Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan, 5 (1): 33-48, 2019
 ISSN: 2302-4666 print/ 2540-9638 online
Available Online at: http://ejournal.undip.ac.id/index.php/lpustaka

Pengendalian Hak Akses pada *Electronic Document and Records Management System* di Kementerian Kelautan dan Perikanan Republik Indonesia

Naila Rahma[1*)], Nina Mayesti[2]

[1] *Departemen Ilmu Perpustakaan dan Informasi, Fakultas Ilmu Budaya, Universitas Indonesia*

[*)] Korespondensi: nailarahma@gmail.com

Abstract

This paper discusses the Electronic Document and Records Management System (EDRMS) implemented by Indonesia's Ministry of Marine Affairs and Fisheries (KKP). KKP has implemented an EDRMS since 2012 to support the management of KKP's electronic records. This study focuses on how KKP controls the access towards their electronic records through SIKap, the EDRMS software, as a means to control the security of the system. The aim of this research is to find out whether SIKap follows the EDRMS requirements set by the International Council of Archives (ICA) when applying its policies regarding the security of its electronic records, and if so, how it is implemented. Data were collected through participant observation, based on ICA's EDRMS requirements regarding access and security control, i.e. requirements number 91 to 107. Complementary data were collected through interviews with the archivists. The findings show that SIKap were used to applies KKP policies regarding archival access and security control in the system, which is controlled by the admin. Out of 17 requirements, 13 requirements are fulfilled by SIKap though some are customized to be aligned with KKP's records management needs. The security and access to electronic records are controlled by the admin through applying security levels in both electronic records and system users, to ensure users are only able to access records whose access are granted to them.

Keywords: access control; EDRMS; electronic records; hybrid record management; system security

Abstrak

Artikel ini membahas Electronic Document and Records Management System *(EDRMS) di Kementerian Kelautan dan Perikanan (KKP) Republik Indonesia. KKP telah mengimplementasikan EDRMS bernama Sistem Kearsipan (SIKap) sejak tahun 2012, untuk menunjang pengelolaan rekod elektronik. Fokus pembahasan artikel ini adalah bagaimana KKP mengendalikan akses terhadap rekod elektronik di SIKap, dalam rangka menjaga keamanan sistem. Tujuan penelitian ini adalah untuk mengidentifikasi persyaratan EDRMS dari* International Council of Archives *(ICA) yang dipenuhi oleh SIKap terkait keamanan rekod elektronik dalam sistem, serta bagaimana hal tersebut diimplementasikan. Data didapatkan melalui observasi partisipatif yang dilakukan berdasarkan persyaratan fungsional EDRMS yang ditetapkan ICA terkait dengan pengendalian akses dan keamanan dalam sistem, yaitu persyaratan nomor 91 hingga 107. Data pelengkap didapatkan melalui wawancara yang dilakukan dengan arsiparis. Hasil temuan penelitian menunjukkan bahwa SIKap mengaplikasikan kebijakan terkait dengan pengendalian akses dan keamanan pada rekod elektronik dalam sistem, yang dikontrol oleh admin. Dari 17 persyaratan yang ditetapkan, 13 persyaratan dipenuhi oleh SIKap, meskipun perlu dilakukan penyesuaian terlebih dahulu agar dapat memenuhi kebutuhan pengelolaan rekod di KKP. Akses dan keamanan pada rekod elektronik di SIKap dikendalikan oleh admin dengan cara mengaplikasikan lapisan keamanan ke masing-masing rekod elektronik dan pengguna sistem, untuk memastikan pengguna hanya dapat mengakses rekod yang dibuka aksesnya untuk mereka.*

Kata kunci: pengendalian akses;* EDRMS*; rekod elektronik; pengelolaan rekod hibrid; keamanan dalam sistem

1. Pendahuluan

Pengelolaan arsip merupakan kegiatan penting dalam berjalannya setiap organisasi karena tanpa arsip dikhawatirkan tidak ada bukti eksistensi sebuah organisasi maupun kegiatan-kegiatan yang telah, sedang, ataupun akan dilakukan. Selain itu perkembangan teknologi yang begitu pesat memungkinkan

kegiatan kearsipan dapat dilakukan secara lebih efektif dan efisien karena adanya bantuan teknologi tersebut. Dalam kegiatan kearsipan, peran teknologi tersebut dapat diupayakan semaksimal mungkin hingga seluruh kegiatan menggunakan teknologi. Mulai dari penciptaan, pengelolaan, penggunaan, preservasi, retensi, penyusutan, retensi, dan pemusnahan.

Pada tahun 1999 mulai dikembangkan perangkat lunak yang dikenal dengan sebutan *Electronic Document and Record Management System* (EDRMS) yaitu sistem pengelolaan dokumen dan rekod arsip dinamis elektronik. Sebagai perangkat lunak yang memang dikhususkan untuk membantu kegiatan kearsipan, maka pada dasarnya sebuah EDRMS mengotomasi seluruh kegiatan kearsipan seperti penciptaan, pengelolaan, pemanfaatan, hingga penyusutan atau pemusnahan. Ada berbagai macam manfaat implementasi EDRMS bagi organisasi seperti misalnya untuk kebutuhan manajemen informasi dalam jumlah besar, penyimpanan, indeks, pencarian, dan temu kembali rekod dan arsip elektronik. EDRMS juga membantu organisasi dalam memastikan autentisitas rekod dan arsip digital yang dikelola, hingga untuk membantu mengontrol jadwal retensi dan melakukan penilaian maupun pemusnahan terhadap rekod dan arsip elektronik.

Kementerian Kelautan dan Perikanan (selanjutnya disebut KKP), merupakan salah satu lembaga pemerintah Republik Indonesia yang sudah mengimplementasikan pemanfaatan tekonologi informasi dalam kegiatan pengarsipannya sehari-hari. Implementasi ini dimulai secara perlahan pada tahun 2005. Seiring dengan penggunaannya, perkembangan terus dilakukan terhadap sistem tersebut atas dasar kendala yang ditemukan, perkembangan teknologi informasi, dan juga adanya peraturan baru. Baru kemudian pada tahun 2011, terbit Peraturan Kepala Arsip Nasional Republik Indonesia (ANRI) yang mendorong organisasi dan lembaga pemerintahan untuk mengelola arsip elektronik.

Setelah melewati pengembangan dan pergantian sistem beberapa kali, unit kearsipan I KKP—yang terletak di Subbagian Persuratan dan Kearsipan KKP—menggunakan EDRMS yang dikembangkannya sendiri dengan nama SIKap (Sistem Informasi Kearsipan). SIKap merupakan sistem yang dikhususkan untuk membantu pengelolaan arsip KKP. Arsip yang dimaksud disini juga tidak hanya terbatas pada arsip statis saja, tetapi juga meliputi arsip dinamis. Saat pertama kali digunakan di tahun 2012 SIKap merupakan aplikasi yang harus di*install* di masing-masing perangkat keras, dan datanya tidak terintegrasi. Baru pada tahun 2014 SIKap dikembangkan dan menjadi aplikasi berbasis jaringan sehingga pertukaran data dapat dilakukan secara lebih mudah.

Pengelolaan rekod yang dilakukan secara elektronik dan berbasis jaringan ini tentu saja mempengaruhi banyak aspek dalam pengelolaan rekod elektronik, salah satunya adalah hak akses pada rekod. Isu terkait dengan hak akses disinggung dalam beberapa poin di kode etik yang diterbitkan ICA (1996), yang secara garis besar mengharuskan arsiparis untuk memberikan akses pada rekod kepada pihak yang memiliki hak dan wewenang kepada rekod tersebut, dan turut menghargai privasi yang dimiliki setiap rekod untuk melindungi informasi yang dikandungnya dari pihak yang tidak berwenang. Smallwood (2013) menjelaskan bahwa dalam implementasi EDRMS, hak akses dan keamanan pada rekod elektronik merupakan salah satu aspek penting yang harus diperhatikan. Organisasi pengguna

doi: 10.14710/lenpust.v5i1.23578

EDRMS harus menetapkan kebijakan berkaitan dengan hak akses dan keamanan tersebut untuk kemudian diimplementasikan, dimonitor, dan dievaluasi secara rutin. Hal tersebut dilakukan agar dapat diaplikasikan dalam EDRMS agar rekod elektronik dapat terus menunjang kegiatan organisasi dengan resiko seminimal mungkin, karena terlindungnya informasi yang sifatnya penting dan rahasia bagi kelangsungan kegiatan organisasi.

Hal serupa juga dijelaskan oleh Imine, Lounis, dan Bouabdallah (2018) yang mengatakan bahwa pengendalian akses merupakan kegiatan yang melibatkan banyak mekanisme untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses data tertentu. Penting untuk diingat bahwa topik pengendalian akses tidak hanya meliputi pemberian hak akses dan pengawasan penggunaan hak akses tersebut saja. Diantara yang perlu diatur dalam pengendalian hak akses adalah pencabutan hak akses tersebut dari pengguna sistem yang dianggap sudah tidak lagi berhak untuk mengakses data tertentu.

Dalam pengaturan hak akses rekod non elektronik, arsiparis terlibat secara langsung dalam kegiatan peggunaannya. Hal ini dikarenakan pada umumnya rekod non elektronik disimpan di ruangan khusus, yang hanya dapat diakses oleh arsiparis atau unit kerja pencipta/penanggungjawab rekod tersebut. Apabila ada yang membutuhkan, maka harus melalui arsiparis atau unit kerja yang bertanggungjawab terlebih dahulu. Karena dalam kasus rekod elektronik penyimpanannya berada dalam server sistem tersebut, maka sistem tersebut lah yang harus dapat mengontrol akses pada setiap rekod elektronik agar tidak diakses oleh pengguna yang tidak berwenang.

Berdasarkan latar belakang di atas, masalah dalam artikel ini adalah bagaimana KKP mengendalikan akses pada rekod elektronik yang dikelola dalam SIKap. Tujuan dari penelitian ini adalah untuk mencari tahu apakah SIKap menetapkan kebijakan dalam terkait dengan keamanan rekod elektronik, dan bagaimana kebijakan tersebut diimplementasikan. Dalam artikel ini akan diidentifikasi dan dideskripsikan bagaimana SIKap mengatur hak akses pada rekod elektronik yang dikelolanya.

2. Metode Penelitian

Penelitian ini dilakukan secara kualitatif dengan menggunakan pendekatan studi kasus. Creswell (2014) menjelaskan metode studi kasus dengan mengutip Stake (1995) dan Yin (2009, 2012) yang mendeskripsikan metode studi kasus sebagai metode penelitian dimana peneliti melakukan analisis masalah tertentu secara mendalam. Salah satu karakteristik metode studi kasus yang membedakannya dengan metode penelitian lainnya adalah terikatnya penelitian yang dilakukan dengan waktu dan kegiatan tertentu. Data yang didapatkan peneliti pada suatu kegiatan dari jangka waktu tertentu, sangat mempengaruhi hasil analisis dan pemecahan masalah penelitian nantinya.

Penelitian dilakukan di unit kerja Subbagian Persuratan dan Kearsipan KKP, pada Maret hingga April 2019. Untuk mendapatkan data, dilakukan wawancara semi-terstandarisasi dan observasi partisipatif. Wawancara dilakukan dengan tiga orang informan yaitu Dede Abdurahman dan Ester Triuma Ida selaku arsiparis ahli, dan Andetta Yulnanda selaku Kepala Subbidang Pengembangan Aplikasi Sistem Informasi dari Pusat, Statistik dan Informasi (PUSDATIN) KKP. Sedangkan objek yang diobservasi ialah

SIKap selaku EDRMS yang digunakan KKP untuk mengelola rekod elektronik, dengan mengacu pada persyaratan EDRMS yang diterbitkan ICA mengenai *Principles and Functional Requirements for Records in Electronic Office Environments*.

Principles and Functional Requirements for Records in Electronic Office Environments merupakan panduan hasil proyek ICA dengan lembaga kearsipan beberapa negara lain yang bertujuan untuk menetapkan prinsip dan persyaratan global untuk EDRMS. Prinsip dan persyaratan yang ditetapkan ICA memiliki dasar ISO 15489 yang membahas mengenai manajemen rekod. Tujuan yang ingin dicapai dari adanya proyek dan panduan ini adalah agar dalam mengembangkan EDRMS, lembaga negara maupun swasta dapat mengacu pada panduan yang telah diciptakan agar ada keseragaman dalam sistem. Dengan digunakannya sistem yang seragam, maka lembaga pengguna tidak hanya menjadi lebih efektif dan efisien dalam melakukan kegiatan kearsipannya, tetapi juga lebih fleksibel terhadap perkembangan teknologi dan EDRMS.

Panduan tersebut terbagi dalam tiga modul. Modul pertama membahas prinsip-prinsip dasar dalam pengelolaan rekod elektronik, untuk memberikan konteks bagi pengguna panduan. Modul kedua fokus pada persyaratan yang diberikan untuk EDRMS. Terdapat 275 persyaratan yang dibagi kedalam empat kategori persyaratan berdasarkan kegiatan yang dilakukan. Empat kategori persyaratan tersebut adalah *create*, *maintain*, *disseminate*, dan *administer*. Terakhir adalah modul ketiga, yang dikhususkan bagi organisasi yang ingin mengintegrasikan kegiatan pengelolaan rekod elektroniknya kedalam perangkat lunak yang digunakan untuk mencatat transaksi bisnis dalam organisasi.

Penelitian artikel ini akan banyak bergantung pada modul kedua, sebagai panduan dasar peneliti dalam melakukan observasi. Agar penelitian terfokus, maka peneliti memutuskan untuk fokus pada persyaratan dari kategori *maintain*. Dalam setiap kategori, ICA masih membagi persyaratan yang ada kedalam beberapa kelompok. Peneliti telah memilah persyaratan yang ada dalam kategori *maintain*, dan menemukan bahwa ada tiga kelompok yang membahas mengenai hak akses pada rekod elektronik dalam sistem.

Kelompok pertama ialah kelompok pengendalian akses, yang terdiri dari satu persyaratan yaitu persyaratan nomor 91. Berikutnya adalah persyaratan kelompok penerapan pengendalian keamanan, yang terdiri dari empat persyaratan yaitu persyaratan nomor 92 hingga 95. Ketiga adalah persyaratan dalam kelompok penerapan tingkat keamanan, yang terdiri dari enam persyaratan yaitu persyaratan nomor 96 hingga 101. Kelompok persyaratan terakhir adalah kelompok eksekusi pengendalian keamanan. Kelompok ini terdiri dari enam persyaratan, yaitu persyaratan nomor 102 hingga 107. Secara keseluruhan, penelitian ini akan membahas temuan di EDRMS KKP berdasarkan 11 persyaratan tersebut.

3. Hasil dan Pembahasan

Seluruh kegiatan kearsipan Kementerian Kelautan dan Perikanan, dipusatkan di Subbagian Persuratan dan Kearsipan. Hal ini disebabkan Subbagian Persuratan dan Kearsipan sebagai unit kearsipan I memiliki tanggung jawab untuk memonitor seluruh kegiatan kearsipan yang berlangsung di KKP. Untuk

doi: 10.14710/lenpust.v5i1.23578

menunjang tanggung jawab tersebut, maka Subbagian Persuratan dan Kearsipan memiliki wewenang untuk membuat kebijakan dan aturan terkait dengan kegiatan kearsipan yang berlangsung di KKP. Sebagai lembaga pemerintah, kebijakan tersebut disusun atas dasar peraturan yang telah ditetapkan oleh ANRI, dan juga bekerja sama dengan pejabat eselon I dan II kearsipan untuk memastikan bahwa kebijakan yang ditetapkan akan sesuai dengan hukum undang-undang yang ada dan juga sesuai dengan kebutuhan dan kegiatan yang ada di KKP.

Kebijakan yang diberlakukan antara rekod dengan arsip tentu saja berbeda. Untuk rekod karena merupakan arsip dinamis dan penggunaannya oleh unit kerja yang terkait cukup tinggi, maka disimpan di unit kerja tersebut masing-masing. Di unit kerja, rekod-rekod tersebut disimpan dan dikelola oleh arsiparis unit kearsipan II atau UPT yang mengatasi unit kerja tersebut. Saat frekuensi penggunaan masih tinggi, penyimpanan dan pengelolaan dilakukan di masing-masing unit kerja untuk mempermudah akses apabila dibutuhkan. Adanya kebijakan ini juga memperjelas siapa penanggungjawab dari masing-masing rekod. Indentifikasi ini penting untuk menjaga keamanan informasi yang terkandung di dalamnya dan memastikan bahwa informasi tersebut tidak akan jatuh ke pihak yang tidak berwenang.

Saat frekuensi penggunaan rekod sudah turun, baru kemudian akan diserahkan ke Subbagian Persuratan dan Kearsipan. Selain rekod yang tingkat penggunaannya menurun, rekod yang telah habis retensinya namun diberikan status permanen karena nilai guna yang dikandungnya, juga diserahkan kepada Subbagian Persuratan dan Kearsipan untuk dikelola sebagai arsip statis. Sebagai unit kearsipan I, Subbagian Persuratan dan Kearsipan difasilitasi ruang arsip sebagai tempat penyimpanan seluruh rekod dan arsip yang diserahkan oleh unit kerja II dan/atau UPT yang hanya boleh diakses oleh arsiparis Subbagian Persuratan dan Kearsipan. Saat rekod dan arsip diserahkan untuk disimpan di ruang arsip, maka tanggung jawab dari rekod dan arsip tersebut juga diserahkan pada arsiparis Subbagian Persuratan dan Kearsipan. Tanpa terkecuali, pengendalian hak akses dari masing-masing rekod dan arsip tersebut juga menjadi tanggung jawab arsiparis Subbagian Persuratan dan Kearsipan.

Kebijakan yang ditetapkan Subbagian Persuratan dan Kearsipan ialah untuk mengakses rekod dan/atau arsip dibutuhkan bukti otorisasi dari pejabat unit kerja yang meminta akses pada rekod tersebut. Apabila sebuah unit kerja membutuhkan rekod yang diciptakan/menjadi tanggung jawab unit kerja lain, maka dibutuhkan juga otorisasi dari pejabat unit kerja yang menciptakan/bertanggung jawab atas rekod yang diminta.

Pada tahun 2012, KKP mulai mengimplementasikan adanya EDRMS untuk memulai transisi ke pengelolaan rekod secara elektronik. Sistem pertama yang digunakan ialah SIKap, yang diimplementasikan dengan harapan dapat meningkatkan efektifitas dan juga kualitas hasil pekerjaan. Seiring dengan berjalannya waktu, perkembangan teknologi, dan respon yang didapat dari penggunaan SIKap, maka untuk kegiatan persuratan dan kearsipan KKP menciptakan dua sistem baru lagi yaitu SIMPeL di tahun 2013, dan SIDoeL di tahun 2016. Meskipun waktu menciptakan ketiga sistem tersebut berbeda, namun kronologis penciptaan tidak merepresentasikan alur proses pengelolaan surat dan rekod. Hal ini disebabkan intensi awal sistem-sistem tersebut diciptakan adalah untuk mengotomasi kegiatan

tertentu, bukan untuk mengotomasi kegiatan secara keseluruhan dalam tahapan yang kronologis. Alur pemanfaatan sistem berdasarkan proses kegiatan persuratan dan kearsipan dimulai dari SIMPeL, SIDoeL, dan diakhiri dengan SIKap.

Pertama adalah SIMPeL, yang dikembangkan sejak tahun 2013. SIMPeL merupakan singkatan dari Sistem Informasi dan Manajemen Persuratan Elektronik. Sesuai dengan namanya, SIMPeL ini memiliki fungsi yang cukup spesifik yaitu untuk mengelola persuratan KKP. SIMPeL tidak hanya digunakan untuk surat masuk maupun surat keluar saja, tetapi merupakan alat bantu untuk mencatat seluruh persuratan yang masuk dan keluar dari KKP. Setelah surat dikelola, maka akan didisposisikan dan pengelolaannya berlanjut ke Sistem Informasi Disposisi Elektronik, yang biasa dikenal dengan nama SIDoeL.

Diciptakan pada tahun 2016, SIDoeL merupakan sistem yang diciptakan untuk menjembatani proses dan kegiatan yang dilakukan di SIMPeL dengan SIKap. Kegiatan yang dilakukan dalam SIDoeL adalah distribusi surat dari petugas persuratan ke unit kerja, untuk membantu pelacakan tindak lanjut dari masing-masing surat. Setelah proses di SIDoeL selesai, maka rekod disimpan di Sistem Informasi Kearsipan, yang biasa disebut sebagai SIKap.

SIKap sendiri telah diciptakan dan digunakan sejak tahun 2012, namun setelah dilakukan pengembangan di tahun 2014 baru SIKap menjadi sebuah sistem yang berbasis jaringan internet. Sebagai sistem yang memfasilitasi pengelolaan arsip dinamis dan statis, maka SIKap memiliki fitur-fitur tambahan untuk melengkapi kegiatan kearsipan seperti misalnya pencatatan metadata arsip, kontrol masa retensi, melayani temu kembali dan penggunaan arsip, hingga membantu arsiparis dalam melakukan penyusutan dan pemusnahan arsip. Fitur-fitur tersebut tidak tersedia dalam SIMPeL dan SIDoeL karena seperti yang telah dibahas sebelumnya, penggunaan SIMPeL lebih dikhususkan pada fungsi penangkapan dan penciptaan arsip berbentuk surat, sedangkan SIDoeL lebih dikhususkan pada fungsi disposisi.

Bersamaan dengan diimplementasikannya EDRMS tersebut sejak tahun 2012, maka tentu saja banyak kebijakan berkaitan dengan kegiatan persuratan dan kearsipan yang diubah untuk disesuaikan dengan keadaan Subbagian Persuratan dan Kearsipan yang kegiatannya sudah lebih banyak terotomasi memanfaatkan teknologi. Meskipun kebijakan dasar dari kegiatan persuratan dan kearsipan itu sendiri tidak diubah secara drastis, namun yang berubah ialah cara kebijakan tersebut diimplementasikan.

Salah satu diantara aspek dari kebijakan yang implementasinya berubah, ialah kebijakan berkaitan dengan hak akses pada rekod elektronik. Terjadinya perubahan implementasi kebijakan mengenai hak akses pada rekod elektronik ini dipengaruhi oleh tidak adanya ruangan yang bisa dikontrol dan diawasi oleh arsiparis secara langsung. Berhubung kegiatan kearsipan tidak lagi dilakukan secara manual, maka tidak mungkin bagi arsiparis untuk menjaga rekod elektronik tersebut secara manual karena tidak wujud fisik dari rekod-rekod tersebut. Oleh karena itu, pengendalian hak akses rekod elektronik harus dilakukan secara digital juga, mengandalkan sistem yang digunakan.

Dalam persyaratan yang diterbitkan ICA (2008), terdapat 17 persyaratan berkaitan dengan hak akses pada rekod elektronik untuk dipenuhi EDRMS yang dibagi kedalam empat kelompok persyaratan. Empat kelompok tersebut terdiri dari pengendalian akses, penetapan pengendalian keamanan, penerapan

doi: 10.14710/lenpust.v5i1.23578

tingkat keamanan, dan penerapan tingkat keamanan. Penyajian data observasi dan hasil analisis akan dikelompokkan berdasarkan tiga kelompok tersebut.

Pengendalian Akses

Kelompok persyaratan pertama adalah pengendalian akses, yang terdiri dari satu persyaratan yaitu persyaratan nomor 91. Yang dimaksud dengan pengendalian akses dalam kelompok persyaratan ini adalah adanya penerapan *Role Based Access Control* (RBAC) untuk memberikan batasan pada fungsi-fungsi tertentu bagi setiap pengguna sistem. RBAC sendiri merupakan mekanisme otorisasi dalam sistem perangkat lunak yang memberikan relasi antara peran pengguna, dengan hak akses kepada objek yang ada dalam sistem. Berikut ini adalah persyaratan nomor 91:

Tabel 1 Persyaratan kelompok pengendalian akses

Nomor	Persyaratan	(V/X)
91	Membatasi akses fungsi sistem bergantung pada peran pengguna dan kontrol admin sistem.	V

Dari persyaratan tersebut, dapat dilihat bahwa dalam EDRMS pengguna diberikan peran berbeda-beda. Dalam SIKap persyaratan ini dipenuhi dengan adanya beberapa peran pengguna yaitu super admin, admin, arsiparis, dan pegawai fungsional umum. Peran-peran ini diadakan untuk membantu melakukan kontrol terhadap akses pada fitur sistem maupun pada dokumen dan rekod elektronik.

Peran yang memiliki hak akses tertinggi adalah super admin yang terdiri dari satu orang pegawai Pusdatin dan satu orang arsiparis ahli dari Subbagian Persuratan dan Kearsipan, dan kemudian diikuti oleh peran admin yang terdiri dari pejabat eselon II, III, dan IV kearsipan dari masing-masing unit kerja. Penetapan peran admin ini juga sesuai dengan pernyataan Ellis (2008) yang mengatakan bahwa pengguna yang dalam sistem diberikan kewenangan untuk mengubah hak akses pengguna lainnya baiknya merupakan pemimpin unit kerja.

Perbedaan antara peran admin dengan super admin adalah peran admin dapat mengatur akses pengguna yang secara struktural memiliki jabatan dibawah masing-masing admin tersebut saja, sedangkan peran super admin dapat mengatur akses seluruh pengguna, termasuk akses para admin. Pada praktiknya, pembedaan antara peran super admin dengan admin diadakan agar akses pengguna non admin dapat diatur langsung oleh admin yang secara struktural bertanggungjawab atas pengguna non admin dari masing-masing unit kerja, sementara peran super admin mengatur akses dari masing-masing admin.

Tidak hanya peran admin dan super admin yang diberikan hak akses fungsi berbeda dari pengguna sistem lainnya, antara peran arsiparis dan pegawai fungsional juga diberikan batasan yang berbeda. Arsiparis diberikan akses pada fungsi input rekod ke dalam SIKap, sedangkan pegawai fungsional hanya dapat mengakses rekod elektronik yang dimana mereka diberikan akses saja. Pembatasan peran pegawai fungsional untuk menginput rekod meliputi kemampuan mereka untuk menginput rekod yang berkaitan dengan unit kerja asal mereka. Kebijakan ini ditetapkan agar penginputan dilakukan secara terfokus oleh arsiparis saja, untuk mempermudah pertanggungjawaban.

Dipenuhinya persyaratan nomor 91 ini juga sesuai dengan penjelasan Bantin (2008) dalam bukunya *Understanding Data and Information Systems for Recordkeeping* yang mengatakan bahwa cara paling mudah untuk membatasi hak akses adalah dengan mengaplikasikan tingkatan keamanan kepada rekod elektronik berdasarkan pengguna sistem. Meskipun dalam SIKap pembatasan yang diterapkan didasarkan atas unit kerja, namun hasil yang dicapai dari pembatasan tersebut sama dengan pencapaian apabila pembatasan yang dilakukan sesuai dengan tingkatan yang dimaksud Bantin (2008).

Penerapan Pengendalian Keamanan

Berikutnya adalah kelompok persyaratan penetapan pengendalian keamanan. Kelompok ini memiliki empat persyaratan yaitu persyaratan nomor 92 hingga 95. Berikut ini adalah persyaratan yang terkandung dalam kelompok penerapan pengendalian keamanan:

Tabel 2 Persyaratan kelompok penerapan pengendalian keamanan

Nomor	Persyaratan	(V/X)
92	Hanya izinkan admin sistem untuk membuat profil pengguna dan mengalokasikan pengguna ke grup.	V
93	Hanya izinkan admin sistem untuk memberikan batasan akses pada rekod, agregasi, dan metadata kepada pengguna atau grup pengguna tertentu.	V
94	Hanya izinkan admin sistem untuk mengubah kategori keamanan rekod.	V
95	Hanya izinkan admin sistem untuk melakukan perubahan atribut keamanan pada pengguna atau grup pengguna tertentu (seperti hak akses dan tingkat keamanan).	V

Empat persyaratan yang ada dalam kelompok persyaratan penerapan pengendalian keamanan dipenuhi seluruhnya oleh SIKap. Persyaratan nomor 92 mengharuskan EDRMS untuk memberikan kewenangan bagi admin untuk membuatkan dan menghapus profil pengguna dalam sistem. Baru pada persyaratan nomor 93, pembahasan mulai membahas mengenai pengendalian akses pada rekod elektronik. Pada persyaratan nomor 93 admin EDRMS diharuskan memiliki kemampuan untuk memberikan batasan akses menuju rekod elektronik tertentu kepada pengguna yang memiliki peran dan asal unit kerja berbeda.

Pengendalian akses pada rekod tidak hanya dibatasi oleh peran yang dimiliki pengguna saja, tetapi juga oleh asal unit kerja pengguna. Untuk menjaga keamanan dari informasi yang terkandung agar tidak disalahgunakan oleh pihak yang tidak berwenang, maka seorang pengguna hanya diberikan akses kepada rekod elektronik yang diciptakan dan/atau diperuntukkan unit kerja asalnya saja. Karena setiap rekod elektronik diasosiasikan kepada setidaknya satu agregasi, maka pengendalian akses kepada rekod dilakukan langsung kepada setiap agregasi agar dapat dilakukan secara mudah. Meskipun begitu, tidak menutup kemungkinan bagi admin untuk mengubah batasan akses bagi rekod-rekod tertentu secara individu, sesuai dengan apa yang disebutkan dalam persyaratan nomor 94. Pentingnya persyaratan ini untuk dipenuhi adalah untuk menghadapi kemungkinan adanya rekod tertentu yang dibutuhkan oleh unit kerja lain selain unit kerja pencipta.

doi: 10.14710/lenpust.v5i1.23578

Untuk memberikan contoh bagi implementasi persyaratan nomor 94, maka akan digunakan unit kerja hubungan masyarakat dengan unit kerja keuangan. Pada dasarnya, pengguna SIKap yang berasal dari unit kerja hubungan masyarakat hanya diberikan akses kepada rekod elektronik yang diciptakan oleh unit kerja hubungan masyarakat saja. Hal tersebut tidak menutup kemungkinan bahwa unit kerja hubungan masyarakat dapat membutuhkan rekod milik unit kerja keuangan pada suatu saat, karena adanya informasi yang terkandung dalam rekod tersebut yang dibutuhkan unit kerja hubungan masyarakat. Saat ada kebutuhan seperti itu lah unit kerja hubungan masyarakat dapat mengajukan kepada super admin untuk diberikan akses kepada rekod yang dibutuhkan tersebut, dengan adanya persetujuan dari unit kerja keuangan. Pengubahan batasan akses pada rekod elektronik secara individu, hanya akan mengubah hak akses pada rekod elektronik itu saja tanpa akan mempengaruhi batasan akses bagi agregasi dimana rekod itu berada.

Implementasi persyaratan nomor 92 hingga 94 ini sesuai dengan kapabilitas kunci yang ditetapkan HP Software Big Data (2015) terkait dengan skema keamanan dan akses. Disebutkan bahwa EDRMS yang baik harus mengimplementasikan sebuah skema keamanan dan akses, agar seluruh pihak yang rekod elektroniknya dikelola dalam EDRMS tersebut merasa data informasinya aman dan terlindungi. Hal tersebut diimplementasikan melalui adanya hak akses yang ditetapkan pada setiap pengguna dalam sistem, dimana pengguna dengan peran tinggi yang dapat menentukan sejauh mana hak akses yang dimiliki oleh setiap pengguna ke setiap rekod elektronik yang ada dalam sistem. Seperti yang telah dijelaskan sebelumnya, hal tersebut dipenuhi dalam SIKap dengan adanya super admin dan admin yang mengatur hak akses setiap pengguna SIKap.

Dalam SIKap, seluruh perubahan yang dibuat terkait dengan hak akses pengguna kepada fitur sistem maupun akses kepada rekod hanya dapat dilakukan oleh admin sistem. Hal ini seusai dengan persyaratan nomor 95, yang mengharuskan EDRMS untuk hanya memberikan kewenangan tersebut kepada admin. Karena kebetulan ada dua peran admin yang diimplementasikan di SIKap, maka peran admin kewenangannya sebatas untuk mengatur hak akses pengguna non admin kepada fitur yang disediakan, sementara super admin dapat mengatur hak akses pengguna admin maupun non admin, kepada fitur dalam sistem dan juga kepada rekod elektronik.

Penerapan Tingkat Keamanan

Selain penerapan RBAC di persyaratan nomor 91, kelompok persyaratan penerapan tingkat keamanan juga masih terkait dengan adanya RBAC di EDRMS. Selain itu, ICA juga meminta EDRMS untuk menerapkan *Attribute Based Access Control* (ABAC) terutapa pada persyaratan nomor 96. Berikut ini adalah persyaratan nomor 96 hingga 97:

Tabel 3 Persyaratan kelompok penerapan tingkat keamanan (1)

Nomor	Persyaratan	(V/X)
96	Hanya izinkan admin sistem untuk memberikan atribut pada pengguna untuk mengatur keamanan dalam sistem. Atribut yang dimaksud mencakup: • melarang akses ke EDRMS tanpa adanya otentikasi dari sistem;	V

	• membatasi akses pengguna ke rekod atau agregasi tertentu; • membatasi akses pengguna pada fitur tertentu (misalnya membaca, memperbaharui, dan/atau menghapus rekod atau metadata tertentu); • membatasi akses pengguna ke rekod dalam jangka waktu tertentu; • mengalokasikan pengguna ke satu grup atau lebih;	
97	Mampu mengendalikan akses pada fungsi-fungsi tertentu dalam sistem ke peran tertentu, seperti pengendalian akses yang dilakukan pada pengguna.	V

Dibuka dengan persyaratan nomor 96, yang mengharuskan EDRMS untuk memberikan atribut kepada profil para pengguna sistem untuk membantu pemberian batasan akses kepada fitur dan rekod. Persyaratan ini dipenuhi dalam SIKap, meskipun tidak seutuhnya. Pada dasarnya, pembatasan akses dalam rangka menjaga keamanan di EDRMS KKP dilakukan dengan adanya peran seperti yang telah dibahas sebelumnya. Pemberian atribut yang dibahas di persyaratan nomor 96 diimplementasikan dengan adanya keterangan mengenai asal unit kerja pengguna untuk memberikan batasan akses kepada rekod. Selain kedua hal tersebut, maka tidak ada atribut tambahan yang diberikan pada pengguna karena pemberian batasan akses hanya didasarkan atas peran dan unit kerja asal pengguna seperti yang telah disebutkan sebelumnya.

Dalam persyaratan nomor 96 juga disebutkan bahwa admin EDRMS diharuskan memiliki kemampuan untuk memberikan jangka waktu akses untuk rekod-rekod tertentu. Hal ini dapat dicapai dalam SIKap, namun tidak dengan cara yang dimaksud dalam persyaratan nomor 96. Untuk memenuhi persyaratan tersebut, maka semestinya admin memiliki opsi untuk memberikan akses dalam jangka waktu tertentu agar nantinya EDRMS itu sendiri yang akan menutup akses pengguna yang diberikan akses tersebut, sesuai dengan apa yang diperintahkan oleh admin sebelumnya. SIKap sendiri tidak memiliki fitur yang dapat memungkinkan hal tersebut, sehingga apabila sebuah rekod akan dibuka aksesnya untuk pengguna tertentu dalam jangka waktu yang telah ditentukan, admin itu sendiri yang bertanggungjawab untuk menutup kembali akses pengguna tersebut.

Persyaratan nomor 96 berkaitan dengan persyaratan nomor 97 yang mengharuskan EDRMS untuk dapat memberikan batasan fungsi dalam sistem kepada pengguna dengan peran tertentu, dengan cara yang sama batasan hak akses pada rekod elektronik diberikan. Persyaratan nomor 97 ini dipenuhi oleh SIKap. Seperti halnya pembatasan hak akses diberikan dengan dasar asal unit kerja pengguna, dalam SIKap juga dibatasi fungsi-fungsi tertentu berdasarkan peran yang dimiliki pengguna. Contohnya antara peran admin, dengan peran arsiparis. Meskipun keduanya dapat menginput rekod ke SIKap, namun hanya peran admin yang dapat mengakses fungsi sistem untuk menambahkan pengguna baru ke dalam sistem. Bisa juga dicontohkan antara peran arsiparis dengan peran pegawai fungsional, yang meskipun keduanya dapat mengakses rekod elektronik namun hanya peran arsiparis yang dapat menambahkan rekod baru ke dalam sistem.

Dari persyaratan nomor 92 hingga 97 dapat dilihat bagaimana RBAC dan ABAC diimplementasikan sebagai mekanisme otorisasi dalam SIKap. Dalam persyaratan nomor 92 hingga 94

doi: 10.14710/lenpust.v5i1.23578

dan 97, RBAC diberlakukan untuk memberikan batasan hak akses dan juga fungsi dalam sistem kepada masing-masing peran pengguna. Sementara dalam persyaratan nomor 95 dan 96, ABAC diberlakukan untuk memberikan atribut pada setiap pengguna dalam rangka meningkatkan keamanan hak akses dalam SIKap. Apa yang ditemukan di SIKap ini serupa dengan saran Lo, Yang, dan Guo (2015) dalam artikelnya *An Attribute-Role Based Access Control Mechanism for Multi-tenancy Cloud Environment*, yang menjelaskan bahwa dengan diaplikasikannya RBAC dan juga ABAC, maka pengendalian hak akses dalam sistem dapat menjadi lebih aman dan dilakukan secara lebih efisien.

Empat persyaratan berikutnya dalam kelompok persyaratan penerapan tingkat keamanan membahas mengenai penciptaan grup pengguna untuk membantu memberikan batasan hak akses, dan juga pemberian izin bagi pengguna kepada rekod dalam agregasi tertentu dan untuk menentukan hak akses rekod elektronik kepada pengguna lainnya. Berikut ini adalah persyaratan nomor 98 hingga 101:

Tabel 4 Persyaratan kelompok penerapan tingkat keamanan (2)

Nomor	Persyaratan	(V/X)
98	Mampu menciptakan grup pengguna yang diasosiasikan dengan agregasi tertentu.	X
99	Mengizinkan pengguna untuk menjadi anggota dalam lebih dari satu grup.	X
100	Mampu membatas akses pengguna pada rekod tertentu yang berada dalam sebuah agregasi.	V
101	Mengizinkan pengguna untuk menentukan siapa saja yang memiliki akses pada rekod tertentu yang dimana pengguna tersebut merupakan penanggungjawabnya.	X

Masih mengenai keamanan dalam sistem, persyaratan nomor 98 dan 99 membahas mengenai pembuatan grup diantara pengguna dalam rangka menciptakan tingkatan keamanan baru. Dalam modul yang diterbitkan ICA (2008), diberikan keterangan pada persyaratan nomor 98 bahwa grup yang dimaksud dalam persyaratan dapat berupa grup ‘HRD’ atau ‘Sales’, yang merepresentasikan unit kerja asal pengguna. Namun berhubung dalam SIKap unit kerja asal pengguna dijadikan atribut pada setiap pengguna, maka kebutuhan untuk membuat grup pun tidak ada. Oleh karena itu, kedua persyaratan ini tidak dipenuhi oleh EDRMS KKP.

Persyaratan nomor 100 merupakan pengembangan dari beberapa persyaratan yang telah dibahas sebelumnya terkait dengan akses pengguna pada rekod elektronik. Persyaratan nomor 100, memastikan kembali bahwa EDRMS harus membatasi akses pengguna kepada rekod yang hak aksesnya tidak dimiliki, meskipun pengguna tersebut diberikan hak untuk mengakses rekod lain dalam agregasi yang sama. Persyaratan ini dipenuhi oleh EDRMS KKP, tepatnya oleh SIKap. Apabila pengguna melakukan penelusuran dalam agregasi, maka rekod elektronik yang haknya tidak dimiliki oleh pengguna tersebut tidak akan muncul dalam daftar maupun dalam hasil pencarian, seakan-akan rekod elektronik tersebut tidak ada dalam sistem. Kebijakan seperti ini diterapkan dalam SIKap untuk memastikan kemananan setiap rekod elektronik agar dapat dijaga semaksimal mungkin.

Kemudian dalam persyaratan nomor 101 admin EDRMS diharuskan untuk bisa memberikan hak lebih pada pengguna tertentu, agar pengguna tersebut bisa mengubah hak akses kepada rekod yang dimana pengguna tersebut merupakan penanggungjawabnya. Hal ini tidak dipenuhi oleh EDRMS KKP, karena peran yang memiliki wewenang untuk mengatur hak akses tiap pengguna hanyalah admin dan super admin. Apabila pengguna selain admin dan super admin diberikan kemampuan untuk mengubah hak akses pada rekod atau pengguna tertentu, maka akan bertentangan dengan anjuran HP Software Big Data (2015) yang telah dibahas sebelumnya, mengenai hanya peran tertinggi yang sebaiknya mengatur hak akses pengguna lainnya dalam sistem.

Eksekusi Pengendalian Keamanan

Kelompok persyaratan terakhir adalah kelompok eksekusi pengendalian keamanan. Terdiri dari enam persyaratan, kelompok persyaratan ini merupakan lanjutan dari kelompok persyaratan penetapan pengendalian keamanan. Pembahasan kelompok persyaratan ini akan dibagi menjadi dua, agar dapat dilakukan analisis secara lebih mendalam. Berikut ini adalah persyaratan nomor 102 hingga 104:

Tabel 5 Persyaratan kelompok eksekusi pengendalian keamanan (1)

Nomor	Persyaratan	(V/X)
102	Hanya izinkan admin sistem untuk mengubah status keamanan seluruh rekod dalam suatu agregasi sekaligus. EDRMS diharuskan untuk memberikan peringatan apabila status keamanan rekod akan diubah, dan menunggu konfirmasi sebelum mengaplikasikan perubahan tersebut.	V
103	Hanya izinkan admin untuk mengubah status keamanan suatu agregasi.	V
104	Mendokumentasikan seluruh perubahan terkait dengan status keamanan dalam metadata rekod atau agregasi yang diubah status keamanannya.	V

Tiga persyaratan pertama yaitu persyaratan nomor 102, 103, dan 104 membahas mengenai kemungkinan admin untuk mengubah batasan keamanan bagi agregasi rekod tertentu dan dokumentasi yang dilakukan terkait dengan perubahan tersebut. Dokumentasi dari setiap perubahan yang dilakukan merupakan bagian penting dari perubahan status keamanan, maupun perubahan aspek lain dari sistem maupun metadata rekod elektronik. Seperti yang dijelaskan Bantin (2008), admin sistem harus terus memantau bahwa kegiatan yang dilakukan di sistem selalu terdokumentasi, dan hal ini tentu saja meliputi perubahan status keamanan terhadap data dalam sistem.

Ketiga persyaratan ini dipenuhi oleh SIKap. Peran super admin memiliki kewenangan untuk mengubah batasan akses agregasi rekod yang ada. Peran admin tidak memiliki kewenangan ini, sehingga harus meminta super admin untuk melakukan perubahan tersebut dilengkapi dengan persetujuan dari unit kerja yang terkait dengan agregasi rekod tersebut. Karena perubahan yang dilakukan berkaitan dengan teknis sistem, maka akan tercatat secara otomatis dalam log yang bersifat rahasia. Dari seluruh peran pengguna, hanya super admin yang dapat mengakses log tersebut. Apabila dibutuhkan untuk keperluan hukum atau pertanggungjawaban, maka super admin diharuskan untuk memberikan log SIKap kepada

doi: 10.14710/lenpust.v5i1.23578

pihak yang berwenang. Hal ini juga sesuai dengan pemaparan Bantin (2008) yang mengatakan bahwa dokumentasi dalam sistem selain harus akurat, juga harus selalu siap untuk diakses dan digunakan oleh pihak-pihak yang berwenang apabila dibutuhkan.

Dalam persyaratan nomor 105 hingga 107, ICA mengatur respon sistem apabila seorang pengguna mencoba untuk mengakses agregasi atau rekod yang tidak menjadi bagian dari hak akses pengguna tersebut. Berikut ini tiga persyaratan terakhir dalam kelompok eksekusi pengendalian keamanan:

Tabel 6 Persyaratan kelompok eksekusi pengendalian keamanan (2)

Nomor	**Persyaratan**	**(V/X)**
105	Memberikan salah satu dari respon berikut, apabila pengguna meminta akses atau melakukan pencarian rekod atau agregasi yang diluar batasan akses mereka: • menampilkan judul rekod atau agregasi beserta metadatanya; • menampilkan keberadaan rekod atau agregasi tersebut, tetapi tidak judul dan/atau metadata dari rekod atau agregasi; atau • tidak menampilkan informasi terkait dengan rekod atau agregasi tersebut, termasuk tidak mengindikasikan eksistensinya dalam sistem.	V
106	Tidak menampilkan rekod yang aksesnya tidak dimiliki pengguna, dalam daftar rekod maupun hasil penelusuran.	V
107	Mendokumentasikan seluruh upaya pengguna dalam mengakses rekod atau agregasi yang hak aksesnya tidak mereka miliki.	X

Persyaratan nomor 105 memberikan beberapa opsi bagi sistem untuk merespon pengguna yang mencoba untuk mengakses agregasi atau rekod yang tidak menjadi bagian dari hak akses pengguna tersebut, dan yang diimplementasikan oleh SIKap adalah opsi untuk tidak menampilkan rekod yang bukan merupakan akses pengguna tersebut dalam daftar maupun hasil pencarian. Ini berkaitan dengan persyaratan nomor 106 yang megharuskan EDRMS untuk tidak menampilkan rekod ataupun agregasi kepada pengguna yang tidak memiliki akses pada rekod dan/atau agregasi tersebut. SIKap mengimplementasikan kedua aturan ini untuk menjaga informasi yang terkandung dalam masing-masing rekod, agar tidak dapat digunakan oleh pihak-pihak yang tidak berwenang.

Dieliminasinya seluruh kemungkinan pengguna untuk mengetahui eksistensi rekod-rekod yang dimana mereka tidak diberikan hak akses dalam SIKap merupakan salah satu bentuk manajemen resiko yang dilakukan oleh KKP untuk melinndungi rekod elektronik yang dikelolanya. Hal ini dijelaskan oleh Safady (2012) dalam bukunya *Managing Electronic Records* yang menjelaskan bahwa akses yang dilakukan oleh pihak yang tidak berwenang merupakan salah satu ancaman dalam implementasi EDRMS. Apabila pihak yang tidak berwenang dapat mengakses rekod-rekod elektronik tertentu, maka informasi yang dikandungnya menjadi rawan terhadap penyalahgunaan. Oleh karena itu kebijakan KKP dalam tidak menampilkan rekod kepada pengguna merupakan tindakan yang tepat bagi rekod elektronik dan pihak-pihak terkait dengan rekod elektronik yang dilindungi.

Dipenuhinya persyaratan nomor 105 dan 106 berdampak pada persyaratan nomor 107, yang menjadi tidak relevan dalam konteks EDRMS KKP meskipun termasuk diantara persyaratan EDRMS yang wajib untuk diimplementasikan. Persyaratan tersebut mengharuskan EDRMS untuk mencatat usaha pengguna untuk mengakses rekod dan/atau agregasi yang dimana mereka tidak memiliki hak akses. Namun karena pengguna hanya dapat melihat rekod dan/atau agregasi yang mereka memiliki hak akses, maka kemungkinan untuk mengakses rekod diluar hak akses mereka menjadi tidak mungkin. Karena hal tersebut, maka persyaratan nomor 107 ini tidak diimplementasikan dalam SIKap.

4. Simpulan

Untuk fungsi pengendalian hak akses dalam sistem, SIKap memenuhi 13 dari 17 persyaratan yang ditetapkan ICA. Pengendalian hak akses pada rekod elektronik di SIKap dilakukan dengan cara memberikan batasan pada masing-masing rekod elektronik dan juga pada pengguna SIKap. Hak akses dalam sistem diatur oleh pengguna yang memiliki peran admin dan super admin dalam sistem, dengan cara memberikan batasan pada setiap rekod elektronik dan pengguna. Saat pengguna didaftarkan, diberikan atribut yang menunjukkan unit kerja asal pengguna tersebut dan juga perannya. Kedua atribut itu lah yang memberikan batasan bagi penggua untuk mengakses rekod elektronik.

Saat melakukan penelusuran dan temu kembali dalam SIKap, pengguna hanya dapat menemukan rekod elektronik yang hak aksesnya mereka miliki. Meskipun ada rekod elektronik yang sesuai dengan kata kunci yang digunakan pengguna saat melakukan penelusuran tetapi hak aksesnya tidak dimiliki pengguna tersebut, maka tidak akan muncul dalam daftar hasil penelusuran. Dapat dikatakan bahwa pengguna tidak dapat mengetahui rekod-rekod elektronik apa saja yang dikelola dalam SIKap, karena hanya rekod elektronik yang hak aksesnya ia miliki yang akan ditampilkan oleh sistem. Hal ini ditetapkan sebagai upaya manajemen resiko dalam sistem, agar arsiparis juga terbantu pekerjaannya dalam menjaga akses pada setiap rekod elektronik dari pihak-pihak yang tidak memiliki wewenang.

Temuan dalam penelitian ini juga cukup serupa dengan temuan dalam Penerapan Standar Internasional Dalam Fitur Registrasi Aplikasi Sistem Informasi Kearsipan Dinamis (SIKD) di Kementerian Pertanian (Sendrian, 2013), yang juga memanfaatkan persyaratan ICA dalam melakukan observasi. Dalam penelitian tersebut ditemukan bahwa SIKD yang digunakan di Kementerian Pertanian secara garis besar sudah memenuhi persyaratan ICA yang berkaitan dengan kegiatan registrasi arsip ke dalam sistem. Ditemukan adanya beberapa persyaratan yang tidak dipenuhi, namun tidak menjadikan SIKD menjadi sistem yang tidak dapat mengakomodir kebutuhan para arsiparis di Kementerian Pertanian. Hanya saja tidak cukup fleksibel untuk menolerir *human error*. Sedangkan dalam penelitian ini, secara garis besar seluruh persyaratan terkait dengan hak akses sudah dipenuhi. Alasan yang ada dibalik beberapa persyaratan yang tidak dipenuhi adalah karena telah dilakukan penyesuaian antara persyaratan ICA dengan kebutuhan dan keadaan di Subbagian Persuratan dan Kearsipan KKP.

doi: 10.14710/lenpust.v5i1.23578

Daftar Pustaka

Ab Aziz, Azlina, Zawiyah Mohammad Yusof, Umi Asma' Mokhtar, and Dian Indrayani Jambari. 2018. "Electronic Document and Records Management System Implementation in Malaysia: A Preliminary Study of Issues Embracing the Initiative." Pp. 585–91 in *Transforming Digital Worlds*, edited by G. Chowdhury, J. McLeod, V. Gillet, and P. Willett. Springer International Publishing. (Retrieved: https://doi.org/10.1007/978-3-319-78105-1_65)

Bantin, Philip C. 2008. *Understanding Data and Information Systems for Recordkeeping*. New York: Neal-Schuman Publishers, Inc.

Creswell, John W. 2014. *Research Design - Qualitative, Quantitative, & Mixed Methods Approaches*. Vol. 4th Ed.

Ellis, Judith. 2008. "Implementing a Solution for Electronic Recordkeeping in the Public Sector." Pp. 163–85 in *Managing Electronic Records*, edited by J. Mcleod and C. Hare. London: Facet Publishing.

HP Software Big Data. 2015. *Choosing an EDRMS for Best Practice Records Management*. (Retrieved: https://cdn.shopify.com/s/files/1/0605/7777/files/HPE_Choosing_EDRMS.pdf)

Imine, Youcef, Ahmed Lounis, and Abdelmadjid Bouabdallah. 2018. "Revocable Attribute-Based Access Control in Multi-Authority Systems." *Journal of Network and Computer Applications* 122(January):61–76. (Retrieved: https://doi.org/10.1016/j.procs.2018.05.078)

International Council on Archives. 2008. *Principles and Functional Requirements for Records in Electronic Office Environments – Module 2: Guidlines and Fuctional Requirements for Electronic Record Management Systems*.

Lo, Nai Wei, Ta Chih Yang, and Ming Huang Guo. 2015. "An Attribute-Role Based Access Control Mechanism for Multi-Tenancy Cloud Environment." *Wireless Personal Communications* 84(3):2119–34. (Retrieved: https://doi.org/10.1007/s11277-015-2515-y)

Mcleod, Julie and Catherine Hare, eds. 2008. *Managing Electronic Records*. London: Facet Publishing.

Republik Indonesia. 2009. *Undang-Undang No 43 Tahun 2009 Tentang Kearsipan*. Jakarta: Sekretariat Negara Republik Indonesia.

Safady, William. 2012. *Managing Electronic Records*. 4th Edition. New York: Neal-Schuman Publishers, Inc.

Sendrian, Rengga. 2013. "Penerapan Standar Internasional Dalam Fitur Registrasi Aplikasi Sistem Informasi Kearsipan Dinamis (SIKD) Di Kementerian Pertanian." Universitas Indonesia.

Smallwood, F. Robert. 2013. *Managing Electronic Records: Methods, Best Practices, and Technologies*. New Jersey: John Wiley & Sons.

Wang, Ziheng. 2015. "Analysing the Impact of Electronic Health Records" edited by S. Siuly, I. Lee, Z. Huang, R. Zhou, H. Wang, and W. Xiang. *Health Information Science* 17(3):156–63. (Retrieved: https://doi.org/10.1007/978-3-030-01078-2_14)

Wijaya, Muhammad. 2013. "Penerapan Persyaratan Fungsional Administrasi Rekod Elektronik Studi Kasus World Bank Indonesia." Universitas Indonesia.

Williams, Caroline. 2006. *Managing Archives: Foundations, Principles, and Practice*. Oxford: Chandos Publishing (Oxford) Limited.

doi: 10.14710/lenpust.v5i1.23578