TR03 - Security Classification of Records in the Cloud in International Organizations:

A Literature Review

February 14, 2018

1. Introduction

For many organizations, security sensitive, or classified, information can be a difficult challenge. In international organizations, this type of information can be particularly complex because of the diverse missions, specific composition, legal status and international and political contexts the organizations exist in. These organisations have an obligation to protect the confidentiality of the information that has been produced by and entrusted to them, while remaining accountable to their various stakeholders for the safe management of such classified information. This latter aspect of the challenges seems particularly urgent given the contemporary emphasis within civic life - especially within developed and democratic societies - on transparency and access to information in the last few decades. The purpose of this literature review is to bring together the various studies, concepts and views on the topic of classified information in international organizations, in order to identify the prevalent themes and gaps in the discourse that require further research.

The initial search for articles was fairly broad, and included government white papers and commission reports, as well as articles from security, legal, and archival perspectives. To guide the search for relevant literature, we used a combination of keyword searches such as: “information security policy,” “confidential information,” and other relevant terms. In addition, citations of relevant articles were noted, and particular interest was paid to articles that were cited frequently in a variety of sources. This was done with the intent to find a broad number of articles, as well as to note those that seemed ‘most important’ within the community since they were most frequently cited. One of the key findings in initial and subsequent searches was the scant focus on information security and the management of classified information within international organizations; those articles that did directly address international organizations focused on a variety of different issues but rarely on handling security classified information. The scarce and disparate nature of the published work on this topic demonstrates the need for more research and discourse on the topic of security classified information within international organizations.

2. Definition of classified information

One of the fundamental aspects that can be drawn from this disparate literature are trends in how classified information is defined and what makes classified information different from non-classified information. Though seemingly a basic concept, the terms are left somewhat ill-defined by current literature, often skimmed over as if simply obvious. This is clearly not the case; even within a given organization, the lack of clarity about what is ‘classified information’ and what is not can cause problems (Hooten 2011). It is usually implied that classified information is secret information with restrictions about who may see it (Aftergood 2000; Aftergood 2002; Aftergood 2008; Aftergood 2009; Aftergood 2010; Aftergood 2013). However, in many organizations restricted information is not confined only to information that is classified for security purposes. For example, personnel information is also restricted,

but for privacy purposes. Classified information is different because of *why* it is kept restricted. Steven Aftergood (2000) notes that in the US government there are three different categories of classified information—genuine, political, and bureaucratic—and that the second two are an abuse. The first, however, "pertains to that body of information which, if disclosed, could actually damage national security in some identifiable way"(Aftergood 2000 p. 25-26). This definition closely resembles the suggestion made in ISO 27002:2013 section 8.2.1, which states that:

an information confidentiality classification scheme could be based on four levels as follows:

a) disclosure causes no harm;

b) disclosure causes minor embarrassment or minor operation inconvenience;

c) disclosure has a significant short term impact on operations or tactical objectives;

d) disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk (International Standards Organization 2013b p. 16 Sec. 8.2.1).

One can deduce from these statements that classified information has been defined in literature as information which would cause harm if disclosed. Though this may seem simple, in practice and consequently in the professional literature, many questions arise on the topic. Leyzorek (1998) asks, for example, what is 'harm' or how much 'harm' counts (a scratch on your hand is significantly different than a broken arm)? Does it mean harm to the organization, the personnel of the organization, their clients, or the world, or maybe all of the above? The Australian government, for example, created different policies regarding national security (that information that threatens the nation as a whole) and non-national security information (that information that would threaten interests of organizations or individuals) (Australia Law Reform Commission 2004 p. 38-40)[1] The frequently used terms, 'Sensitive but Unclassified' and 'Security Sensitive' are particularly volatile terms, causing confusion wherever they go. Aftergood (2002 p. 26) explains this confusion: "no one knows what it means. The meaning of 'unclassified' is clear, of course, but the crucial term 'sensitive' is not defined." Is 'Sensitive but Unclassified' information a type of classified information, or something else altogether and therefore, should 'Sensitive But Unclassified' information be under the same policies of other classified information; or do they need their own policies? (Aftergood 2002; Hooten 2011; Leyzorek 1998; Relyea 2008 p. 924-925) Though frequently addressed, this topic has been somewhat inadequately answered—with the USDA Departmental Regulation 3440-0023 of January 30, 2000 describing Security Sensitive Information as "unclassified information of a sensitive nature, that if publicly disclosed could be expected to have a harmful impact on the security of Federal operations or assets..." (Relyea 2008 p. 14). Meanwhile, the Australian government's special commission on classified and sensitive information defined security sensitive information as "information that has implications for Australia's security, but is not formally classified, for whatever reason"(Australia Law Reform Commission 2004 p. 41)

[1]

Another facet of security classified information to consider is the role and impact of international organizations (IGOs) in the matter. According to Hitchens (1997 p. 1), IGOs are "Bodies based on a formal instrument of agreement between the governments of nation states...including three or more states...and a permanent Secretariat performing ongoing tasks." They are greater than its parts, and can address issues or challenges that transcend national borders (Hitchens 1997 p. 148). The legal status, responsibilities, privileges and immunities of IGOs are all different from those of governments -- it is therefore important to discuss the information policy of IGOs as something also distinct from governmental information policy (Dikker Hupkes 2009). Moreover, IGOs both produce and collect information used in administration and decision-making, including information from their member governments. Political collaboration on key global issues also happens at the intergovernmental level. This information is important to a wider audience of citizens, NGOs, academics and other stakeholders. For this reason, Hitchens (1997 p. 143-145) argues that it is important to consider the dissemination of IGO information in information policy discussions. As of yet, much of the discussion has happened at the national level.

3. Protection, management of classified information

While the majority of the literature reviewed focuses on the principles of security classified information regardless of the storage location of the information, the management of classified records per se is not necessarily discussed. The current literature shows a gap on the best practice of managing classified records in a cloud environment, which is exacerbated when taking an inter-governmental or international organizational context into account. With regards to the management of classified records the focus of the literature is on security declassification in the US federal government.

The most succinct summary of the principles of classified information can be gleaned from the international standard ISO 27001 (2013a) titled Information Technology – Security Techniques – Information Security Management Systems – Requirements, which was designed to "provide requirements for establishing, implementing, maintaining and continually improving an information security management system". The standard stresses the importance of integrating the information security system with the core business processes of the organization as well as its management structure and calls for information security concerns to be considered whenever new systems or processes are being designed (v). Leyzorek (1998 p. 2), who uses a fictional example of a leak of classified information to discuss the management of classified information in records management systems breaks this premise down by providing a concise, if poorly referenced, run-through of the key steps of defining an information security framework, from defining what and why information should be classified to providing training on the enforcement of the framework

ISO 27001 (2013a p. 5) also expands on the need to clearly define the objectives of information security in or complemented by the information security policy framework of the organization. The information security policy also should to take into account all work modes available in the organization as well as all forms of equipment used to access classified information (International Standards Organization 2013a p. 11). Hooten (2011 p. 6), who argues for organization-wide consistency of information security policies in his article "How Many Times Can Classified Be Said?", provides examples from the IMF and World Bank

archives which illustrate the complication of information access when left to individual departments.(2013a p. 5) also expands on the need to clearly define the objectives of information security in or complemented by the information security policy framework of the organization. The information security policy also should to take into account all work modes available in the organization as well as all forms of equipment used to access classified information. Hooten (2011), who argues for organization-wide consistency of information security policies in his article "How Many Times Can Classified Be Said?", provides examples from the IMF and World Bank archives which illustrate the complication of information access when left to individual departments.

Steven Aftergood (2000 p. 26) argues that while political secrecy, "the deliberate and conscious use of classification authority for political advantage" is the most dangerous "to the political health of the nation" , bureaucratic secrecy, "the largely unconscious hoarding and withholding of information" , seems to be the predominant factor in current classification activities. A crucial principle of the management of information security is therefore that the level of classification assigned to information assets an employee produces needs to be clearly defined as well as justified, as both over- and under classification should be avoided.

To counter unchecked classification, ISO 27001 (2013a p. 12) outlines that "information shall be classified in terms of legal requirements, criticality and sensitivity to unauthorized disclosure of modification" . However, even with a classification framework defined and in place, the classification process itself is inherently subjective (Aftergood 2008 p. 107). As Aftergood (2008 p. 107) notes in the context of US federal security classification, "…] there is no precise, objective definition of what constitutes unacceptable 'damage to national security' that would justify such decisions. Instead, classification decisions must be based on judgment and experience. On matters of judgment, there are always likely to be disagreements". In practice why and at what level information is classified is widely left at the prerogative of the employee who runs the risk of exposing sensitive information and might act "out of a fear of repercussion for failing to protect classified information" (Lin 2014 p. 444).(2008 p. 107) notes in the context of US federal security classification, "…] there is no precise, objective definition of what constitutes unacceptable 'damage to national security' that would justify such decisions. Instead, classification decisions must be based on judgment and experience. On matters of judgment, there are always likely to be disagreements". In practice why and at what level information is classified is widely left at the prerogative of the employee who runs the risk of exposing sensitive information and might act "out of a fear of repercussion for failing to protect classified information".

This habit might also be exacerbated, as analyzed by Herbert Lin in his proposal to reduce government classification, by the bias to view classified information as inherently more valuable than classified information, as well as the pressure employees are under to protect information from unauthorized access. When faced with a large volume of information which needs to undergo risk analysis to determine a potential classification category, Lin states that employees err on the side of classification. Additionally, he argues, that the act of classifying information in itself is seen as a free good and as such overused (Lin 2014 p. 444)

The definition and execution of the handling and control of classified information should extend not just to the information itself, but also to its environment, be it a digital system or a file cabinet (International Standards Organization 2013a p. 14) and apply to any point of the information lifecycle and location within the organization . (International Standards Organization 2013a p. 14)

Another key principle defined in the literature Classified information needs to be clearly recognizable, labelled as well as hold pertinent metadata to allow the management of the information (International Standards Organization 2013a p. 6)

Roles and responsibilities as well as access rights need to be clearly defined on a need-to-know basis following the principle of compartmentalization and assigned among personnel to ensure accountability and avoid conflict of interests (International Standards Organization 2013a p. 3). In areas where a conflict of interest is possible, the responsibilities need to be separated to ensure that unauthorized modifications or misuse of classified information remain minimal (International Standards Organization 2013a p. 10). The necessity to define roles and authority points was illustrated by Kaija Schilde (2015) and John Michael Weaver (2017). Schilde (2015 p. 168) covers the handling of classified information in EU information policy and "the confusion over who has the authority to access, protect, analyze, and disclose EU-classified information" with the example of access to TFTP information. Written with regards to computer network attacks, computer network exploitation and leaks of classified information, Weaver stresses the importance to hold everyone with access to classified information in a given country to the same standards and regulations (Weaver 2017 p. 10-11) .(International Standards Organization 2013a p. 3). In areas where a conflict of interest is possible, the responsibilities need to be separated to ensure that unauthorized modifications or misuse of classified information remain minimal.

Prior to handling classified information, employees need to attend information security awareness training as well as complete regular refreshers (International Standards Organization 2013a p. 11). Weaver (2017 p. 10) underscores the importance of information security training by noting that in the US "those who work in the intelligence community endure lengthy instruction on why it is obligatory for those charged with a nation's secrets to properly handle the information and the damage that can ensue from poor practices"(International Standards Organization 2013a p. 11) .

Just as under classification poses grave risks for an organization, so also does over classification, as it impedes decision making and presents a barrier to accountability. Aftergood (2008 p. 103) and Relyea (2008 p. 26) argue that while national security and classification mechanisms are a valid tool which serves the public interest, unchecked and arbitrary over classification hampers accountability of the political process and prevents informed decision making by imposing restrictions on information sharing. This insight applies not just to classified information which would not have warranted a classification marking in the first place, but also to classified information which remains classified for longer than necessary (Aftergood 2008 p. 103).

Therefore, re- and declassification procedures need to be put into place in parallel with classification procedures and other information security mechanisms (Wallace 1993 p. 796). Kastenhofer and Katuu (2016) argue in their analysis of declassification procedures in international organizations that risk based declassification reviews are the most efficient way to systematically declassify information, based on the premise that in most cases the justification of classification decreases over time.. While re- and declassification address existing classification labels with regards to their applicability, retroactive classification negates a previous classification assessment by classifying information retroactively and thereby potentially removing information from the public domain which was previously potentially accessible (Abel 2015). Jonathan Abel (2015 p. 1041)covers retroactive classification in his article "Do You Have to Keep the Government's Secrets", where he argues in the context of US federal classification regulations that "the current law provides no effective restraint on the practice of retroactive

classification". He makes suggestions on how to improve the current situation through regulatory input to reduce the potential of system abuse, for example by "changing the executive orders that govern retroactive classification, addressing the problem of retroactive classification statutorily, and amending House and Senate rules to avoid a separation of powers issue" (Abel 2015 p. 1043).

Key principles defined in the standard which were not covered in the literature reviewed include that classified information needs to be clearly recognizable, labelled as well as hold pertinent metadata to allow the management of the information (International Standards Organization 2013a p. 6), that management support is crucial for the continued maintenance of information security (International Standards Organization 2013a p. 2) and that information security needs to be proactively, rather than reactively, managed.

4. Access, declassification, emerging trends: transparency

A key theme in the literature on security classified information pertains to issues around public access to classified information. The discourse delves into sub-topics such as declassification and reclassification, tensions between privacy and security versus accountability and transparency, the interplay of freedom of information laws, and the disclosure of classified information in court proceedings, to name a few aspects of this theme. The question of public access to information is, not surprisingly, posed largely in relation to national governments. A smaller portion of the literature focuses on classified information policy and access to information related to intergovernmental organizations (IGOs).

The ever-present tension between the right to information and the need for security and therefore secrecy is one of the defining issues within the literature. Hitchens (1997 p. 145) observes that accountability and public involvement are democratic expectations. Although access to information does not guarantee citizen involvement, there can be no discourse without it; as such, “the provision of information is the first step in the process of consultation, openness and accountability” (Hitchens 1997 p. 145). Hitchens (1997 p. 151) argues that this is true not only at the state level, but also in the context of IGOs, since access to IGO information is “essential to discourse and accountability at the global level”. Similarly, Roche (2015 p. 55) who focuses on public access policies at the North Atlantic Treaty Organization (NATO), perceives that as a publicly-funded IGO, NATO “has an obligation to its members’ citizens of open and honest recordkeeping”(Hitchens 1997 p. 145). Similarly, who focuses on public access policies at the North Atlantic Treaty Organization (NATO), perceives that as a publicly-funded IGO, NATO “has an obligation to its members’ citizens of open and honest recordkeeping”.

A small but discrete portion of the literature centers on classified information policy and information access trends for IGOs (Castaner 2014; Eckman 2005; Hitchens 1997; Roberts 2004; Roche 2015). Eckman (2005), Hitchens (1997) and Roberts (2004) move towards transparency in IGOs such as the World Bank (WB), International Monetary Fund (IMF) and the World Trade Organization (WTO) in the latter part of the 1990s. In particular, Eckman (2005 p. 1)notes the increased transparency in policy-making and policy reviews in IGOs, and the establishment of archival access policies within several IGOs during this period. Castaner (2014 p. 313) describes the Archives Transparency Project, an effort by the IMF from 2003-2008 to provide archival descriptions for records dating from 1946-1988, “effectively creating the historical archives of the Institution”, where previously there had been none. Roche (2015 p. 57) discusses the evolution of access to NATO archives starting from transparency efforts in the 1970s

and moving towards the official opening of the archives in 1999, “with tens of thousands of NATO records open to the public for the first time ever”. Contemporary efforts at transparency and greater public access to information have manifested in the digitization and availability of archival holdings online (Castaner 2014; Roche 2015), public communications strategies, and robust exhibitions and publications showcasing archival holdings at NATO (Roche 2015). (Castaner 2014; Eckman 2005; Hitchens 1997; Roberts 2004; Roche 2015),

Positive as such public access initiatives may be, as Roberts (2004 p. 92) cautions, an appearance of transparency should not exclude a critical approach of the realities. Several authors discuss the often invisible barriers to access to information, more often in a national context but also in an IGO context. For example, in the case of the latter, interviews by Peter Jagnal with researchers and diplomats have revealed problems encountered when trying to gather IGO information, such as poor distribution of documents, IGO secrecy, and insufficient access to IGO databases (Hitchens 1997 p. 145) . Williams (1988) explains that it is difficult to even discover the existence of IGO publications, documents and data files, let alone gain access to them . Hitchens (1997 p. 151) further illustrates conflicts in the stated policies of IGOs and the realities of the distribution system, bibliographic control, timeliness, and quality of available information, and argues that the gap between the ideals of explicit policies and the realities of implicit policies needs to be tightened. Castaner (2014 p. 312-314), discussing the case for increased transparency at the IMF, explains that although documents may be “public,” many are actually nearly impossible to access . A lack of resources is the main culprit for example budgetary and workload burdens that are associated with manual review (Castaner 2014; Eckman 2005 p. 1). Relyea (2008), Bennett (2002) and Kosar (2010) further describe the costs of classification in comparison to the scarce resources and low prioritization given to declassification projects. (Hitchens 1997 p. 145) .

A substantial part of the literature, whether expository or critical in tone, focuses on classified information policy within the U.S. government. Kosar (2010), writing as an analyst within the U.S. government, explains the purpose and content of U.S. classified information policy, and traces the ebb and flow of policy and practice, illustrating that the emphasis on government secrecy or transparency at a given moment in history depends on the policies set by contemporaneous U.S. presidents, and is therefore by no means linear. At the time of publication of Kosar’s report, the policy was set by former President Barack Obama’s 2009 Executive Order (EO) 13526. Among other initiatives, EO 13526 established the National Declassification Centre and the Reducing Overclassification Act, part of a broader effort within the Obama administration towards open government and transparency (Kosar 2010 p. 9). The impact of the open government trend on classified information policy is also explored by Bennett (2002) in the context of British intelligence information. Bennet describes the various factors that led, in the late 1990s and 2000s, to greater openness within British intelligence agencies and to the transfer of intelligence records to the UK Public Records Office. (Kosar 2010 p. 9).

A key component of the legislative framework for public access to information exists in the form of national freedom of information laws. Hitchens (1997 p. 145) describes public access to information laws as “policy statements on public access to and the use of information,” and notes that they constitute a “modern legislative trend since the 1960s”. The Freedom of Information Act (FOIA) in the U.S. gives the public the right of access to government information, while also giving the government the capacity to withhold certain types of information (Aftergood 2002 p. 25). Access to information laws have ‘rapidly’ increased following the fall of the Berlin Wall in 1989, amounting to 5.2 billion people in 95 countries who theoretically benefit from such laws (Open Society Foundation 2013 p. 6). This trend

has contributed to heightened awareness and questions raised regarding what information should be kept secret (Open Society Foundation 2013 p. 6) . This debate typically occurs at the national level, focusing on the citizen-to-state relationship and vice-versa (Hitchens 1997 p. 146-147) . These patterns are reflected in the professional literature published in the late 1990s and early 2000s, which frequently focused on government secrecy, and argued for more transparency (Aftergood 2002; Hitchens 1997; Lin 2014; Roberts 2004). More recently, anti-terrorist laws have helped to encourage government proposals for more restrictive 'secrecy legislation' (Open Society Foundation 2013) .

As with IGOs, national efforts at transparency at the policy and/or legislative level do not necessarily equal access to information in reality. Wallace (1993 p. 795) points out that mechanisms for public access such as the FOIA in the U.S. place legal, financial, and temporal burdens on requesters . Similarly, Aftergood (2009 p. 406) discusses the limits of FOI and states that the policy only provides access to a limited number of documents and is not a systematic approach to openness . Aftergood (2000 p. 25) in general is highly critical of the U.S. government, stating, "most of the policies and practices that were established in the early days of the Cold War to protect official secrets remain intact". In a later article, Aftergood (2010 p. 840) states, "too much information is classified and withheld from the public in the name of national security, and that has undesirable effects on public policy and on public discourse" .

In some cases, over-classification is a purposeful way of hiding documentation, as in the example of parallel recordkeeping systems used by Hoover (Wallace 1993 p. 804-806). Relyea (2008 p. CRS-4) reports that the 1985 U.S. Department of Defence (DoD) Security Review Commissions found that "too much information appears to be classified and much at higher levels than is warranted". Relyea (2008) explains that the proliferation of control markings outside of the classification system is, at least in part, a large part of the problem. A 1972 oversight hearing of the U.S. FOIA found that 58 control markings outside of official classification markings were in use (Relyea 2008 p. CRS-6).These control markings frequently lack the clear definitions and stringent policies and procedures surrounding security classification, and therefore lead not only to confusion, but to a marked lack of information sharing (Relyea 2008 p. 25-26). (Relyea 2008 p. CRS-6). Aftergood (2000 p. 27) proposes that every classification policy and guide in the U.S. government, at an agency level, should be reviewed in an effort to systematically reduce over-classification (Aftergood 2008 p. 105). He includes the FOIA, regular review of the classification policies, strong leadership and pressure groups as effective ways to reduce secrecy (Aftergood 2010). David (2013) writing at around the same time, argues that to improve access, records should be transferred to the National Archives and Records Administration (NARA) earlier, and more authority given to the national archives. Additionally, Aftergood (2009) argues that an important part of transparency should be to write a list of what has and has not yet been processed.

Along with the act of classifying information comes the responsibility to establish policies and procedures for declassifying information. Both Kastenhofer and Katuu (2016 p. 3) and Relyea (2008, p. 27) frame declassification in the context of a records lifecycle. However, as Kastenhofer and Katuu (2016 p. 7) observe, many articles on declassification focus on the political aspects of declassification, such as the rationale for classifying and declassifying information, the often conflicting opinions of member states, and the "idiosyncratic" policies and regulations of IGOs. By contrast, Kastenhofer and Katuu (2016 p. 8-9) focus on the "mechanical" processes of declassification, including systematic and ad-hoc declassification; and provide a schema of the six types of actions involved in declassification processes. Relyea (2008 p. 27) states that automatic or systematic declassification can help to relieve the situation in the American context, in which a move to greater secrecy post 9/11 has resulted in more

classified information being produced, while fewer declassified information has become available. This highlights the disparity in the rate at which classified information is being produced, as compared to the much slower rate at which information is being declassified. Roche (2015, p. 57) likewise asserts that systematic declassification saves time and effort: “The more documents are made public by design, the less time the NATO Archives will have to spend processing these documents in the future.” Aftergood (2000 p. 27) argues that the authority to declassify records should expand beyond the originating agency. David (2013 p. 434) adds that increasing public understanding and involvement in the declassification process would have an overall positive impact on declassification programs and general transparency. Overall, the literature on transparency and access to classified information is, as mentioned earlier, often expository and/or critical, tackling issues of government or institutional secrecy, and the management or mis-management of classified information. There is a need for more literature on best practices and strategies for managing classified information, especially from a records and information management perspective. Organizations could benefit from the expertise of records professionals in addressing the substantial challenges of classification and declassification, in order to increase efficiency, transparency, and the security of classified information.

5. Digital information

Adams (2003 p. 57) argues that information may be sensitive or classified for a variety of reasons—because it is highly personal, commercially valuable, or relevant to ongoing operations. He further states that "once information has been classified, agencies are required to observe certain minimum procedural requirements in handling, using, storing, transmitting and disposing of the information," (Adams 2003 p. 58).

Lin argues that over classification is a threat to national security because it inhibits information sharing within a bureaucracy. There are many reasons for over classification including a culture of secrecy, fear of repercussions for failing to protect sensitive information, lack of adequate time for the classifier to be able to classify appropriately, and concealing information in order to hide misconduct or incompetence (Lin 2014 p. 443-444). Lin (2014) points to several steps one could take to reduce overclassification. However, these could be subsumed in the structure offered by Leyzorek (1998). Leyzorek (1998 p. 47)argues that there are eight steps necessary to secure information: Determine the information to be protected;

Identify the individuals who handle sensitive information;

Define the ways that information is handled;

Define procedures for information protection;

Provide adequate access to needed information;

Balance security with operational effectiveness;

Develop controls and assign responsibility;

And, finally, develop employee training programs.

Elaborating on the eight steps, Leyzorek argues that in determining the information to be protected "the criterion to be employed in evaluating a given category of information as to its confidentiality is whether

some person or agency will be hurt if the information is released without authorization" the key is that "a clear distinction must be made between actual damage in the form of loss of money, reputation, or share of market, for example, versus simple embarrassment," (Leyzorek 1998 p. 47). On the second step, identifying the individuals who handle sensitive information, Leyzorek further states that there should be reference checks prior to employment. However, Schilde (2015 p. 176)debated staff vetting, pointing to the tensions that existed between NATO and a number of European states in the late 1990s and early 2000s. According to Schilde (2015 p. 176) "granting of security clearances based on lifestyle issues—rather than a record of security violations—was never integrated into the vetting processes of European states until 2005." (Leyzorek 1998 p. 47). On the second step, identifying the individuals who handle sensitive information, Leyzorek further states that there should be reference checks prior to employment. However, debated staff vetting, pointing to the tensions that existed between NATO and a number of European states in the late 1990s and early 2000s. According to Schilde (2015) "granting of security clearances based on lifestyle issues—rather than a record of security violations—was never integrated into the vetting processes of European states until 2005."

Leyzorek (1998 p. 47) expanded on defining the ways of information handling by stating that there should be detailed procedures for all types of formats. He adds that "electronic media present the most difficult problem" since they are not as easily inspected as paper. Regardless of physical or electronic format, however, professionals agree that it is complicated. Haight (1989 p. 36-37) argues that declassification is made complicated not just from identifying documents with security markings but also assessing documents that have no markings but may contain sensitive information. (David 2013) demonstrated that the US government has several information classification categories that made it especially complex to handle. Bennet adds to the discussion with an analysis of the declassification efforts within the UK Intelligence agencies. The analysis shows different levels of success in institutional efforts to undertake declassification processes determined by various factors including the lack of adequate historical records in the case of MI6 compared to MI5 and CGHQ (David 2013 p. 28). Leyzorek (1998 p. 47) expanded on defining the ways of information handling by stating that there should be detailed procedures for all types of formats. He adds that "electronic media present the most difficult problem" since they are not as easily inspected as paper. Regardless of physical or electronic format, however, professionals agree that it is complicated. argues that declassification is made complicated not just from identifying documents with security markings but also assessing documents that have no markings but may contain sensitive information. demonstrated that the US government has several information classification categories that made it especially complex to handle. Bennet adds to the discussion with an analysis of the declassification efforts within the UK Intelligence agencies. The analysis shows different levels of success in institutional efforts to undertake declassification processes determined by various factors including the lack of adequate historical records in the case of MI6 compared to MI5 and CGHQ .

In defining procedures for information protection, Leyzorek (1998 p. 47) states there should be specific procedures for the protection of classified information including how they are transmitted and ultimately disposed. Lin (2014 p. 444) similarly argues that there should be clear guides that govern how information is classified. Neither goes into great detail with suggestions or recommendations for these procedures though Leyzorek (1998 p. 47)does specify that precautions must be made for the use of personal computers where confidential data is created or stored with capabilities of locking files to prevent unauthorised access . Leyzorek (1998 p. 47) states there should be specific procedures for the

protection of classified information including how they are transmitted and ultimately disposed. similarly argues that there should be clear guides that govern how information is classified. Neither goes into great detail with suggestions or recommendations for these procedures though Leyzorek does specify that precautions must be made for the use of personal computers where confidential data is created or stored with capabilities of locking files to prevent unauthorised access .

Regarding adequate access, Leyzorek (1998 p. 48) recognizes that there should be a delicate balance between restricting and providing access. This ties in close with the sixth step about balancing security with operation effectiveness. Leyzorek (1998 p. 48) argues there is a need to balance between real as well as intangible costs versus the expected benefits of information security systems. He argues the cost of maintaining an effective information security system will increase relative to the amount of information categories and number of people that need to access the information. Aftergood (2008 p. 104), concerned with overclassification in the government, states that government agencies "should be specifically directed to seek out and identify classified information that no longer requires protection and that be publicly disclosed. The primary objective of the review should be to reduce classification to its minimum required scope" . (1998 p. 48) recognizes that there should be a delicate balance between restricting and providing access. This ties in close with the sixth step about balancing security with operation effectiveness. Leyzorek argues there is a need to balance between real as well as intangible costs versus the expected benefits of information security systems. He argues the cost of maintaining an effective information security system will increase relative to the amount of information categories and number of people that need to access the information. , concerned with overclassification in the government, states that government agencies "should be specifically directed to seek out and identify classified information that no longer requires protection and that be publicly disclosed. The primary objective of the review should be to reduce classification to its minimum required scope".

Aftergood (2010 p. 845)warns that there if often inadvertent, unintentional disclosure of classified information because the secret system "is porous and accident prone, failing to provide the protection that is its reason for existence". He further warns that with the growing dominance of electronic records, inadvertent disclosures seem to have steadily increased considering the speed of transmission and publication of information that is wrongly handled (Aftergood 2010 p. 845). Leyzorek (1998 p. 48) argues that the development of controls and assignment of responsibility would help mitigate these kinds of problems. He further states that there should be elaborate procedures and people responsible for those procedures, particularly for digital information. An important part of these systems should be the development of employee training programs. Leyzorek (1998 p. 48) alludes to the need for extensive and well-structured activities to ensure employees understand how to protect the organization's information.(Aftergood 2010 p. 845). argues that the development of controls and assignment of responsibility would help mitigate these kinds of problems. He further states that there should be elaborate procedures and people responsible for those procedures, particularly for digital information . An important part of these systems should be the development of employee training programs. alludes to the need for extensive and well-structured activities to ensure employees understand how to protect the organization's information.

Leyzorek (1998 p. 47) () argues that maintaining information security is as much a cultural challenge as it is a procedural one. Therefore, an organization should undertake changes at both ends of the challenge. Yarborough (2013) explores the tedious nature of procedural changes by outlining the breakdown of records management in the US Army during the Gulf War of the early 19990s. He explains that the loss

of records detailing where Army units were and when, and what they did there was "near-total collapse of the Army's system for managing operation records" (Yarborough 2013 p. 1428) . In order to address the crisis, President Clinton mandated efforts in the mid-1990s to collect, digitize and declassify records. Leyzorek (1998 p. 47)argues that maintaining information security is as much a cultural challenge as it is a procedural one. Therefore, an organization should undertake changes at both ends of the challenge. explores the tedious nature of procedural changes by outlining the breakdown of records management in the US Army during the Gulf War of the early 19990s. He explains that the loss of records detailing where Army units were and when, and what they did there was "near-total collapse of the Army's system for managing operation records" . In order to address the crisis, President Clinton mandated efforts in the mid1990s to collect, digitize and declassify records.

Aftergood (2008 p. 107) argues that the "continuing disputes over classification policy are inevitable due to the inherently subjective character of the classification process". Aftergood (2010 p. 841) later argued that the secrecy system does not exist in abstract isolation but is "an ordinary bureaucratic artifact that is subject to pressure on many levels—political, legal, sociological, international, and others". He points out that there are three categories of government secrecy: genuine national security secrecy, bureaucratic secrecy, and political secrecy (Aftergood 2009 p. 401). Genuine national security secrecy is the only legitimate form of secrecy and protects information that would pose a security threat to a nation "by compromising its defense or the conduct of its foreign relations" which may include "confidential diplomatic initiatives and other sensitive matters whose protection is not controversial and whose safeguards are the raison d'être of the classification system, and the public interest is served when this information remains secure" (Aftergood 2009 p. 401). The second category of information secrecy is 'bureaucratic secrecy' which reflects the Weberian drive to amass information in order to increase the superiority of the professionally informed. To be on the safe side, too much rather than too little information is classified and protected from the public scrutiny (Aftergood 2009 p. 401). Additionally, because classified information is considered to be more valuable than unclassified information, classification mechanisms are used to guard organizational authority, or as Oscar Wilde is believed to have said "the bureaucracy is expanding to meet the needs of the expanding bureaucracy" (Good Reads 2015).

The third category of information secrecy is 'political secrecy,' which misapplies the authority to classify for political advantage. While probably the smallest in quantitative terms, this form of secrecy is actually the most problematic and objectionable. It exploits the generally accepted legitimacy of genuine national security interests in order to advance a self-serving agenda, to evade controversy, or to thwart accountability (Aftergood 2009 p. 401). Even though there are legitimate reasons for classifying information, bureaucratic and political reasons may be abused. This may result in classification that is not based on risk analysis but rather merely protecting against disclosure that reveal embarrassing information or misconduct. These reasons are enough for organizations to often consider over-classifying information just to be on the safe side (Kastenhofer and Katuu 2016 p. 4).

6. Conclusion

This review of the literature revealed that there is little information on the topic of classified information within international organisations. Those few articles that specifically address this topic focus predominantly on access to classified information and in particular the declassification and disclosure

process. But much of the discussion on security classified happens at the national level. This discussion focuses on access to classified information and the management and protection of this information. There is a need for more literature on best practices and strategies for managing classified information, especially from a records and information management perspective. Furthermore, there is a need to further research the issue of security classified information within international organisations. As Dikker Hupkes indicated “the legal status, responsibilities, privileges and immunities of IGOs are all different from those of governments -- it is therefore important to discuss the information policy of IGOs as something also distinct from governmental information policy” (2009).

7. References

Abel, J. (2015). "Do You Have to Keep the Government's Secrets?: Retroactively Classified Documents, the First Amendment, and the Power To Make Secrets Out of the Public Record." University of Pennsylvania Law Review 167(1037): 1037-1096.

Adams, C. (2003). "Protecting classified and security sensitive information." Reform(83): 56-61.

Aftergood, S. (2000). "Secrecy is back in fashion." Bulletin of the Atomic Scientists 56(6): 24-30.

Aftergood, S. (2002). "Making Sense of Government Information Restrictions." Issues in Science & Technology 18(4): 25-26.

Aftergood, S. (2008). "If in Doubt, Classify." Index on Censorship 37(4): 101-107.

Aftergood, S. (2009). "Reducing Government Secrecy: Finding What Works." Yale Law & Policy Review 27(2): 399-416.

Aftergood, S. (2010). "National security secrecy: how the limits change." social research 77(3): 839-852.

Aftergood, S. (2013). "An Inquiry into the Dynamics of Government Secrecy." Harvard Civil Rights-Civil Liberties Law Review 48(2): 511-530.

Australia Law Reform Commission (2004). "Protecting Classified and Security Sensitive Information – Discussion Paper 67." Retrieved 12th November, 2017, from https://www.alrc.gov.au/sites/default/files/pdfs/publications/DP67.pdf.

Bennett, G. (2002). "Declassification and Release Policies of the UK's Intelligence Agencies." Intelligence and National Security 17(1): 21-32.

Castaner, G. (2014). "Description of Archival Holdings of the International Monetary Fund and the Project to Make Descriptions Available Online." Technical and Substantive Problems of Classical and

Electronic Archiving. Retrieved 25th April, 2017, from http://www.pokarh-mb.si/uploaded/datoteke/radenci2014/26_castaner_2014.pdf.

David, J. (2013). "Can We Finally See Those Records? An Update on the Automatic/Systematic Declassification Review Program." The American Archivist 76(2): 415-437.

Dikker Hupkes, S. D. (2009). "Protection and Effective Functioning of International Organizations. Final Report International Institutional Law; Secure Haven Project." Retrieved 22nd June, 2015, from https://openaccess.leidenuniv.nl/handle/1887/14119.

Eckman, C. (2005). "Information Classification and Access Policies at Selected IGOs." DttP: Documents to the People 33(2): 23-25.

Good Reads (2015). "Oscar Wilde Quotes." Retrieved 24th May, 2015, from http://www.goodreads.com/quotes/130452-the-bureaucracy-is-expanding-to-meet-the-needs-of-the

Haight, D. (1989). "Declassification of Presidential Papers: The Eisenhower Library's Experience." Provenance, Journal of the Society of Georgia Archivists 7(2): 33-53.

Hitchens, A. (1997). "A call for IGO policies on public access to information." Government Information Quarterly 14(2): 143-154.

Hooten, B. T. (2011). "How Many Times Can "Classidied" Be Said?". Retrieved 10th December, 2014, from http://members.rimpa.com.au/lib/StaticContent/StaticPages/pubs/nat/inForum2011/HootenPaper.pdf.

International Standards Organization (2013a). ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements. Geneva, International Standards Organization.

International Standards Organization (2013b). ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls. Geneva, International Standards Organization.

Kastenhofer, J. and S. Katuu (2016). "Declassification: A clouded environment." Archives and Records: The Journal of the Archives and Records Association 37(2): 1-27.

Kosar, K. R. (2010). Classified information policy and executive order 13526. Washington DC, Congressional Research Services, Library of Congress.

Leyzorek, M. (1998). "A missing feature in some records management systems." Information Management 32(4): 46-48.

Lin, H. (2014). "A Proposal to Reduce Government Overclassification of Information Related to National Security." Journal of National Security Law and Policy 7: 443-527.

Open Society Foundation (2013). The Global Principles on National Security and the Right to Information (Tshwane Principles). New York, Open Society Foundations & Open Society Justice Initiative.

Relyea, H. C. (2008). Security Classified and Controlled Information: History, Status, and Emerging Management Issues. Washington DC, Congressional Research Services; Library of Congress.

Roberts, A. (2004). "A partial revolution: The diplomatic ethos and transparency in intergovernmental organizations." Public Administration Review 64(4): 410-424.

Roche, N. (2015). "From top secret to publicly disclosed: engaging with NATO's declassified records." Comma(2): 55-65.

Schilde, K. E. (2015). "Cosmic top secret Europe? The legacy of North Atlantic Treaty Organization and cold war US policy on European Union information policy." European Security 24(2): 167-182.

Wallace, D. A. (1993). "Archivists, Recordkeeping, and the Declassification of Records: What We Can Learn from Contemporary Histories." American Archivist 56(4): 794-814.

Weaver, J. M. (2017). "Security of classified information: one standard or many?" International Journal of Public Leadership 13(1): 9-12.

Williams, R. V. (1988). "The role of intergovernmental organizations in international information transfer and policy." Special libraries 79(1): 1.

Yarborough, W. M. (2013). "Undocumented Triumph: Gulf War Operational Records Management." Journal of Military History 77(4): 1427-1438.