

Ráðstefna Félags um skjalastjórn

- Þetta þarftu að vita!

Ragna Kemp Haraldsdóttir, PhD. Dósent í
upplýsingafræði við Háskóla Íslands.

- Stjórnkerfi upplýsinga, hvers vegna, hvernig tengist
þetta, hver er ávinningurinn?

Dagskrá



- Hvað er stjórnkerfi upplýsinga (e. Information Governance) og hvað kemur það okkur við?
- Hvað veldur þessum aukna áhuga – hvaða innri og ytri þættir eru það sem ýta undir þörf fyrir stjórnkerfi upplýsinga?
- Hvert er hlutverk sérfræðinga í upplýsingastjórnun þegar kemur að stjórnkerfi upplýsinga?
- Hvað segja rannsóknir okkur?

Information Governance

- Governance er skilgreint á vef Merriam-Webster sem:
 - the act or process of governing or *overseeing the control and direction of something*
- Þar eru tilgreind nokkur samheiti m.a.

administration

authority

government

jurisdiction

regime

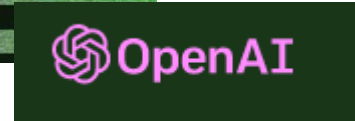
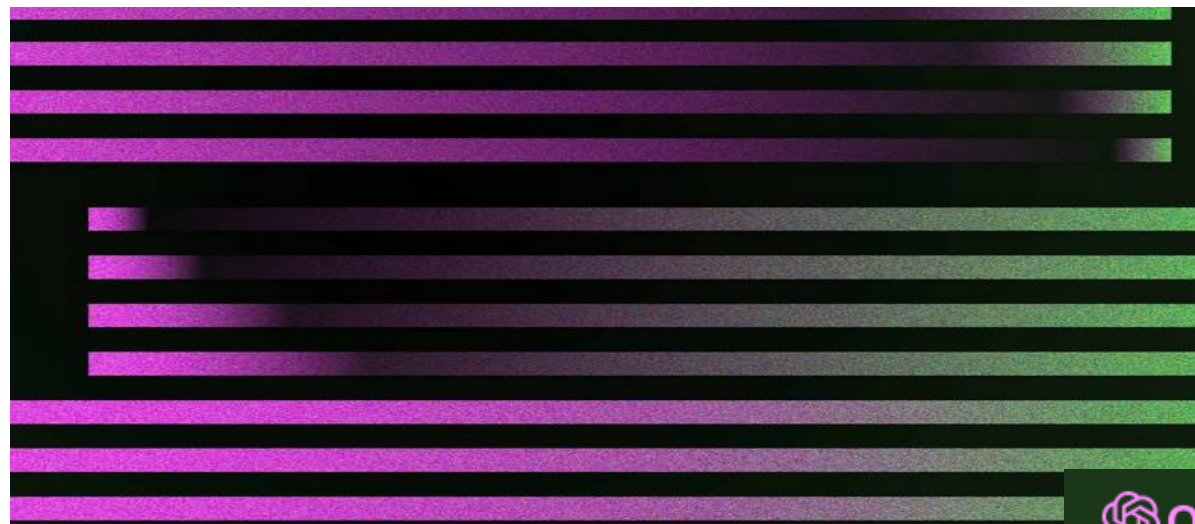
régime

regimen

rule

- Samkvæmt ensk-íslenskri orðabók þýðir hugtakið *governance* stjórn eða stjórnun
- Bein þýðing væri þá líklega stjórnun upplýsinga eða upplýsingastjórnun (e. information management)
- Á fagmáli á íslensku er yfirleitt talað Information Governance sem stjórnsýslu upplýsinga, stjórnarhætti upplýsinga eða *stjórnkerfi upplýsinga*

Niðurstöður frá ChatGTP



What can you tell me about information governance?

Information governance is a comprehensive approach to managing and protecting an organization's information assets. It includes **a set of policies and procedures** that define how information is created, stored, used, and disposed of. It also helps **ensure compliance with privacy, security, and other regulations**. A good information governance program **ensures that an organization's information is secure, accurate, and accessible**. It helps an organization **manage risk, protect its reputation, and improve efficiency**.

Information Governance

- Information governance is **the overarching and coordinating strategy for all organizational information**. It establishes the *authorities, supports, processes, capabilities, structures, and infrastructure to enable information to be a useful asset* and reduced liability to an organization, based on that organization's specific business requirements and risk tolerance.

Arma.org

- The strategic, **cross-disciplinary framework** composed of **standards, processes, roles, and metrics** that *hold organizations and individuals accountable for the proper handling of information assets*. The framework helps organizations achieve business objectives, facilitates compliance with external requirements, and minimizes risk posed by sub-standard information-handling practices.

Glossary, Arma International, 2016

- Field of management responsible for the **efficient and systematic control** of the creation, receipt, maintenance, use and disposition of records, including **processes** for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Skilgreining á hugtakinu upplýsinga- og skjalastjórn skv. ISO 15489-1:2016

Stjórnkerfi upplýsinga (e. Information Governance)

- Hugmyndafræði og aðferðir sem tengjast *Stjórnkerfi upplýsinga* taldar vera tækifæri fyrir skjalastjórn eða kannski nauðsynlegt nýnæmi sem ætti að taka við af skjalastjórn þar sem skjalastjórn í hefðbundnum skilningi þyki of tengd pappírsgögnum til að geta uppfyllt nútíma kröfur skipulagsheilda um upplýsingar (Brooks, 2018).
- Er stjórnkerfi upplýsinga kannski bara *“a trendsetting container for capturing almost everything and nothing in the world of information management”* (Hagmann, 2013).
- Tilgangur stjórnkerfis upplýsinga er að skilgreina *“all aspects of how information is being managed”* á meðan tilgangur skjalastjórnar er að hafa stjórn á sumum hliðum þessara upplýsinga (Parapadakis, 2018).
- Er stjórnkerfi upplýsinga að taka við af skjalastjórn? Og hvers vegna – vegna þess að skjalastjórn ræður ekki við umfang og útbreiðslu upplýsinga á tímum stafvæðingar:

“Simply put, records management has not been able to keep up with the velocity, volume and variety of formats for digital assets” (Zarkout, 2014).

Stjórnkerfi upplýsinga (e. Information Governance)

- Er Stjórnkerfi upplýsinga einfaldlega Skjalastjórn 2.0?
- Ný og endurbætt útgáfa á aðferðum kerfisbundinnar skjalastjórnar (Carlis, 2015) eða eins og Medina (2015) orðar það:

But if you look under the hood, the engine is STILL basic records management, with increased horsepower [...] and a few other bells and whistle.

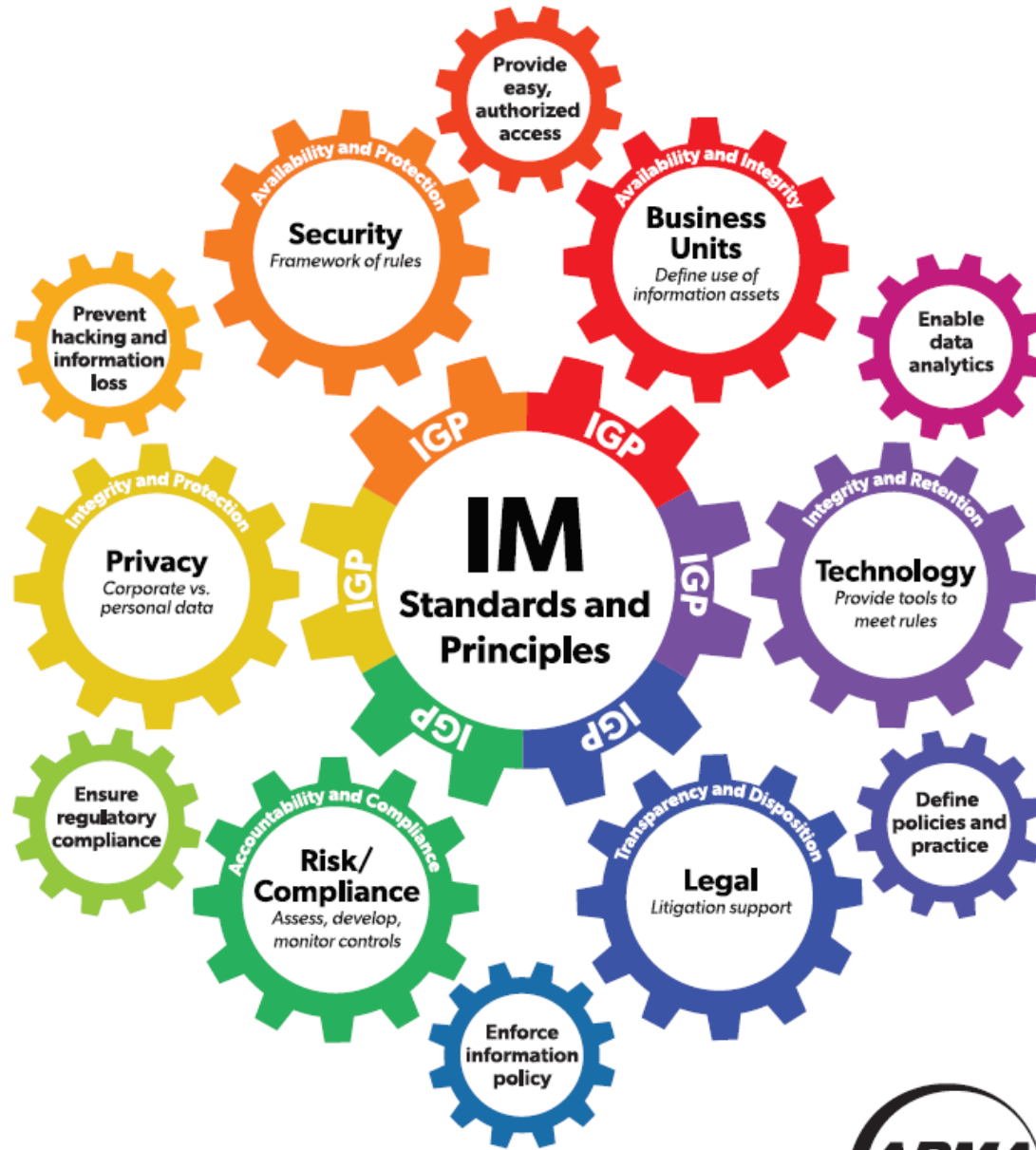
- Equally critical to success is **corporate communication** which truly values information as a corporate asset and highlights the importance of information lifecycle management rather than technology under the motto “putting the ‘I’ into IT” (Hagmann, 2013).

Hluti af stærri heild – aukinn skilningur / stuðningur?

*In other words, while on the one hand, records management was deemed to be insufficient on its own to fulfil an organisation's information needs, it was at least **now clearly valued as part of a wider information landscape**. Indeed, after years of advocating for records management to be further up organisational agendas, **being part of an IG framework had strengthened its position by recognising its role within a more strategic information framework**. As noted, another key advantage recognised in much of the literature was that **IG strategically positioned records managers alongside a range of other vital stakeholders and allies – including IT, legal, risk, information security, privacy, compliance and business unit heads – those who previously the records managers may have had to forge alliances and relationships with on their own initiative***

(Brooks, 2018, s. 9)

ARMA International's Information Governance Core Concepts

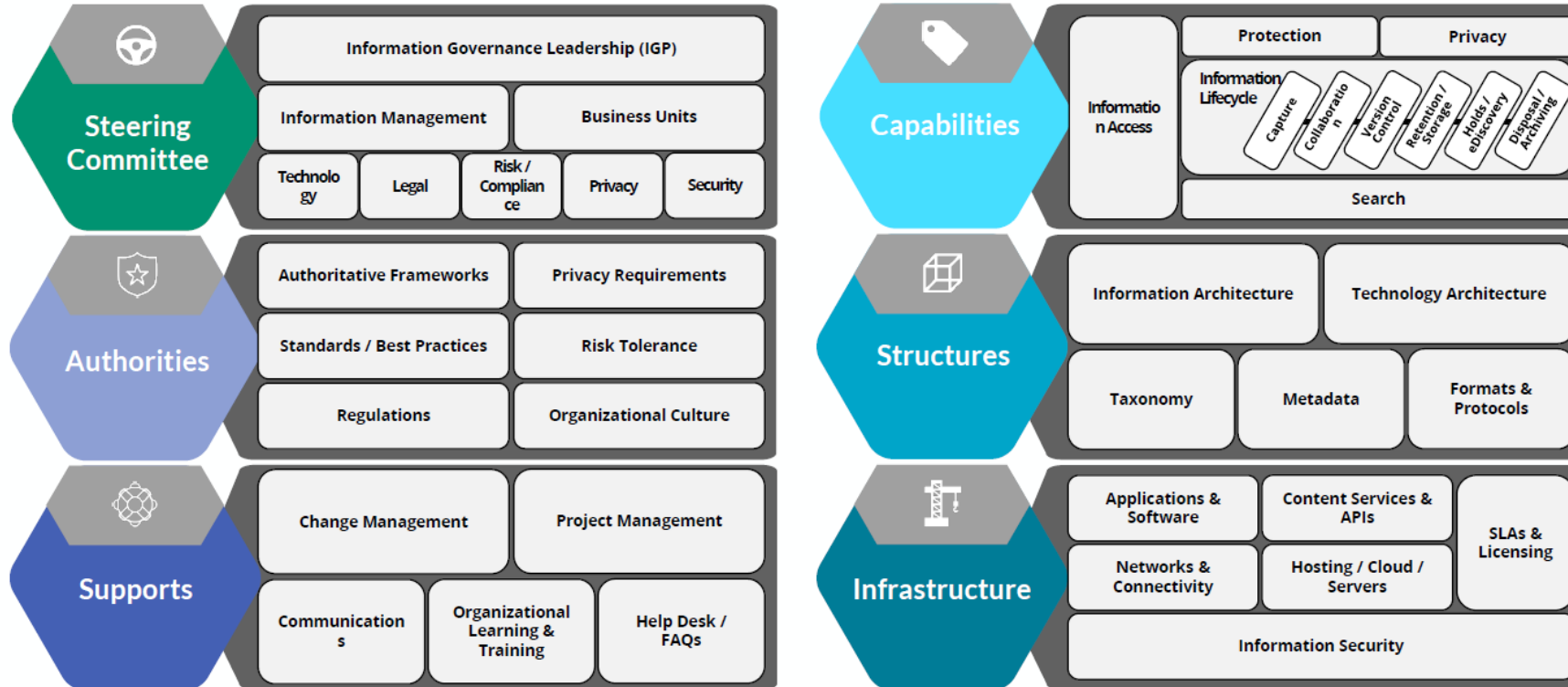


Innleiðing á stjórnerfi upplýsinga (Information Governance)



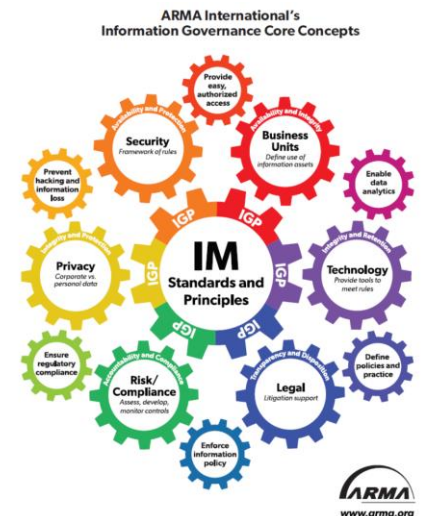
Information Governance Implementation Model

<https://www.arma.org/igim>



Meginreglurnar átta – að setja innri kröfur

- **Ábyrgð** – hafa yfirsýn yfir stjórnkerfi upplýsinga (information governance) og útdeila ábyrgð til viðeigandi sérfræðinga. Innleiða stefnur og verkferla til að tryggja að kerfið geti verið vottað.
- **Heilindi** – að kerfið sé þannig uppbyggt að það innihaldi viðeigandi ráðstafanir til að tryggja uppruna og áreiðanleika upplýsinga.
- **Gagnavernd** – að viðhalda persónuvernd, trúnaði og leynd gagna eftir því sem við á
- **Hlíting** (sem nær yfir kröfur úr þroskalíkani ÞÍ) – að vinnsla gagna sé í samræmi við gildandi lög og reglur sem og stefnu viðkomandi skipulagsheildar
- **Tiltækileiki** – að tryggja skjótt og öruggt aðgengi að gögnum til þeirra sem eiga erindi í gögnin.
- **Varðveisla** – að gögnin séu geymd í samræmi við lög, reglur, stefnur og aðrar kröfur sem gilda um varðveislu gagna.
- **Ráðstöfun** – að tryggja örugga eyðingu þeirra gagna sem ekki lengur eru í notkun
- **Gagnsæi** – skráning og skipulag stjórnkerfis upplýsinga skal vera gagnsætt þannig að hægt sé að skoða og sannreyna ákvarðanir sem teknar hafa verið.



Fyrsta og annað stig

- **LEVEL 1 (Sub-Standard):** This level describes an environment where information governance and recordkeeping concerns are not addressed at all, are addressed minimally, or are addressed in an *ad hoc* manner. Organizations that identify primarily with these descriptions should be concerned that their programs will not meet legal or regulatory scrutiny and may not effectively serve the business needs of the organization.
- **LEVEL 2 (In Development):** This level describes an environment where there is a developing recognition that information governance and prudent recordkeeping have an impact on the organization and that the organization may benefit from a more defined information governance program. However, in Level 2, the organization is still vulnerable to scrutiny of its legal or regulatory and business requirements because its practices are ill-defined, incomplete, nascent, or only marginally effective.

- **LEVEL 3 (Essential):** This level describes the essential, or minimum, requirements that must be addressed to meet the organization's legal, regulatory, and business requirements. Level 3 is characterized by defined policies and procedures and the implementation of processes specifically intended to improve information governance and recordkeeping. Organizations that identify primarily with Level 3 descriptions still may be missing significant opportunities for streamlining business and controlling costs, but they have the key basic components of a sound program in place and are likely to be at least minimally compliant with legal, operational, and other responsibilities.

Generally Accepted Recordkeeping Principles. Arma International



- **LEVEL4 (Proactive):**This level describes an organization that **has established a proactive information governance program throughout its operations** and has established continuous improvement for it. Information governance issues and considerations are routinely **integrated into business decisions**. The organization is substantially more than minimally compliant with good practice and **easily meets its legal and regulatory requirements**. The entity that identifies primarily with these descriptions should begin to pursue the additional business and productivity benefits it could achieve by increasing enterprise-wide information availability, mining its information for a better understanding of clients' and customers' needs, and otherwise transforming itself through increased use of its information.
- **LEVEL5 (Transformational):**This level describes an organization that has **integrated information governance into its overall corporate infrastructure** and business processes to such an extent that compliance with program requirements and legal, regulatory, and other responsibilities are routine. This organization has recognized that **effective information governance plays a critical role in cost containment, competitive advantage, and client service**, and it has successfully implemented strategies and tools to achieve these gains on a plenary basis.

Dæmi – Gagnavernd



Protection

An information governance program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection.

No consideration is given to information protection. Records and information are stored haphazardly, with protection taken by various groups and departments and with no centralized access controls. Access controls, if any, are assigned by the author.

1

Some protection of information assets is exercised. There is a written policy for records and information that require a level of protection (e.g., personnel records). However, the policy does not give clear and definitive guidelines for all information in all media types. Guidance for employees is not universal or uniform. Employee training is not formalized. The policy does not address how to exchange these records and information among internal or external stakeholders. Access controls are implemented by individual content owners.

2

The organization has a formal written policy for protecting records and information, as well as centralized access controls. Confidentiality and privacy considerations are well-defined within the organization. The importance of chain of custody is defined, when appropriate. Training for employees is available. Records and information audits are conducted only in regulated areas of the business. Audits in other areas may be conducted, but they are left to the discretion of each functional area. The organization has defined specific goals related to records and information protection.

3

The organization has implemented systems that provide for the protection of the information. Employee training is formalized and well-documented. Auditing of compliance and protection is conducted on a regular basis.

4

Executives and/or senior management and other governing bodies (e.g., board of directors) place great value in the protection of information. Audit information is regularly examined, and continuous improvement is undertaken. Inappropriate or inadvertent information disclosure or loss incidents are rare. The organization's initial goals related to protection have been met, and it has an established process to ensure its goals for protection are routinely reviewed and revised.

5

ISO 24143:2022 – Alþjóðlegur staðall um Information Governance

“Information is a critical asset that is indispensable to support business processes and therefore, a foundation for the success of any business activities. Due to numerous existing and emerging forms and uses of information and information-related risks, organizations often struggle with implementing consistent and comprehensive systems to store, retrieve, share and analyse information. The current global digital transformation and the changes in societal expectations increasingly demand greater transparency, accountability, data protection, security, interoperability and information sharing within and between organisations. This trend requires a solid vision and strategy for Information Governance that supports the business process at a strategic level including digital transformation initiatives. Many governmental and non-governmental organisations worldwide already perceive the necessity and understand the benefits of coordinating at a strategic level the efforts of multiple information-, data- and knowledge-related disciplines”

(ISO 24143:2022, s. v)

Information Governance – skilgreiningar úr gæðastaðli

A.2.2 Concepts relating to information

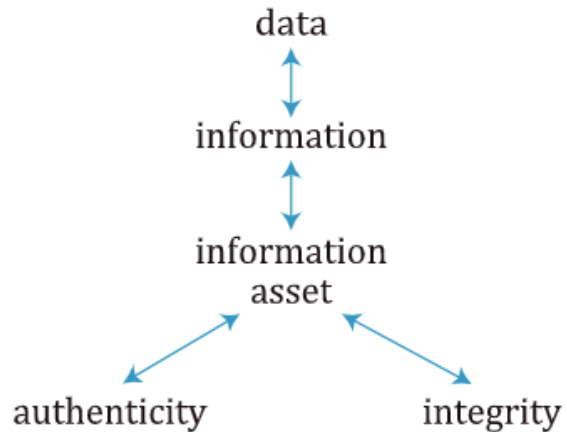


Figure A.1 — Core concepts relating to information

- strategic framework for governing [information assets \(3.1.4\)](#) across an entire organization in order to enhance coordinated support for the achievement of business outcomes and obtain assurance that the risks to its [information \(3.1.3\)](#), and thereby the operation capabilities and [integrity \(3.1.5\)](#) of the organisation, are effectively identified and managed
- Information Governance includes (but is not limited to) policies, processes, procedures, roles and controls put in place to meet regulatory, legal, risk and operational requirements. Data is one form of information asset.

Information Governance – samhengi ólíkra/samtengdra þátta

A.2.3 Concepts relating to Information Governance

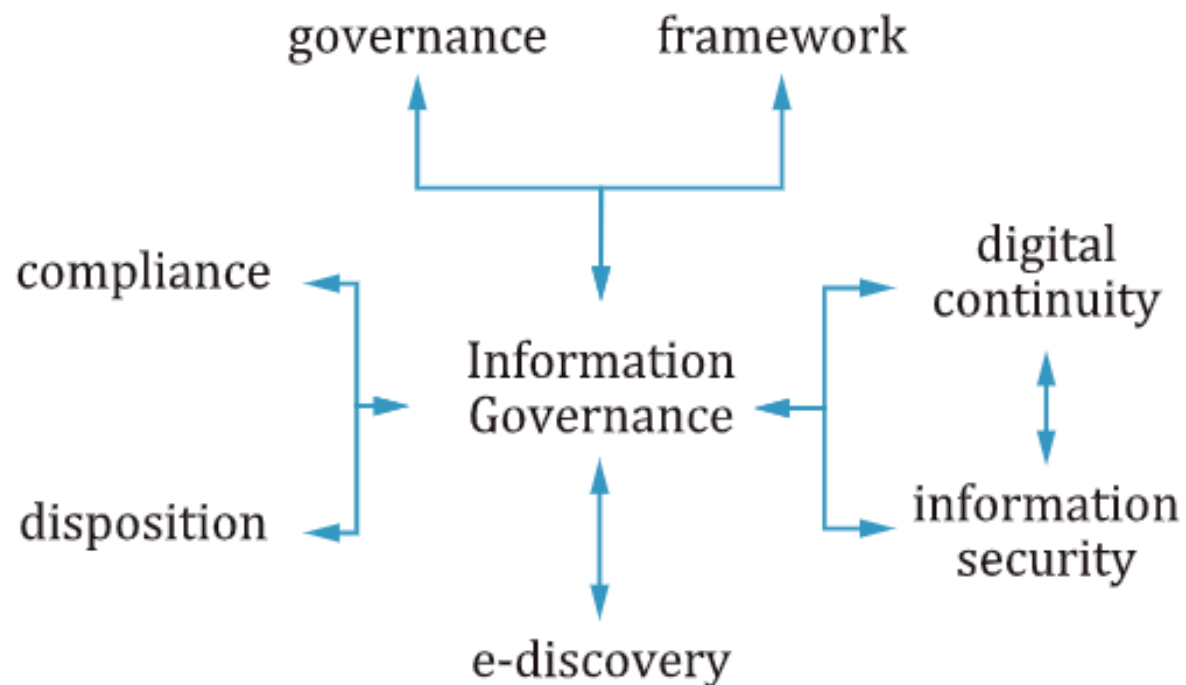


Figure A.2 — Concepts relating to Information Governance

Ytri kröfur – ISO ÍST 27001:2017

A.8 Verðmæstastjórnun		
A.8.1 Ábyrgð á verðmætum		
Markmið: Að tilgreina verðmæti skipulagsheildarinnar og skilgreina viðeigandi verndarábyrgð.		
A.8.1.1	Verðmætaskrá	<p><i>Stýring</i></p> <p>Bera skal kennsl á upplýsingar, önnur verðmæti tengd upplýsingum og aðstöðu til upplýsingavinnslu og gera skal skrá yfir öll þessi verðmæti og viðhalda henni.</p>
A.8.1.2	Eignarhald verðmæta	<p><i>Stýring</i></p> <p>Verðmæti í skránni skulu hafa eiganda.</p>
A.8.1.3	Ásættanleg notkun verðmæta	<p><i>Stýring</i></p> <p>Bera skal kennsl á reglur um ásættanlega notkun upplýsinga og verðmæta sem tengjast aðstöðu til upplýsingavinnslu, skjalfesta þær og innleiða.</p>
A.8.1.4	Verðmætum skilað	<p><i>Stýring</i></p> <p>Allir starfsmenn og utanaðkomandi notendur skulu við lok ráðningartíma, samnings eða samkomulags skila öllum verðmætum skipulagsheildarinnar sem eru í þeirra vörslu.</p>

Ytri kröfur – ISO ÍST 27001:2017



A.8.2 Flokkun upplýsinga		
Markmið: Að tryggja að upplýsingar njóti viðeigandi verndar í samræmi við mikilvægi þeirra fyrir skipulagsheildina.		
A.8.2.1	Flokkun upplýsinga	<i>Stýring</i> Upplýsingar skulu flokkaðar með tilliti til réttarfarsákvæða, virðis, mikilvægis og viðkvæmni fyrir óheimilli birtingu eða breytingum.
A.8.2.2	Merkingar upplýsinga	<i>Stýring</i> Þróa skal og innleiða viðeigandi verklagsreglur um merkingu upplýsinga í samræmi við það upplýsingaflokkunarkerfi sem skipulagsheildin hefur tekið upp.
A.8.2.3	Meðhöndlun verðmæta	<i>Stýring</i> Þróa skal og innleiða viðeigandi verklagsreglur um meðhöndlun verðmæta í samræmi við það upplýsingaflokkunarkerfi sem skipulagsheildin hefur tekið upp.

Takk fyrir mig!



