is made available at this location. All employees are required to complete this tutorial immediately upon taking charge of their official duties.

P. The University is in the process of evaluating and purchasing suitable auto-classification software solution for record management. Once a decision has been made, all the employees will be advised to undergo series of trainings to provide required knowledge in the use of the software solution.

**Audit Finding reference : C.12. (Records and Data Management, No.12 )**

**Statement:**

‘UMGC lacks procedures for ensuring proper creation and storage of documents to support consistent version control. For some staff, searching for the latest version of a document is highly inefficient.

1. MAPPING TO UMGC POLICIES

Referenced UMGC Policy No. UMGC X-1.03, Policy link : [Records and Information Management](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/records-and-information-management-procedures), Policy procedures link: [UMGC P-X-1.03: Records and Information Management Procedures](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/records-and-information-management-procedures).

Existing Policy details: The policy contact is identified as the [University records manager](mailto:recordsmanagement@umgc.edu).

The purpose of the policy states how University records must be managed throughout their life cycle including archiving and secure destruction, complying with allied policies and procedures for the same. The scope of the policy is comprehensive, lists all types of employees, consultants, and contractors as obliged to follow the policy.

There is a comprehensive roles and responsibilities section, enumerating the designated employees and their responsibilities.

1. DISCUSSION OF GAPS AND BEST PRACTICES

The policy statements cover all aspects of the management of the Record Life cycle, retention, disposition and destruction, exceptions to the instructions and of course archiving. The policy statements with regard to conversion of physical records to electronic form and instructions for preservation of electronic records are laid down clearly. Most importantly, this policy has an ancillary [UMGC P-X-1.03: Records and Information Management Procedures](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/records-and-information-management-procedures) document which states the procedures for implementation of the [Records and Information Management](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/records-and-information-management-procedures) policy.

However, there is no mention of implementation of a version control mechanism and a matching record access pattern for employees based on their roles and responsibilities. Neither the policy statements nor the procedures address the challenge faced by staff in the finding which is difficulty in finding the latest version of a document.

*Best Practices proposed by experts*: I could not find any particular reference to the version control problem in the Smallwood textbook, however, I found this informative blog post on the topic at [imageAPI](https://www.imageapi.com/blog/version-control), named ‘Mastering Document Version Control: A comprehensive Guide for 2024’. The article explains the challenge succinctly, when it says that in any organization, thousands of documents, both physical and digital are generated, circulated, referenced and duplicated daily. The challenge is keeping this incredible volume of documentation organized and under control. Therefore, document version control implementation is the critical enabler for productivity, efficiency, and accuracy for any organization. ‘When multiple stakeholders or contributors are working on a document at the same time, version control makes sure that the latest, most up-to-date version of the document is clearly identifiable for circulation, providing a single point of truth for that particular document, and avoiding duplicates.’ (imageAPI blogpost on Mastering Document version control, August 9,2023)

*This solution mitigates the challenge being faced at present by UMGC employees* and therefore it is recommended that, UMGC evaluate and purchase a suitable version control software solution and make changes to the [Records and Information Management](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/records-and-information-management-procedures) policy.

UMGC then benefits from

1. Having a formal information governance policy that includes document version control solutions.
2. Implementing a version control software that allows
   1. removal of duplicates,
   2. preservation of drafts and previous versions,
   3. provides a mechanism to audit document histories,
   4. archive older document versions and
   5. permits collaborative work on documents.
3. Determining and implementing document access patterns by employees enforcing security levels.
4. Ensuring adequate training for staff on the usage of the new software/solution, to ensure consistent application of version control.
5. PROPOSED CHANGES IN IG POLICY IMPLEMENTATION IN IDENTIFIED AREAS

The [Records and Information Management](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/records-and-information-management-procedures) policy may be amended to include the rules for use of the version control solution for official documents generated at UMGC, as per the draft amendments suggested below.

***Purpose amended*** :UMGC Records must be managed in a consistent, systematic, and secure manner to ensure their authenticity, reliability, integrity, confidentiality, and availability. Official documents must be marked and processed through the version control software solution adopted by the University and will form part of UMGC Records. This Policy provides the requirements for managing UMGC Records throughout their lifecycle, including archiving or secure destruction and, together with any related procedures or administrative guidelines, and the UMGC Records Retention Schedule, forms the basis for a UMGC Records Management Program which complies with federal and state laws and regulations and [**University System of Maryland ("USM") Policy VI-6.10-Policy on Records Management**](https://www.usmd.edu/regents/bylaws/SectionVI/VI610.html).

***Scope amended***: This Policy applies to all employees, including exempt, non-exempt, and overseas staff, 12-month collegiate faculty and collegiate traveling faculty as well as third parties working for and providing services or products to or on behalf of UMGC such as adjunct faculty, contractors, consultants, and temporary employees. Every employee and third party working on behalf of UMGC who creates, sends, or receives electronic, or paper Records is responsible for making sure Records are properly maintained. Official documents generated by employees must be marked and processed using the version control software solution adopted by the University, and are to be treated the same as University Records.

Amendments to the Policy Statements

1. Record Lifecycle: (addition to present set of policy statements)
2. Version Control for Official documents: Every employee creating an official document is responsible for ensuring that it is standardized, tagged and version numbered to support efficient version control. Labeling each document with a version number, date and authorship information is the responsibility of the employee generating the document. No official document may be saved in personal storage areas or unapproved locations. All documents must be stored in designated storage areas where access control is implemented based on roles and responsibilities.
3. Training requirements: All employees must undergo training for the use of version control software solution adopted by UMGC within one week of their taking charge of their position.

**Audit Finding reference : D.5. (Privacy & Cybersecurity, No.22 )**

**Statement:**

‘The University is increasingly facing threats to its information security from external sources and does not have systems in place which do a good job of mitigating potential internal threats. Staff are not given much in the way of directions on how to manage sensitive electronic data. For example, there is a lack of awareness of VPN and Citrix options for working remotely.’

1. MAPPING TO UMGC POLICIES

Referenced UMGC Policy No. UMGC X-1.04 & 1.05

Policy links : [UMGC X-1.04 Information Security](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/information-security) &

[UMGC X-1.05 Information security awareness and training](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/information-security-awareness-training):

Existing Policy details, UMGC X-1.04

The purpose of the policy is stated as protecting University information and information resources, laying out how University records must be managed throughout their life cycle ‘including when created or collected, stored, transmitted or transferred, and destroyed.’

The scope of the policy specifies ‘Information Resources residing in UMGC internal or external environments that store and process UMGC data.’, effectively including devices used in WFH situations. The policy’s supporting standards and procedures are applicable to all that have access to UMGC information and information resources, and to any information system owned or managed by the University. The Roles and responsibilities section clearly indicates the officials responsible for monitoring compliance with the policy.

Existing Policy details, [UMGC X-1.05 Information security awareness and training](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/information-security-awareness-training):

On examination of this policy, I find that most of the concerns raised by the finding are mitigated in the implementation of this policy. Though there is no specific mention of the details of the practices that mitigate external threats, such as the use of VPN and Citrix solutions, there is a role-based security awareness training program envisaged in this policy, that may prescribe the use of these tools. Internal threats such as staff responding to phishing emails resulting in ransomware attacks or such, can also be mitigated through strictly enforcing the security awareness training requirements for staff, immediately upon joining duty and periodically thereafter. This is envisaged in this policy.

1. DISCUSSION OF GAPS AND BEST PRACTICES

***Best practices proposed by experts:*** Smallwood prescribes a remedy for both external and internal threats, eloquently in the chapter on Information Governance and mobile devices when he says ‘Social engineering—using various ways of fooling the user into providing private data—is the most common approach criminal hackers use, and it is on the rise. Machines do their job, and software performs exactly as it is programmed to do, but human beings are the weakest link in the security chain, and as usage trends in the direction of a more mobile and remote workforce, people need to be trained as to what threats exist, and constantly updated on new criminal schemes and approaches. This training is all part of an overall information governance (IG) effort, controlling who has access to what information, when, and from where.’ .(Smallwood,2020.p321)

Further, he points out that holding regular security awareness training (SAT) sessions helps reduce the risk of data loss on mobile devices.(Smallwood,2020.p321)

I believe that the security awareness training is intended as role based in UMGC. Therefore, a security officer may receive required training with regard to the identified University attack vectors and player tactics that the officer should be aware of with regard to those attack vectors and be prepared to mitigate external threats. So also, all employees may undergo a training program on social engineering attempt methodologies and the internal procedures that one must adhere to, to mitigate these kinds of internal threats.

1. PROPOSED CHANGES IN IG POLICY IMPLEMENTATION IN IDENTIFIED AREAS

Upon review of both the relevant policies, small amendments are recommended to add a few details to the [UMGC X-1.05 Information security awareness and training](https://www.umgc.edu/administration/policies-and-reporting/policies/info-governance-security-technology/information-security-awareness-training) policy.

Purpose: No amendment proposed

Scope: No amendment proposed

Addition to item D. under Section IV. Information security and awareness training

1. Additional specialized or role-based security training may be required for Users who:
   1. Have Privileged User access.
   2. Have access to Confidential Data
   3. Are eligible for WFH privileges, and use BYOD or University provided devices to access University resources over remote networks.
2. CONCLUSION

As the value for information increases with new use cases, so does the danger to its safety because of bad actors. Every digital organization, therefore, must have a sound information governance program to protect its information assets and maintain the overall governance posture of the organization at a high standard. UMGC to a large extent has a well-established policy framework, but there is scope for improvement in some policies. It must absorb the industry’s best practices in strengthening its information governance policy structure. Most importantly, the involvement of the Board of Trustees in the governance arena must be evident.

1. CITATIONS

*The Sedona Conference, Commentary on Information Governance*, Second Edition, 20 SEDONA CONF. J. 95 (2019)

Smallwood, R.F. *Information Governance: Concepts, Strategies, and Best Practices*. John Wiley & Sons, Inc., 2020.

Article: [Ten steps to successful data governance in mergers and acquisitions, Onna Technologies Inc](https://www.jdsupra.com/legalnews/ten-steps-to-successful-data-governance-2662273/).

[University of Pennsylvania Journal of Business Law Vol.23 No.1,2020](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3821991) : Boards in Information Governance, [NYLS Legal studies research paper No.3821991](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3821991)

AHA Trustee Services : <https://trustees.aha.org/understanding-board-trustees-role>

imageAPI : Mastering Document Version Control: A comprehensive Guide for 2024’ https://www.imageapi.com/blog/version-control