Jurnal Ilmu Informasi, Perpustakaan dan Kearsipan

Volume 25 | Number 2 Article 5

10-31-2023

Kepatuhan Persyaratan Fungsional Pengendalian Hak Akses pada OLA (Office Letter Automation) Berdasarkan ISO 16175-2: 2011

Trina Nur Faturohmah
Cowell Development, trina.nur@ui.ac.id

Achmad Fachmi
Ekosistem Kearsipan & Dokumen, achmad.fachmi90@gmail.com

Recommended Citation

Faturohmah, Trina Nur and Fachmi, Achmad (2023) "Kepatuhan Persyaratan Fungsional Pengendalian Hak Akses pada OLA (Office Letter Automation) Berdasarkan ISO 16175-2: 2011," *Jurnal Ilmu Informasi, Perpustakaan dan Kearsipan*: Vol. 25: No. 2, Article 5.
DOI: 10.7454/JIPK.v25i2.1001
Available at: https://scholarhub.ui.ac.id/jipk/vol25/iss2/5

KEPATUHAN PERSYARATAN FUNGSIONAL PENGENDALIAN HAK AKSES PADA OLA (*OFFICE LETTER AUTOMATION*) BERDASARKAN ISO 16175-2: 2011

Trina Nur Faturohmah[1], Achmad Fachmi[2]

[1] Cowell Development, Senen Raya, Jakarta Pusat, Indonesia.
[2] Ekosistem Kearsipan dan Dokumen, Cakung, Jakarta Timur, Indonesia.

trinafatturahman@gmail.com
achmad.fachmi90@gmail.com

Abstrak

Penelitian ini membahas tentang kepatuhan sistem *Office Letter Automation* (OLA) PT X terhadap persyaratan fungsional pengendalian hak akses berdasarkan ISO 16175-2 2011. PT X telah menggunakan sistem tersebut sejak tahun 2019, dan OLA merupakan aplikasi berbasis web yang digunakan untuk pengendalian kegiatan korespondensi dan kegiatan manajemen arsip elektronik di perusahaan. Penelitian ini bertujuan untuk mengidentifikasi apakah OLA memenuhi standar EDRMS terkait dengan hak akses atau *access control*. Penelitian ini menggunakan pendekatan kualitatif dengan cara studi literatur dan melakukan observasi untuk mengetahui ketepatan implementasi sesuai persyaratan standar ISO 16175-2:2011 yang diteliti dengan OLA sebagai objek penelitian. Hasil penelitian menunjukkan bahwa dari 17 persyaratan fungsional kontrol akses, OLA dapat memenuhi 16 persyaratan wajib. Sehingga belum memenuhi standar minimum persyaratan yang diminta oleh standar dan masuk dalam temuan mayor. Untuk itu organisasi perlu melakukan tindakan perbaikan dan pencegahan agar OLA dapat patuh dengan permintaan standar ISO 16175-2 2011. Namun, secara keseluruhan OLA sudah cukup baik dalam mendukung kegiatan manajemen arsip elektronik khususnya untuk sistem keamanan pada bagian hak akses.

Kata kunci: *akses kontrol; EDRMS; arsip elektronik; sistem keamanan; Office Letter Automation*

Abstract

This research discusses the compliance of PT X's Office Letter Automation (OLA) system with the functional requirements for controlling access rights based on ISO 16175-2 2011. PT X has been using the system since 2019, OLA is a web-based application used to control correspondence and other activities. Electronic records management in PT X. This research aims to identify whether OLA meets EDRMS standards related to access rights or access control. This research uses a qualitative approach by studying literature and making observations to identify the implementation accuracy according to the ISO 16175-2:2011 standard requirements, which is examined with OLA as the research object. The research results show that of the 17-access control functional requirements, OLA can fulfill 16 mandatory requirements. So, it does not meet the minimum standards required by the standards and is included in the major findings. For this reason, organizations need to take corrective and preventive actions so that OLA can comply with the ISO 16175-2 2011 standard requirements. However, overall, OLA is good enough to support electronic security management activities, especially for security systems in the access rights section.

Keywords: *access control; EDRMS; electronic records; security system; Office Letter Automation*

I. PENDAHULUAN

Berkembangnya teknologi saat ini menjadikan individu maupun organisasi semakin berlomba untuk berusaha memenuhi kebutuhan dengan mengembangkan dan mengimplementasikan teknologi dalam kehidupan sehari-hari agar aktivitas yang dilakukan menjadi lebih efektif dan efisien. Teknologi informasi menjadi salah satu bagian yang dikembangkan organisasi guna mendukung aktivitas bisnis, seperti pengelolaan arsip. Saat ini arsip tidak hanya dalam bentuk konvensional/kertas tetapi juga dalam bentuk elektronik. Ini memberikan efek yang positif bagi organisasi saat ini seperti, temu kembali informasi yang efektif dan efisien, pengindeksan yang fleksibel, pencarian secara penuh, memperkecil kehilangan, tak terbatas tempat, mudah untuk berbagi, menjaga keamanan, memberi kemudahan

untuk memulihkan data, dan mengurangi risiko kerusakan fisik (Anugrah, 2020).

Melihat fenomena tersebut, tentunya memberikan keuntungan yang baik pada pengelola arsip, Namun, juga memberikan sebuah tantangan baru untuk dapat mengelola arsip dalam bentuk konvensional dan elektronik. Untuk itu dibutuhkan sistem otomasi pengelolaan kearsipan, dengan menerapkan sistem otomasi yang memungkinkan terjadinya integrasi kegiatan pengelolaan dokumen dan arsip pada kegiatan bisnis organisasi. Dengan demikian, dapat dihindari kesalahan penyampaian informasi dan juga meningkatkan efektif dan efisiensi kerja dari sebuah organisasi karena bantuan teknologi (Svärd, 2017). Sistem otomasi tersebut yang dikenal dengan *Electronic Document and Record Management System* (EDRMS) yang lahir pada tahun 1999 dan dengan seiringnya perkembangan teknologi EDRMS terus berkembang. EDRMS memang dikhususkan untuk kegiatan manajemen dokumen dan arsip mulai dari penciptaan, pengelolaan, pemanfaatan, hingga pemusnahan (Rahma dan Mayesti, 2019).

Seperti pada PT X salah satu perusahaan BUMN yang mendorong perkembangan teknologi informasi dalam pengelolaan arsip, pada awalnya kegiatan pengelolaan arsip masih serba konvensional atau manual. Kemudian, dengan kemauan untuk berkembang dan mengikuti zaman kegiatan pengelolaan arsip beralih menjadi dengan memanfaatkan sistem otomasi manajemen arsip. Hal tersebut terjadi karena pada organisasi tersebut memiliki departemen yang cukup banyak sehingga membutuhkan kecepatan yang cukup tinggi untuk menunjang kegiatan bisnis organisasi. Sampai pada tahun 2019 sistem otomasi yang bernama *Office Letter Automation* (OLA) resmi dipublikasikan untuk dipergunakan dalam ruang lingkup internal di seluruh departemen yang berada di PT X. Selama kurang lebih dua tahun proses implementasi teknologi informasi berjalan, EDRMS ini dikembangkan guna memberikan kemudahan dalam proses administrasi dan meningkatkan kecepatan, ketepatan, serta produktivitas kegiatan bisnis organisasi.

Bila berbicara terkait dengan EDRMS, tentu akan memengaruhi banyak aspek, salah satunya adalah hak akses dan keamanan. Sebab, kontrol akan hak akses arsip memiliki tujuan untuk menjaga otentisitas dan reliabilitas arsip serta mengamankan integritas sebuah arsip (Rustam, 2019). Oleh karena itu penting bagi EDRMS memiliki standar yang mengatur kegiatan kontrol akan keamanan dan hak akses. Di dalam EDRMS terdapat *required functionality* yang tiap-tiap sistem akan berbeda-beda dari tiap-tiap organisasi tergantung kebutuhan dan tujuan spesifik organisasi. Namun, perlu diperhatikan bahwa, terdapat *core set of required functionality* yang harus sesuai (Adam, 2007). Untuk itu dibutuhkan standar yang dapat digunakan sebagai panduan dalam melakukan pengelolaan EDRMS. Salah satunya ISO 16175-2: 2011 *Information and documentation - Principles and functional requirements for record in electronic office environments - Part 2: Guidelines and functional requiremnts for digital records management systems*, yang dapat digunakan menjadi standar pedoman pengelolaan EDRMS.

Terkait dengan hal tersebut, terdapat beberapa penelitian yang juga membahas pemenuhan persyaratan ISO 16175-2: 2011, seperti penelitian oleh Fachmi dan Mayesti (2021) mengenai kepatuhan persyaratan hak akses pengguna EDRMS pada aplikasi pengelolaan arsip elektronik berbasis web yang disebut dengan Arteri(Arsip Elektronik Terintegrasi). Ditemukan bawah pada sistem Arteri hanya dapat memenuhi 12 dari 17 persyaratan kinerja manajemen wajib, artinya Arteri yang merupakan EDRMS belum memenuhi standar minimum yang disyaratkan oleh standar. Selain itu, dalam penelitian Rahma dan Mayesti (2019) tentang EDRMS di Kementerian Kelautan dan Perikanan Republik Indonesia yang disebut SIKap (Sistem Informasi Kearsipan), hanya 13 dari 17 persyaratan yang terpenuhi. Meskipun tidak sesuai dengan standar ISO 16175-2: 2011, administrator utama sudah dapat mengontrol penggunaan keamanan dengan memberikan keamanan yang berlapis pada sistem.

Berdasarkan pemaparan di atas maka pertanyaan penelitian dari penelitian ini adalah bagaimana OLA di PT X dapat mengelola hak akses. Tujuan penelitian ini adalah menganalisis kepatuhan fungsional pada hak akses EDRMS OLA berdasarkan standar ISO 16175-2:2011 sehingga hasil penelitian ini dapat digunakan sebagai masukan dan pengembangan PT X dalam memperbarui dan meningkatkan sistem OLA.

https://scholarhub.ui.ac.id/jipk/vol25/iss2/5
DOI: 10.7454/JIPK.v25i2.1001

II. TINJAUAN LITERATUR

A. Arsip Elektronik

Menurut ISO 15489-1:2016 *Information and Documentation Records management* pada Part 1 *Concepts and principles*:

"*General Records are both evidence of business activity and information assets. Any set of information, regardless of its structure or form, can be managed as a record. This includes information in the form of a document, a collection of data or other types of digital or analogue information which are created, captured and managed in the course of business*" (The International Standard Organization, 2016)

Arsip merupakan bukti kegiatan kerja dan aset organisasi terkait dengan informasi dalam bentuk apa pun. Hal ini termasuk informasi dalam bentuk dokumen, koleksi data atau jenis lain dari informasi analog atau digital yang diciptakan, ditangkap, dan dikelola dalam rangkaian pekerjaan. Arsip elektronik berisi informasi yang dapat dibaca oleh manusia dan mesin termasuk gambar, video dan grafik, termasuk juga rekaman suara dan musik yang dihasilkan oleh komputer (Saffady, 2009). Di lingkungan kerja saat ini, arsip elektronik semakin banyak dibuat dan disesuaikan dengan kepentingan masing-masing lembaga baik pemerintahan maupun swasta.

Perkembangan teknologi informasi tentu memberikan pengaruh dan tantangan tersendiri bagi industri kertas. Dengan masifnya informasi dalam bentuk elektronik, sektor industri kertas harus berjuang dalam gempuran perkembangan teknologi saat ini. Hal tersebut tentu berdampak pada kegiatan pembuatan dan pengarsipan surat, formulir, dan catatan kertas lainnya. Oleh karena itu sebagian besar organisasi berpandangan bahwa arsip elektronik adalah sumber informasi yang dapat diandalkan untuk kegiatan bisnis sehari-hari, serta perencanaan jangka panjang, dan pengambilan keputusan.

B. Otomasi Manajemen Arsip

Teknologi canggih telah bekerja dengan baik, salah satunya adalah kemungkinan otomasi kegiatan pengarsipan. Otomasi tersebut merupakan tahapan dari mulai arsip diciptakan, dikelola, digunakan disimpan dan sampai dengan kegiatan temu kembali informasi. Namun, perlu diketahui pada arsip elektronik memiliki pengelompokan yang berbeda dalam format dan media yang berbeda. Pengenalan otomasi memastikan efisiensi, mengurangi, atau mengembangkan kebutuhan duplikasi jika diperlukan, transfer data, pemrosesan, penyimpanan, dan pencarian informasi dapat dilakukan secara otomatis menggunakan sistem (Mulyantono, 2016).

Sistem otomasi manajemen arsip adalah sistem yang digunakan untuk mendukung pelaksanaan manajemen arsip dan merupakan bagian integral dari pelaksanaan manajemen arsip secara komputerisasi atau berbasis komputer. Menurut *International Council on Archives*, sistem manajemen arsip elektronik adalah sistem yang dirancang khusus untuk mengelola pemeliharaan dan pembuangan arsip. Sistem mempertahankan konten, konteks, struktur, dan tautan antar dokumen untuk memungkinkan aksesibilitas dan mendukung nilai tampilan dokumen (ISO 16175-2: 2011 – *Principles and Functional Requitements for Records in Electronic Office Environments*, 2011). Pendapat lain mengatakan bahwa manajemen arsip elektronik memiliki fungsi yang mendukung lokasi, organisasi, klasifikasi, penyimpanan, pengambilan, penggunaan, dan pembuangan arsip elektronik, metadata, dan arsip fisik (NARA, 2023).

C. Electronic Document and Record Management System (EDRMS)

Berkembangnya teknologi saat ini menjadikan perusahaan semakin berlomba untuk mengembangkan implementasi sistem informasi sebagai pendukung kegiatan bisnis perusahaan. Penerapan teknologi khususnya teknologi informasi, yaitu untuk menganalisis kegiatan kerja organisasi, meningkatkan kualitas penyebaran informasi, membantu aktivitas manajemen, serta efisiensi terhadap waktu dan biaya. Salah satu penerapan teknologi informasi Perusahaan, yaitu pada pengelolaan dokumen dan arsip yang disebut *Electronic Document and Record Management System* (EDRMS) yang dijelaskan oleh Azad Adam (2007) "*In electronic document and records management systems (EDRMS), a record can be defined as an electronic folder consisting of one or more documents"* yang berarti bahwa dalam sistem manajemen dokumen dan arsip, arsip dapat didefinisikan sebagai folder elektronik yang terdiri dari satu atau lebih dokumen.

Pasal satu (1) Peraturan Arsip Nasional Republik Indonesia Nomor 6 Tahun 2021 tentang Pengelolaan

Arsip Elektronik menjelaskan bahwa pengelolaan arsip elektronik adalah proses yang efektif dan efisien dalam pengendalian arsip elektronik secara sistematis. Hal tersebut meliputi penyiapan, penerimaan, penggunaan, pengawetan, pemeliharaan, pemindahan pembawa data, penghapusan, per*ole*han, pendeskripsian, pengolahan, pengawetan, pengaksesan, dan penggunaan. Maka perubahan pada praktik dari manajemen arsip tercetak ke manajemen arsip elektronik, membutuhkan pengawas dari berbagai pemangku kepentingan seperti pengawas, vendor, manajer, dan pengetahuan staf dengan pengalaman dalam implementasi EDRMS yang diperlukan untuk mengatasi kendala atau kesulitan yang dihadapi oleh pengguna. (Joseph et al., 2012).

D. Hak Akses Arsip

Pengertian akses adalah hak, kesempatan dalam arti informasi dalam suatu arsip dapat dicari, digunakan, dan diambil kembali (Badan Standardisasi Nasional, 2018). Untuk itu sebaiknya organisasi mengembangkan pedoman atau aturan tertulis yang menentukan siapa yang memiliki akses ke arsip sesuai dengan kebutuhan masing-masing. Akses ke arsip dibatasi hanya jika diperlukan secara khusus oleh persyaratan bisnis atau hukum. Pemberian hak akses terlebih dahulu ditentukan oleh badan usaha pemilik arsip karena arsip dapat bersifat pribadi, komersial, atau mengandung informasi sensitif atau rahasia, dan pembatasan akses dapat digunakan untuk pihak internal arsip maupun eksternal organisasi (Badan Standardisasi Nasional, 2018).

Pada persyaratan sistem manajemen yang disebutkan oleh Kennedy dan Schauder (1998) terdapat beberapa fungsi akses yang harus disediakan oleh sistem otomasi manajemen arsip. Salah satunya adalah menciptakan akses pengguna yang efektif sebagai fungsi keamanan yang dapat menentukan hak akses dan pembatasan akses ke *file* dan catatan individual. Pembatasan akses yang dimaksud seperti menentukan akses pengguna. hak untuk melihat, memodifikasi atau menghapus *file* sistem, membatasi akses pengguna ke modul atau fungsi sistem tertentu, menentukan hak akses individu atau grup, memiliki pengguna milik beberapa grup, dan memiliki hak akses yang berbeda tergantung pada pembatasan lokasi (elektronik dan fisik) dalam grup tempat pengguna dapat menyimpan catatan.

III. METODE PENELITIAN

Penelitian ini menggunakan metode *literature review* dan observasi terhadap objek yang diteliti. Tinjauan pustaka atau *literature review* merupakan metode untuk memahami kajian literatur ilmiah suatu topik tertentu dengan menempatkan konteks tertentu pada sumber-sumber seperti tulisan akademik. Cakupan dari tinjauan literatur, yaitu evaluasi kritis terhadap materi. Oleh karena itu, metode ini tidak disebut sebagai laporan literatur, tetapi tinjauan literatur (University of Edinburgh, 2023). Terdapat dua tujuan utama dari tinjauan literatur, yaitu 1) melakukan diskusi peneliti sendiri tentang konten dan evaluasi kritis terkait topik penelitian dan 2) meninjau konten yang mencakup bukti yang ada, penelitian, dan teori.

Proses analisis data menggunakan ISO 16175-2: 2011 - Prinsip dan persyaratan fungsional untuk dokumen elektronik di lingkungan kantor sebagai pedoman standar dan kepatuhan yang harus dipenuhi oleh OLA sebagai objek observasi. Kegiatan observasi merupakan proses untuk mengidentifikasi ketepatan penerapan sesuai dengan standar yang diperiksa dengan cara melihat kesesuaian OLA dengan *checklist* permintaan persyaratan pada ISO 16175-2:2011 yang berfokus pada 17 persyaratan wajib terkait dengan hak akses. Diketahui bahwa pada tahun 2011 ISO mengadopsi ISO 16175-2:2011 *Principles and Functional Requirements for Records in Electronic Office Environments* (ICA-REQ) yang diterbitkan oleh *International Council on Archives* (ICA) sebagai kerangka dasar. Prinsip-prinsip catatan dan persyaratan kerja di lingkungan kantor elektronik. Di dalam ISO 16175-2: 2011 – *Principles and functional requitements for records in electronic office environments* yang cakupan bagian ISO ini hanya terbatas pada produk yang sering diistilahkan sebagai EDRMS untuk aplikasi perangkat lunak yang fungsi utamanya adalah dalam manajemen arsip dan memberikan panduan pada prinsip dan fungsi terkait pengelolaan yang digunakan dan disimpan dalam sistem bisnis (ISO 16175-2: 2011 – *Principles and Functional Requitements for Records in Electronic Office Environments*, 2011). ISO 16175-2: 2011 memiliki 5 (lima) klausa, pada klausa 5. *Functional Requirments* terdapat 4 (empat)

https://scholarhub.ui.ac.id/jipk/vol25/iss2/5
DOI: 10.7454/JIPK.v25i2.1001

klompok utama/subklausa, yaitu: 5.1. *Create*; 5.2. *Maintain*; 5.3. *Disseminate*; dan 5.4. *Administer*.

IV. PEMBAHASAN

A. Subklausa 5.4.3 – Access Control

Subklausa pertama pada Persyaratan fungsional untuk hak akses, yaitu *access control*, dalam subklausa tersebut terdapat 1 (satu) persyaratan yang diminta oleh ISO 16175-2: 2011, yaitu nomor 91 tentang pembagian peran akses pengguna atau yang sering disebut dengan RBAC (*Role-based access control*). RBAC sendiri merupakan model pembagian akses kontrol menurut *role*/peran dari pengguna dalam sebuah organisasi.

Pada model RBAC yang paling sederhana struktur akses didefinisikan oleh tiga *set*, yaitu 1). *set* U untuk *users*/pengguna; 2). *set* R untuk *roles/*peran; dan 3). dan *set* S *of services*/layanan. Juga terdapat 2 (dua) relasi, yaitu (*user-role assignment*/penugasan peran pengguna UA $\subset$ U×R dan *role-service assignment*/peran-penugasan layanan SA $\subset$ R×S). Pengguna *u* memenuhi syarat untuk mengakses layanan *s* jika dan hanya jika terdapat peran *r* sehingga (u, r) $\in$ UA dan (r, s) $\in$ SA (Cruz et al., 2018).

TABEL 1. ACCESS CONTROL REQUIREMENT

No.	Persyaratan	V/X
91	*Restrict access to system functions according to a user's role and strict system administration controls*	V

Dari Tabel 1. dapat diketahui bawah OLA sebagai EDRMS telah memenuhi persyaratan nomor 91 dari subklausa 5.4.3 – *Access Control.* Dalam OLA terdapat *role access* atau yang disebut dengan *role dat*a yang berarti setiap pengguna diberikan akses yang berbeda-beda sesuai dengan peran dan hirarki dalam organisasi. Dalam sistem OLA sendiri terdapat beberapa *role* akses, yaitu, pertama *role* akses yang memiliki seluruh akses dan tertinggi adalah *super admin* yang dapat mengatur dan mengubah data OLA dan unit yang bertanggung jawab adalah *corporate secretary* (Corsec) dan PIC dari IT *Officer*. Corsec sendiri dalam memberikan akses dan membatasi akses pada sistem OLA akan mengacu pada SOP alur surat di PT X. Selanjutnya, adalah administrator yang mendapat akses hanya terkait dengan data terkait unitnya saja. Untuk *role* administrator umumnya yang bertanggung jawab adalah sekretaris pada tiap-tiap unit kerja di PT X. Untuk yang ketiga dan terakhir adalah *role user* merupakan karyawan yang diberikan akses dan beraktivitas pada OLA sesuai ruang lingkup unitnya saja dan tidak dapat memberikan akses serta tidak dapat membatasi pengguna lain.

Maka dengan terpenuhinya persyaratan nomor 91 pada subklausa 5.4.3 – *Access control* maka PT X dalam melakukan manajemen arsip pada aplikasi OLA telah melakukan prinsip seperti *Auditability, Confidentiality, information integrity, high availability*, dan *adherence to policy* (Holliday, 2009). PT X memperhatikan betul dalam pengelolaan arsip elektronik terkait dengan konsep keamanan arsip, yaitu cara kontrol akses pada sistem untuk diberikan *role-role* akses pada pengguna aplikasi OLA. Dengan demikian, potensi terjadinya *data breach* dapat diperkecil. Selain itu, dengan terpenuhinya persyaratan sub- klausa 5.4.3 pada OLA maka hal tersebut sesuai dengan argumen Sutirman (2016) yang mengatakan bahwa EDRMS merupakan aplikasi manajemen arsip elektronik yang memiliki kelebihan terkait dengan keamanan serta pengendalian akses pada sistem kearsipan dengan adanya fitur kontrol akses dan pembagian *role* akses. Oleh karena itu, ide dasar dari RBAC terkait dengan pemberian kewenangan pemberian akses mengikuti hierarki organisasi yang lahir pada tahun 1992 masih relevan hingga saat ini.

B. Subklausa 5.4.3 – Establish Security Control

Selanjutnya pada subklausa 5.4.3 – *Establish Security Control* terdapat 4 (empat) persyaratan yang terdapat di dalamnya, mulai dari nomor 92 sampai dengan nomor 95. Tujuannya adalah sebagai kontrol keamanan sistematis atas akses, kemudahan ditemukan, dan pencarian mendukung pemeliharaan *authenticity, reliability, integrity* dan *usability* (ISO 16175-2: 2011 – Principles and Functional Requitements for Records in Electronic Office Environments, 2011). Oleh karena itu, subklausa

5.4.3 – *Establish Security Control* harus dilaksanakan dengan tepat. Hal ini menjadi penting karena dengan penilaian risiko dapat menginformasikan keputusan bisnis tentang seberapa ketat kontrol yang diperlukan, sebagai *log-audit*, dan juga untuk membuktikan bahwa tindakan yang disetujui dilakukan oleh orang yang berwenang. Persyaratan-persyaratan pada subklausa 5.4.3 – *Establish Security Control* dapat dilihat pada tabel 2 sebagai berikut.

TABEL 2. ESTABLISH SECURITY CONTROL REQUIREMENT

No.	Persyaratan	V/X
92	*Allow only administration to set up user profiles and allocate users to groups*	**V**
93	*Allow only administrator to limit access to records, aggregations and records management metadata to specified users or user groups*	**V**
94	*Allow the administrator to alter the security category of individual records*	**V**
95	*Allow changes to security attributes for groups or users (such as access rights, security level, privileges, initial password allocation and management) to be made only by the administrator*	**V**

Dari keempat yang disyaratkan pada subklausa 5.4.3, OLA telah memenuhi semua persyaratan-persyaratan yang diminta pada standar. Pada persyaratan nomor 92 *role super admin*, yaitu Corsec di PT X dapat membuatkan pengguna baru sesuai dengan permintaan dan prosedur atau SOP yang sudah ada. Selanjutnya, pada persyaratan nomor 93 Corsec memberikan akses ke karyawan dan unit-unit terkait sesuai dengan perannya masing-masing.

Pada persyaratan nomor 93 juga Corsec memberikan batasan akses dan dapat memasukkan karyawan pada grup/unit kerja di PT X sesuai dengan *role* dan permintaan dari manajemen. Batasan-batasan ini berlaku untuk semua karyawan yang terdapat di PT X, contohnya pada satu unit/grup karyawan yang diberikan akses hanya dapat melakukan aktivitas pada unit/grup kerja tersebut. Sementara itu, *role* administrator unit dapat melakukan aktivitas lebih hanya pada unit kerja atau grup masing-masing.

Selanjutnya, pada persyaratan nomor 94 dan 95 perubahan hak akses pada dasarnya dapat dilakukan oleh *super admin* atau Corsec sehingga untuk dapat melakukan ini pengguna atau karyawan dapat meminta sesuai prosedur atau SOP alur surat yang terdapat di PT X. Untuk itu permintaan akses juga harus disetujui dan direkomendasikan oleh atasannya/VP. Dengan demikian, kontrol terkait siapa saja yang dapat mengakses pada OLA dapat berjalan dengan baik dan menjaga keamanan pada informasi yang terkandung arsip elektronik.

Pada persyaratan-persyaratan yang terdapat pada subklausa 5.4.3 terkait dengan keamanan kontrol, yaitu persyaratan nomor 92 sampai dengan persyaratan nomor 95 merupakan klausa yang erat kaitannya dengan keamanan secara administratif yang dapat dikenal dengan *administrative safeguards*. Keamanan administratif tersebut adalah pengamanan kontrol dalam bentuk kebijakan, praktik, dan prosedur di suatu organisasi untuk diperiksa secara teratur terkait akses yang diberikan guna menekan kerentanan dan meningkatkan keamanan di organisasi (Kruse et al., 2017). Lebih lanjut, Kruse (2017) mengatakan bahwa analisis manajemen risiko, dan karyawan yang diberikan akses dengan *role* tertentu perlu dilakukan. Ini merupakan tujuan yang sama, yang diminta oleh ISO 16175-2: 2011 pada subklausa 5.4.3. Karena subklausa tersebut meminta untuk dipatuhi agar dapat melakukan penilaian risiko terkait dengan ancaman-ancaman keamanan kontrol dari OLA. Pada PT X sendiri telah secara sistematis dan terstruktur tertuang dalam prosedur berupa SOP yang dijadikan panduan dalam pemberian akses untuk karyawan.

C. Subklausa 5.4.4 – Assigning Security Levels

Berikutnya terdapat 6 (enam) persyaratan yang diminta dalam Subklausa 5.4.4 – *Assigning Security Levels*, yaitu mulai dari nomor 96 sampai dengan nomor 101. Diketahui bawah untuk setiap EDRMS harus atau wajib memenuhi persyaratan-persyaratan ini, dengan keamanan arsip elektronik lebih terjamin dengan adanya level keamanan. Hal tersebut sesuai dengan pendapat Sugiarto dan Wahyono (2015) yang mengatakan bawah terdapat 10 kelebihan dari

https://scholarhub.ui.ac.id/jipk/vol25/iss2/5
DOI: 10.7454/JIPK.v25i2.1001

pengelolaan arsip elektronik salah satunya, yaitu terkait dengan keamanan data.

TABEL 3. ASSIGNING SECURITY LEVELS REQUIREMENT

No.	Persyaratan	V/X
96	*Allow only the administrator to attach to the user profile attributes that determine the features, records management metadata fields, records or aggregations to which the user has access. The attributes of the profile will:* • *Prohibit access to the digital records management system without an accepted authentication mechanism attributed to the user profile* • *Restrict user access to specific or aggregations* • *Restrict user access according to the user's security clearance* • *Restrict user access to particular features (for example, read, update and/or delete specific records management metadata fields)* • *Deny access after a specified date, and* • *Allocate the user to a group or groups*	**V**
97	*Be able to provide the same control functions for roles, as for users.*	**V**
98	*Be able to set up groups of users that are associated with an aggregation.*	**V**
99	*Allow a user to be a member of more than one group.*	**V**
100	*Be able to limit users access to parts of the list (to be specified at the time of configuration)*	**V**
101	*Allow a user to stipulate which other users or groups can access records that the user is responsible for.*	**V**

Dimulai pembahasan dari nomor 96 dan 97, pada OLA sendiri persyaratan tersebut sudah terpenuhi yang berarti implementasi dari *Attribute Based access Control* (ABAC) juga telah dilaksanakan. Model ABAC sendiri tidak hanya terdapat pada persyaratan nomor 91 tetapi juga pada persyaratan 96 dan 97 yang memberikan *super admin*, yaitu Corsec untuk dapat memberikan atribut-atribut pada user atau karyawan yang menggunakan OLA. Seperti yang dijelaskan sebelumnya bahwa Corsec PT X memiliki kewenangan untuk membatasi akses karyawan kepada arsip-arsip tertentu tergantung hierarki dan permintaan akses. Pada *role user* sendiri akses hanya dapat diberikan untuk karyawan yang terdapat di unitnya masing-masing sehingga kegiatan lainnya tidak dapat dilakukan baik untuk membaca, membuat ataupun menghapus yang bukan dari unitnya berasal.

Di dalam OLA sendiri untuk akses aplikasi tersebut, dibutuhkan otentikasi bertingkat dengan menggunakan ID dan kata sandi kemudian memasukkan *role* data yang hanya menampilkan *office code* dari tiap-tiap karyawan sesuai dengan *role* masing-masing. Selain itu, aplikasi OLA juga menyediakan fitur *deadline* yang merupakan fitur terkait waktu atau tanggal tertentu untuk mengakses. Hal ini erat kaitannya dengan tugas dan tanggung jawab pengelola arsip, seperti pada kode etik pada pengelola arsip Australia memiliki nilai-nilai untuk para pengelola arsip untuk dapat menjelaskan dan memberikan batasan terkait dengan akses dan kontrol secara adil bagi organisasi (Kistanto et al., 2014). Maka dapat dipahami bawah permintaan standar tidak akan lepas dari nilai-nilai pengelola arsip walau medium atau jenis pengelolaan arsip berkembang dari konvensional sampai dengan perkembangan saat ini, yaitu di medium digital. Cara dan nilai dalam pengelolaan akan tetap menjadi landasan yang harus terpenuhi dalam manajemen kearsipan.

Selanjutnya pada persyaratan nomor 98 dan 99 pada aplikasi OLA juga telah terpenuhi. Persyaratan ini erat kaitannya dengan pengelompokan atau pembagian akses karyawan di grup-grup atau unit-unit kerja. Pada Fachmi dan Nina (2021) diberikan contoh oleh ICA bahwa yang dimaksudkan dalam persyaratan 98, yaitu pembagian grup/unit kerja seperti grup 'HRD'atau 'Sales'. Pada aplikasi OLA hal tersebut juga disediakan pembatasan akses yang akan dilaksanakan sesuai dengan *role* dan juga unit kerja masing-masing. Hal tersebut dapat ditemui

ketika pengguna masuk dan mengakses pada halaman *dashboard*.

Berikutnya pada persyaratan nomor 100 dan nomor 101 juga telah terpenuhi oleh aplikasi OLA. Sebagai EDRMS, aplikasi OLA memiliki kemampuan untuk membatasi akses karyawan sesuai dengan hierarki, unit kerja, dan *role* yang diberikan. Adapun, terkait dengan penetapan siapa saja yang dapat mengakses arsip tertentu itu akan dibedakan dari *role* yang digunakan karena *role* yang digunakan mengacu pada prosedur serta memiliki tugas dan tanggung jawab masing-masing.

Seperti pada persyaratan 91, terdapat beberapa tingkatan yang terdapat pada organisasi PT X. Pertama, yaitu *super admin* memiliki otoritas dan akses yang luas juga memiliki kemampuan untuk memberikan *role* pada karyawan PT X lainnya. *Super admin* dapat memberikan *role* administrator kepada karyawan yang memiliki level di bawah VP. Sementara, untuk *role user* diberikan untuk pelaksana di bawah administrator dalam sebuah unit kerja. Namun, hak akses yang diberikan hanya melakukan aktivitas kerja di dalam unit tersebut dan tidak lebih besar aksesnya dari administrator.

Akan tetapi, penting untuk dipertimbangkan bawah hal tersebut dilakukan berdasarkan SOP yang sudah ada. Itu merupakan kebijakan dari organisasi untuk memberikan izin serta menentukan hak akses karyawan PT X dalam penggunaan aplikasi OLA. Tentunya pada persyaratan ini pengelola arsip dengan menggunakan sistem OLA telah melakukan hal-hal yang diamanatkan dalam undang-undang kearsipan Nomor 43 tahun 2009 pada pasal 44 poin 2 (dua) dan 3 (tiga), yaitu pengelola arsip wajib menjaga kerahasiaan arsip dan pengelola arsip wajib menentukan prosedur berdasarkan standar pelayanan (Republik Indonesia, 2009). Selain itu, penting bagi organisasi untuk dapat menentukan *level* atau klasifikasi keamanan dalam menentukan hak akses. terdapat beberapa langkah yang perlu diperhatikan ketika membuat kebijakan terkait hal tersebut seperti menganalisis fungsi unit kerja, analisis risiko, analisis *job description*, dan juga ketentuan-ketentuan hukum maupun kebijakan yang terdapat di dalam organisasi tersebut. (Sari dan Rahmah, 2013).

D. Subklausa 5.4.5 – Executing Security Controls

Untuk klausa terakhir pada persyaratan hak akses pada EDRMS, yaitu menjalankan kontrol keamanan yang terdapat pada subklausa 5.4.5. Pada subklausa ini terdapat 6 (enam) poin persyaratan yang diminta oleh standar ISO, mulai dari nomor 102 sampai dengan nomor 107. Pembahasan akan dimulai dari nomor 103 sampai dengan nomor 104 yang dapat dilihat pada tabel 4 sebagai berikut.

TABEL 4. EXECUTING SECURITY CONTROLS REQUIREMENT

No.	Persyaratan	V/X
102	*Allow the administrator, subject to section 5.4.6 security categories, to alter the security category of all records within an aggregation in one operation. The digital records management system shall provide a warning if the security classifications of any records are lowers, and await confirmation before completing the operation.*	**V**
103	*Allow the administrator to change the security category of aggregations, subject to the requirements of section 5.4.6 security categories*	**V**
104	*Records full details of any change to security category in the records management metadata of the record, volume or aggregation affected*	**V**
105	*Provide one of the following responses (selectable at configuration time) whenever a user request access to, or searches for, a record, volume or aggregation that they do not have the right to access* • *Display title and records management metadata* • *Display the existence of an aggregation or records (that is, display its file or record number) but not its title or other records management metadata; or* • *Not display any record information or indicate its existence in any way*	**V**
106	*Never include, in a list of full text or other search result, any record that the user does not have the right to access*	**V**
107	*Log all unauthorized attempts to access aggregations (and their volumes) or records in their respective unique metadata*	X

https://scholarhub.ui.ac.id/jipk/vol25/iss2/5
DOI: 10.7454/JIPK.v25i2.1001

Pada persyaratan nomor 102, 103, dan 104, aplikasi OLA telah memenuhi ketiga permintaan standar ISO tersebut. Permintaan-permintaan tersebut terkait bagaimana sistem yang dikelola oleh admin dapat mengubah batasan keamanan serta memiliki *log history* atau *log activity*. *Log* tersebut menjadi hal penting karena terkait dengan evaluasi dan audit sistem akan berpengaruh dan menjadi *evidence* dari setiap aktivitas yang telah dilakukan dan itu bersifat harus terpenuhi dan dilakukan.

Dengan tercatatnya aktivitas tersebut maka sistem pengelolaan arsip tersebut menjadi sistem yang aman. Hal tersebut tentu akan dipertimbangkan dalam *risk register* bila tidak ada. Hal tersebut sejalan dengan pendapat dari Rahma dan Mayesti (2019) yang menyatakan bawah dalam sebuah EDRMS, admin sistem harus dapat melakukan *tracking* pada setiap aktivitas kegiatan yang dilakukan pada EDRMS serta dapat menarik *log activity* yang dilakukan di dalam aplikasi baik itu aktivitas bisnis maupun aktivitas perubahan status keamanan terhadap data yang terdapat di dalamnya.

Pada organisasi PT X sendiri, terdapat PIC dari unit IT *Officer* yang berkewajiban untuk memelihara dan mengelola sistem OLA, selain itu PIC IT *Officer* tersebut juga dapat berlaku sebagai *super admin backup* bila terjadi permasalahan dalam OLA. PIC IT *Officer* juga dapat memberikan izin untuk mengubah status keamanan bila mana diminta dan mendapatkan izin oleh manajemen puncak ataupun orang yang memilik wewenang dalam pengelolaan EDRMS. Pada persyaratan ini merupakan persyaratan penjagaan akses kontrol secara teknikal yang harus dilakukan oleh admin sistem.

Untuk itu bila berbicara mengenai teknikal maka perlu juga melakukan keamanan yang disebut *technical safeguard*, yaitu teknik atau cara untuk mencegah atau membatasi akses ke sistem yang berarti sebuah cara kontrol untuk membatasi akses kepada pihak-pihak yang memiliki wewenang. Perlindungan ini dapat berupa akses berbasis peran kontrol, peran akses berbasis atribut, dan berbasis identitas kontrol akses. Namun, tidak terbatas pada hal tersebut *technical safeguard* tidak terkecuali pada kontrol akses, tetapi juga termasuk kontrol media, otentikasi entitas, enkripsi, *firewall, audit trails*, dan *virus checking* (Kruse et al., 2017).

Selanjutnya, pada persyaratan nomor 105, 106, dan 107 merupakan persyaratan yang membahas tentang keamanan. Di dalam EDRMS, standar meminta untuk sistem menjaga keamanan dari pengguna-pengguna yang mencoba untuk mengakses OLA, tetapi bukan dengan *role* yang orang tersebut miliki. Tiga persyaratan tersebut meminta untuk sistem memberikan respons apabila seseorang tidak memiliki akses dengan batas-batasan sesuai dengan tabel 4. Selain itu pada nomor 106, OLA juga diminta untuk tidak menampilkan apa yang dicari oleh orang yang tidak memiliki akses. Serta yang terakhir persyaratan 107, yaitu memberikan *log history* terkait aktivitas yang dilakukan oleh orang luar yang tidak memiliki akses ketika mencoba mengakses yang bukan *role* atau tidak memiliki akses.

Hal ini tentu menjadi penting karena terdapat beberapa karakteristik yang dikatakan sebagai karakteristik dari arsip itu sendiri. Pertama, dari ISO 15489-1: 2016 tentang *Records Management* dikatakan bawah arsip harus autentik, kegunaan, andal, dan memiliki integritas (The International Standard Organization, 2016). Pada bagian karakteristik Integritas menjadi hal penting bahwa arsip dapat dilindungi dari tindakan perubahan yang tidak sah. Oleh karena itu, permintaan klausa tersebut sejalan terkait dengan karakteristik arsip, yaitu integritas. Perlu adanya kebijakan pengelolaan arsip yang harus dapat mencatat dan memiliki *log history* untuk dapat dilacak (Pratiwi, 2019). Namun, pada aplikasi OLA hanya persyaratan nomor 105 dan nomor 106 yang memenuhi permintaan standar. Untuk persyaratan 107 aplikasi OLA belum dapat memenuhi persyaratan tersebut.

V. KESIMPULAN

Untuk pemenuhan persyaratan ISO 16175-2: 2011 – *Principles and functional requitements for records in electronic office environments* terkait dengan hak akses. Aplikasi OLA telah mematuhi sebanyak 16 persyaratan dari 17 yang diminta oleh standar. Secara pemenuhan standar, OLA belum mematuhi dengan permintaan minimal dari standar karena 17 permintaan tersebut merupakan persyaratan wajib yang harus dipenuhi. Bila berbicara standar ISO terdapat 3 (tiga) *obligation levels, yaitu may, should,* dan *shall.* Untuk 17

persyaratan hak akses merupakan level yang wajib dipenuhi.

Terkait tentang temuan audit pada pemenuhan persyaratan hak akses pada ISO 16175-2: 2011, OLA dapat disimpulkan dari temuan mayor pada proses identifikasi atau audit saat ini. Temuan ini berarti organisasi belum melakukan sesuai dengan apa yang terdapat di standar. Dengan demikian, akan terbentuk Laporan Tindakan Perbaikan dan Pencegahan (LTPP) yang harus dilaksanakan oleh organisasi.

Namun, bila berbicara secara umum OLA sudah cukup baik untuk EDRMS karena hanya 1 (satu) yang belum patuh dengan standar ISO 16175-2: 2011 terkait dengan hak akses. OLA sudah menerapkan klasifikasi akses dan keamanan, pengguna juga sudah dibagi sesuai dengan *role* dan hirarki dalam organisasi dengan *role super admin*, administrator, dan *user*. Maka menjadi poin utama yang perlu dikembangkan, diperbarui, dan dievaluasi dari OLA adalah terkait dengan *log history* keamanan. Pada persyaratan ISO 16175-2: 2011 terkait dengan hak akses diminta untuk memiliki *log history* yang mencatat semua upaya yang tidak sah untuk mengakses OLA bagi pengguna yang tidak memiliki hak akses sesuai dengan *role* yang diberikan.

Ke depannya, PT X diharapkan dapat memperbarui OLA agar dapat memenuhi 17 persyaratan wajib ISO 16175-2: 2011 terkait dengan hak akses. Hal ini sejalan dengan salah satu karakteristik dari arsip, yaitu integritas yang menjadi hal penting bahwa arsip dapat dilindungi dari tindakan perubahan yang tidak sah. Untuk itu diharapkan OLA dapat patuh dengan seluruh persyaratan wajib yang diminta oleh standar.

DAFTAR PUSTAKA

Adam, A. (2007). Implementing Electronic Document and Record Management Systems. In *Implementing Electronic Document and Record Management Systems*. https://doi.org/10.1201/9780849380600

Anugrah, E. P. (2020). Electronic Record Keeping to Support Indonesia E-Government Implementation. *Record and Library Journal*, *6*(1). https://doi.org/10.20473/rlj.v6-i1.2020.31-44

Badan Standardisasi Nasional. (2018). *SNI ISO 15489-1-2016 tentang Informasi dan dokumentasi - Pengelolaan arsip - Bagian 1: Konsep dan prinsip* (p. 31). BSN.

Cruz, J. P., Kaji, Y., dan Yanai, N. (2018). RBAC-SC: *Role*-based access control using smart contract. *IEEE Access*, *6*. https://doi.org/10.1109/ACCESS.2018.2812844

Fachmi, A., dan Mayesti, N. (2021). Kepatuhan Functional Requrements Hak Akses pada Electronic Records Management System Arteri. *JIPI (Jurnal Ilmu Perpustakaan Dan Informasi)*, *6*(1), 61. https://doi.org/10.30829/jipi.v6i1.9264

Holliday, J. (2009). *Professional SharePoint 2007 Records Management Development: Managing Official Records with Microsoft Office SharePoint Server 2007* (1st ed.). Wrox Press.

Joseph, P., Debowski, S., dan Goldschmidt, P. (2012). Paradigm shifts in recordkeeping responsibilities: implications for ISO 15489's implementation. *Records Management Journal*, *22*(1), 57–75. https://doi.org/10.1108/09565691211222108

Kennedy, J., dan Schauder, C. (1998). The records life cycle model and the records Continuum Model. In *Records Management* (pp. 9–12). Addison Wesley Longman Australia.

Peraturan Arsip Nasional Republik Indonesia Nomor 6 Tahun 2021 Tentang Pengelolaan Arsip Elektronik, Arsip Nasional Republik Indonesia 24 (2021).

Kistanto, N. H., Lestari, N., dan Subekti, S. (2014). *Etika Profesi Kearsipan* (Ed.2). Universitas Terbuka.

Kruse, C. S., Smith, B., Vanderlinden, H., dan Nealand, A. (2017). Security Techniques for the Electronic Health Records. *Journal of Medical Systems*, *41*(8), 127. https://doi.org/10.1007/s10916-017-0778-4

Mulyantono, I. (2016). *Otomasi Dalam Kearsipan* (Edisi 2). Universitas Terbuka.

NARA. (2023). *NARA Records Management Key Terms and Acronyms 1 NARA Records Management Key Terms and Acronyms*. Archives.Gov. https://www.archives.gov/files/records-mgmt/rm-glossary-of-terms.pdf

Pratiwi, D. (2019). *Manajemen Rekod Aktif* ((Edisi 2)). Universitas Terbuka.

Rahma, N., dan Mayesti, N. (2019). Pengendalian Hak Akses pada Electronic Document and Records Management System di Kementerian Kelautan dan Perikanan Republik Indonesia. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi Dan Kearsipan*, *5*(1), 33. https://doi.org/10.14710/lenpust.v5i1.23578

Republik Indonesia. (2009). *Undang-Undang Republik Indonesia Nomor 43 Tahun 2009 Tentang Kearsipan*.

Rustam, M. (2019). *Pengelolaan Arsip Elektronik* (Edisi 2). Universitas Terbuka.

Saffady, W. (2009). *Managing Electronic Records* (Fourth Edi). Neal-Schuman Publishers, Inc.

Sari, W. M., dan Rahmah, E. (2013). Kebijakan Akses dan Layanan Arsip di Kantor Perpustakaan, Arsip dan Dokumentasi (KPAD) Kota Bukit Tinggi. *Jurnal Ilmu Informasi Perpustakaan Dan Kearsipan*, *2 No. 1*(September), 237–245.

Sugiarto, A., dan Wahyono, T. (2015). *Manajemen Kearsipan Modern (Dari Konvensional ke Basis Komputer)* (Pertama). Gava Media.

Sutirman, S. (2016). URGENSI MANAJEMEN ARSIP

https://scholarhub.ui.ac.id/jipk/vol25/iss2/5
DOI: 10.7454/JIPK.v25i2.1001

ELEKTRONIK. *EFISIENSI - KAJIAN ILMU ADMINISTRASI*, *13*(1). https://doi.org/10.21831/efisiensi.v13i1.7861

Svärd, P. (2017). Enterprise content management, records management and information culture amidst E-government development. In *Enterprise Content Management, Records Management and Information Culture Amidst E-Government Development*.

The International Standard Organization. (2016). *ISO 15489-1: 2016 Information And Documentation — Records Management*. PART 1: CONCEPTS AND PRINCIPLES.

ISO 16175-2: 2011 – Principles and functional requitements for records in electronic office environments, The International Standards Organisation (2011).

University of Edinburgh. (2023). *Literature review | The University of Edinburgh*. Institute for Academic Development University of Edinburgh. https://www.ed.ac.uk/institute-academic-development/study-hub/learning-resources/literature-review