IMS
GOOD JOURNALISM | BETTER SOCIETIES

SAFEnet

PANDUAN AUDIT KEAMANAN DIGITAL UNTUK MEDIA DARING



PANDUAN AUDIT
KEAMANAN DIGITAL
UNTUK MEDIA DARING



SAFEnet

2025

Panduan Audit Keamanan Digital untuk Media Daring

Oktober 2025

Tim Penyusun:
Adi Marsiela
Anton Muhajir
Ardy Wibisana
Nike F. Andaru

Desainer & Tata Letak
Syamsul Arifin

Penerbit
Southeast Asia Freedom of Expression Network (SAFEnet)
Jalan Gita Sura III Nomor 55 Peguyangan Kaja
Denpasar, Bali 80123

Telepon : +62 817 9323375
Surel: info@safenet.or.id
Twitter & Instagram: @safenetvoice
Situs web: safenet.or.id

Lisensi Hak Cipta
CC BY-SA 4.0
Atribusi-BerbagiSerupa 4.0 Internasional

Daftar Isi

Daftar Isi.....vi
Pengantar Tim Penyusun.....vii
Pengantar IMS.....x
Tentang Panduan.....xii
Panduan Etik Audit.....xvi

A **Persiapan**.....1

1. Persiapan dan Perencanaan.....2
1.1 Ringkasan.....2
1.2 Tahapan.....2
1.2.1 Pembuatan Perjanjian.....3
1.2.2 Pengumpulan Informasi.....4
1.2.3 Penyusunan Jadwal.....5
1.2.4 Pertemuan Awal.....6
1.2.5 Persiapan Auditor.....7
1.3 Catatan.....8
1.4 Keluaran.....8
1.5 Acuan.....9

B **Pelaksanaan**.....11

2. Penilaian Risiko dan Ancaman.....12
2.1 Ringkasan.....12
2.2 Tahapan.....13
2.2.1 Analisis Isu dan Program.....13
2.2.2 Analisis Kerentanan.....19
2.2.3 Analisis Ancaman.....20
2.2.4 PAKEM DIRI.....22
2.3 Catatan.....22
2.4 Keluaran.....23
2.5 Acuan.....23

3. Penilaian Aset & Data.....25
3.1 Ringkasan.....25
3.2 Tahapan.....26
3.2.1 Memahami Konsep CIA/3K.....26
3.2.2 Menilai Kepatuhan terhadap Regulasi.....27
3.2.3 Memetakan Aset Digital.....30
3.2.4 Mendaftar Media Sosial & Pengelolaannya.....33
3.3 Catatan.....34
3.4 Keluaran.....34
3.5 Acuan.....35

4. Pemetaan Infrastruktur & Jaringan.....36
4.1 Ringkasan.....36
4.2 Tahapan.....37
4.2.1 Observasi Infrastruktur.....37
4.2.2 Pemindaian Situs Web.....39
4.2.3 Pemetaan Jaringan (Wi-Fi).....43
4.3 Catatan.....49
4.4 Keluaran.....49
4.5 Acuan.....49

C **Pelaporan.....51**

5. Penyusunan Laporan.....52
5.1 Ringkasan.....52
5.2 Tahapan.....53
5.2.1 Penyusunan Laporan.....53
5.2.2 Penyampaian Laporan.....55
5.3 Catatan.....55
5.4 Keluaran.....56
5.5 Acuan.....56

Daftar Istilah.....57
Daftar Piranti & Aplikasi.....65
Tabel Daftar Aset.....67
PAKEM DIRI.....68

Pengantar Tim Penyusun

MEDIA dan jurnalis merupakan salah satu kelompok rentan dan berisiko tinggi menjadi sasaran serangan digital di Indonesia. Berdasarkan pemantauan SAFEnet, dari total 323 korban serangan digital sepanjang tahun 2024, setidaknya 27 jurnalis dan media menjadi korban serangan dan insiden keamanan digital. Bentuk serangan digital itu termasuk peretasan situs web, penolakan terhadap layanan (DDoS), dan upaya pengambilalihan akun media sosial Instagram dan Twitter.

Serangan digital cenderung meningkat ketika ada isu kontroversial di tingkat nasional maupun lokal. Pada Mei 2024, serangan digital secara masif terjadi terhadap aktivis The People's Water Forum (PWF) yang mengadakan forum alternatif selama pelaksanaan World Water Forum (WWF) di Bali. Serangan dalam beragam bentuk, terutama peretasan akun WhatsApp dan doxing, juga terjadi pada masyarakat sipil yang menggelar aksi #PeringatanDarurat pada Agustus 2024.

Sejumlah media juga pernah mengalami serangan digital dalam bentuk penggantian tampilan halaman depan (*deface*), penyusupan malware, *distributed denial-of-service* (DDoS), dan pengambilalihan akun. Hal ini terjadi antara lain pada media lokal, seperti BaleBengong di Bali, Floresa di Manggarai Barat, dan Puan Khatulistiwa di Pontianak, maupun media nasional, seperti Tempo, Kompas, Project Multatuli, dan Suara.

Namun, meskipun serangan digital semakin masif dan beragam, di sisi lain masih banyak kelompok rentan dan berisiko tinggi ini yang masih belum memiliki kapasitas memadai dalam keamanan digital. Kesadaran tentang pentingnya keamanan digital, termasuk dari sisi kebijakan dan kemampuan teknis, di kalangan media Indonesia masih rendah. Riset Aliansi Jurnalis Independen (AJI) yang diterbitkan pada Agustus 2024 menemukan bahwa secara umum, indeks keamanan digital perusahaan media daring termasuk kurang baik, karena nilainya 19,71 dari nilai maksimal 31. Riset tersebut melibatkan 116 media daring (siber) di Indonesia dan mengukurnya dari aspek praktik dan persepsi keamanan digital.

SAFEnet, organisasi yang memperjuangan hak-hak digital, termasuk di dalamnya hak atas rasa aman di ranah digital, melihat pentingnya keamanan digital sebagai topik yang harus disebarluaskan kepada kelompok rentan dan berisiko tinggi di Indonesia, termasuk media. Untuk itu, selama tujuh tahun terakhir, SAFEnet melaksanakan program peningkatan kapasitas masyarakat sipil Indonesia di bidang keamanan digital.

Sebagai bagian dari upaya meningkatkan kapasitas keamanan digital masyarakat sipil tersebut, SAFEnet juga melakukan audit dan pendampingan keamanan digital bagi organisasi masyarakat sipil, termasuk jurnalis dan media. Audit bertujuan untuk menemukan risiko dan ancaman terhadap media serta bagaimana kapasitas mereka dalam menghadapi ancaman dan serangan tersebut.

Untuk menambah jumlah auditor dan memperluas jangkauan audit keamanan digital, SAFEnet melaksanakan proyek penyusunan panduan audit bagi media. Hal ini seiring dengan semakin tingginya kebutuhan audit keamanan digital, termasuk untuk media, tetapi di sisi lain jumlah auditor masih relatif terbatas.

Terima kasih kepada International Media Support (IMS) yang telah mendukung penyusunan panduan audit keamanan digital ini. Juga kepada semua peserta diskusi kelompok terpumpun (FGD) yang telah memberikan masukan penting terhadap panduan ini.

Kami berharap panduan ini bisa membantu praktisi keamanan digital maupun pengelola media daring yang ingin melakukan audit keamanan digital baik secara mandiri maupun pihak eksternal. Dan, tentu saja, dalam jangka panjang, temuan audit akan menjadi landasan bagi media untuk semakin meningkatkan keamanan digital masing-masing.

Denpasar, Oktober 2025

SAFEnet

Pengantar IMS

SEJAK tahun 2021, International Media Support (IMS) berkolaborasi untuk mendukung pertumbuhan dan perkembangan media lokal di Indonesia. Kami menyadari bahwa keamanan digital bukan hanya soal perlindungan teknis, tetapi juga sangat berpengaruh terhadap keberlanjutan bisnis media. Media yang mampu menjaga aset digital dan melindungi sistem kerjanya akan memiliki fondasi lebih kokoh untuk bertahan dan berkembang di tengah dinamika industri.

Di era digital saat ini, media memegang peran penting dalam memastikan masyarakat mendapatkan informasi yang akurat, independen, dan dapat dipercaya. Namun, peran tersebut tidak lepas dari tantangan, salah satunya meningkatnya risiko serangan digital yang mengancam kerja-kerja jurnalistik, keberlangsungan media, serta keamanan para jurnalis di Indonesia.

Kami percaya bahwa keamanan digital adalah fondasi bagi media untuk dapat bekerja secara profesional, terlindungi, dan berkelanjutan. Media tidak hanya memproduksi konten berkualitas, tetapi juga memastikan bahwa aset digital, data, serta infrastruktur kerja mereka terlindungi dari berbagai bentuk ancaman.

Atas dasar kebutuhan inilah, IMS mendukung inisiatif SAFEnet untuk menyusun *Panduan Audit Keamanan Digital untuk Media Daring*. Pan-

duan ini hadir sebagai instrumen praktis yang membantu media melakukan evaluasi, mengenali kerentanan, serta meningkatkan kapasitas perlindungan digital mereka. Dengan pendekatan yang sistematis—mulai dari persiapan, pelaksanaan, hingga pelaporan—panduan ini diharapkan dapat menjadi acuan penting bagi media, auditor, maupun praktisi keamanan digital.

Kami meyakini bahwa panduan ini bukan sekadar dokumen teknis, tetapi juga bagian dari upaya kolektif memperkuat ekosistem informasi yang sehat, inklusif, dan aman di Indonesia. IMS berharap panduan ini dapat memperluas jangkauan perlindungan digital, tidak hanya bagi media di kota-kota utama, tetapi juga bagi media lokal hingga ke pelosok nusantara. Dengan semakin banyak media yang mampu melindungi dirinya secara digital, semakin kuat pula daya tahan demokrasi kita terhadap ancaman disinformasi, serangan siber, dan upaya pembungkaman ruang publik.

IMS menyampaikan apresiasi kepada SAFEnet yang telah berhasil mewujudkan panduan ini, serta kepada para jurnalis dan pengelola media yang telah berkontribusi dalam proses penyusunan panduan ini. Semoga panduan ini dapat menjadi pijakan bagi media untuk terus berkembang dan menjalankan fungsi sosialnya dengan lebih aman.

Jakarta, Oktober 2025

International Media Support (IMS)

Tentang Panduan

PANDUAN ini merupakan acuan dalam melaksanakan audit keamanan digital untuk media, khususnya media daring. Materi panduan mencakup landasan teoritis dan praktis bagaimana sebuah audit keamanan digital media sebaiknya dilakukan, termasuk memahami konsep, tujuan, dan tahapan kerjanya.

Penyusunan panduan ini menggunakan tiga metode utama, yaitu:

- Kajian pustaka (*desk study*)
- Refleksi pengalaman (empiris)
- Diskusi kelompok terpumpun (FGD).

Materi utama panduan ini berdasarkan pada panduan audit keamanan digital yang sebelumnya sudah ada, meskipun tidak spesifik untuk media daring. Tiga materi utama sebagai acuan adalah:

- *CISA Official Review Manual 28th Edition* yang diterbitkan *Information Systems Audit and Control Association* (ISACA). Buku ini sebenarnya lebih ditujukan untuk kandidat Auditor Sistem Informasi Tersertifikasi (CISA), tetapi memberikan panduan lengkap bagaimana sebuah audit dilakukan.
- *Security Auditing Framework and Evaluation Template for Advocacy Groups* (SAFETAG), panduan audit keamanan digital untuk organisasi masyarakat sipil (OMS) dan kelompok advokasi yang diterbitkan Internews, serta

- *Panduan Audit Keamanan Digital untuk Organisasi Masyarakat Sipil* yang diterbitkan SAFEnet mengacu pada SAFETAG dan pengalaman SAFEnet sendiri melakukan audit maupun pendampingan keamanan digital bagi OMS.

Ketiga panduan tersebut memiliki karakter masing-masing. *CISA Official Review Manual 28th Edition*, misalnya, menyajikan panduan detail yang terbagi dalam lima domain, yaitu proses audit, tata kelola teknologi informasi, hingga pelindungan aset informasi. Panduan ini lebih tepat digunakan untuk perusahaan-perusahaan skala besar, seperti perbankan. Adapun SAFETAG secara spesifik khusus untuk OMS dan kelompok advokasi. Panduan ini lebih bersifat modular dan fleksibel penerapannya.

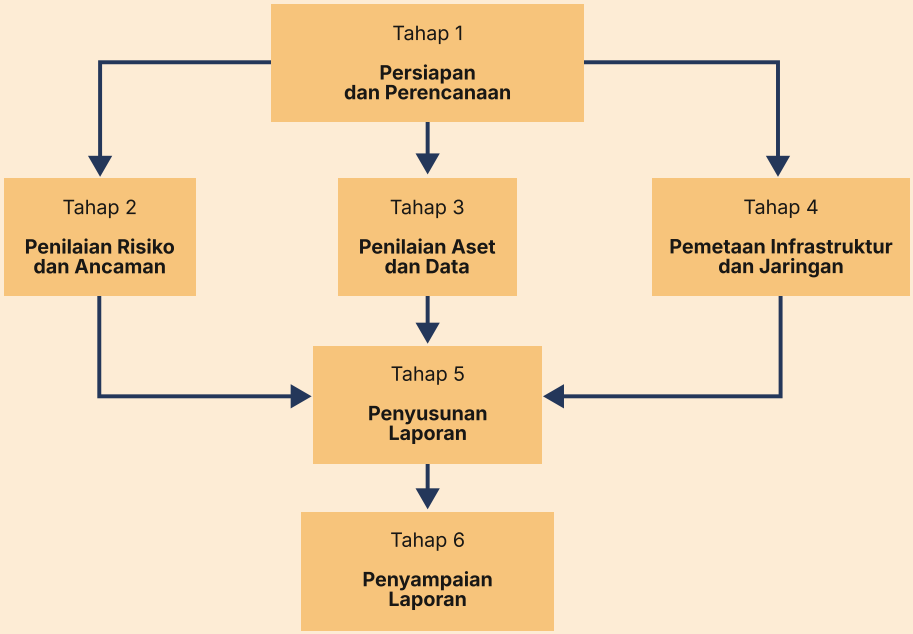
Tim penyusun panduan kemudian melakukan adaptasi dengan cara mengambil bagian-bagian yang relevan dengan tujuan utama audit keamanan digital untuk media daring. Bagian yang relevan dari ketiga panduan tersebut kami padukan dengan pengalaman secara langsung melakukan audit keamanan digital selama lima tahun terakhir. Meskipun audit oleh tim SAFEnet tersebut lebih banyak dilakukan untuk OMS, tetapi secara metode dan alur memiliki banyak kesamaan dengan audit untuk media daring. Tentu saja tetap ada karakter dan kebutuhan spesifik dalam audit media daring.

Untuk menguji hasil kajian pustaka dan refleksi pengalaman tersebut, kami melaksanakan FGD melibatkan dua kelompok utama, yaitu pengelola media dan praktisi keamanan digital. Selama FGD pada 8-9 September 2025 di Bali ini, para peserta yang memiliki pengalaman dan persepsi berbeda-beda tentang keamanan digital media daring, mendiskusikan draf panduan, terutama dari sisi struktur dan alur. Secara substansi, semua tahapan dan langkah juga dibahas meskipun tidak bisa sedetail mungkin karena keterbatasan waktu.

Materi Panduan

Panduan ini mencakup tiga bagian utama dalam proses audit, yaitu persiapan, pelaksanaan, dan pelaporan. Bagian Persiapan terdiri dari satu tahapan yaitu Persiapan dan Perencanaan yang terbagi dalam lima kegiatan mulai dari pembuatan perjanjian hingga persiapan auditor. Bagian Pelaksanaan terdiri dari tiga tahapan yaitu Penilaian Risiko dan Ancaman, Penilaian Aset dan Data, serta Pemetaan Infrastruktur dan Jaringan. Banyaknya tahapan di bagian ini menunjukkan bahwa bagian ini merupakan bagian paling penting dari keseluruhan proses audit. Bagian terakhir adalah Pelaporan yang terdiri dari dua tahapan, yaitu Penyusunan Laporan dan Penyampaian Laporan.

Berikut tahapan audit dalam bentuk bagan alur.



Setiap bagian mencakup kegiatan-kegiatan praktis bagaimana pelaksanaannya. Sebagai satu kesatuan proses, semua tahapan dan kegiatan dalam panduan ini harus dilakukan secara bertahap dan berurutan. Pengabaian terhadap salah satu tahapan dan kegiatan akan memengaruhi kedalaman temuan.

Oleh karena itu, panduan ini ditujukan untuk pengguna yang memiliki kapasitas dasar dalam keamanan digital. Misalnya sudah pernah mengikuti pelatihan keamanan digital, memiliki pendidikan formal manajemen informatika, sistem informasi atau staf teknologi informasi di medianya sendiri. Kapasitas dasar di sini mencakup pengetahuan dan keterampilan, baik dari sisi manajemen maupun teknis tertentu, misalnya pemeriksaan jaringan.

Kapasitas dasar bagi pengguna panduan ini sangat berguna sebagai landasan agar audit bisa berjalan lebih baik. Hal tersebut karena panduan ini berisi informasi dan istilah-istilah terkait keamanan digital yang belum tentu bisa dipahami publik secara luas, terutama dalam konteks keamanan digital bagi media daring.

Panduan Etik Audit

PANDUAN etik adalah sejumlah norma yang perlu diperhatikan baik oleh auditor maupun auditi. Panduan ini berfungsi untuk menciptakan ruang aman bagi kedua belah pihak dan memastikan proses audit berjalan dengan baik.

Panduan Etik Auditor

Pada saat melaksanakan sebuah audit, seorang auditor terikat pada etika, baik bersifat umum maupun spesifik. Panduan etik di bawah diadaptasi dari Kode Etik ISACA dan SAFETAG, di mana seorang auditor harus:

- Menghormati auditi, termasuk latar belakang dan identitas maupun konteks isu yang mereka kerjakan.
- Melindungi informasi, privasi, dan keamanan auditi kecuali terdapat permintaan untuk kepentingan hukum.
- Menghindari penggunaan pengetahuan, keterampilan dan atau akses untuk melakukan kekerasan atau kerusakan terhadap auditi.

- Menghindari konflik kepentingan melalui transparansi dalam kontrak, pelaporan dan rekomendasi.
- Melakukan pekerjaan secara bertanggung jawab dan profesional sesuai dengan standar audit yang dimiliki.
- Menghormati auditor lain sebagai rekan serta mendorong proses audit yang aman, inklusif, dan bebas kekerasan.
- Memberitahukan hasil audit kepada auditi secara komprehensif termasuk temuan dan rekomendasinya.

Panduan Etik Auditi

Meskipun belum ada panduan hitam di atas putih oleh satu organisasi atau lembaga apapun, pada dasarnya seorang auditi juga tetap perlu memiliki panduan etik ketika sedang diaudit. Etika tersebut termasuk:

- Memberikan akses sepenuhnya kepada auditor untuk melakukan pekerjaannya, terutama terhadap dokumen, personel, atau aset digital, yang diperlukan selama audit.
- Memberikan informasi yang benar, jujur, dan lengkap sesuai dengan kebutuhan audit.
- Mengelola dan menyimpan semua dokumen yang dibuat sebelum, selama, maupun setelah pelaksanaan audit.
- Tidak melakukan intervensi terhadap proses audit yang bisa memengaruhi hasil audit sehingga tidak sesuai dengan keadaan sebenarnya.
- Menyediakan waktu dan sumber daya yang cukup untuk mendukung proses audit agar audit bisa selesai sesuai rencana.
- Menindaklanjuti temuan dan rekomendasi audit sesuai kesepakatan dengan auditor termasuk dari sisi prioritas dan jadwal pelaksanaan.

BAGIAN A

PERSIAPAN



1. Persiapan dan Perencanaan

1.1 Ringkasan

Sebelum melaksanakan audit, auditor terlebih dahulu harus membuat persiapan dan perencanaan. Tujuan utamanya untuk memastikan kedua belah pihak, baik auditor maupun auditi, memahami alur kerja dan keluarannya berdasarkan perjanjian kerja sama dan jadwal yang disepakati.Tahapan ini termasuk membuat perjanjian kerja sama (PKS) dan perjanjian kerahasiaan atau *non-disclosure agreement* (NDA) dengan media yang diaudit, khususnya jika auditor adalah pihak eksternal. Persiapan ini juga termasuk menentukan ruang lingkup, tahapan, dan jadwal audit.

Rangkaian audit tersusun atas tahap persiapan, pelaksanaan, dan penyusunan laporan. Beberapa audit mungkin memiliki tahapan ekstra, yaitu tahap perbaikan dan tahap uji ulang. Pendekatan yang mencakup dua tahap tambahan ini lebih komprehensif dan memuaskan karena diharapkan setelah rangkaian kegiatan audit selesai, sudah tidak ada lagi (atau sangat minim) sisa masalah yang ditemui saat audit.

1.2 Tahapan

Kegiatan yang harus dilakukan dalam tahap persiapan termasuk:

- Pembuatan Perjanjian
- Pengumpulan Informasi
- Penyusunan Jadwal
- Pertemuan Awal
- Persiapan Auditor

1.2.1 Pembuatan Perjanjian

PKS dan NDA diperlukan sebagai jaminan tertulis atau bahkan dasar hukum bahwa kedua belah pihak, yaitu auditor dan auditi, sepakat melakukan kerja sama audit dan akan menjaga kerahasiaan satu sama lain. Hal ini karena selama proses audit akan banyak informasi internal media yang diaudit akan dibagikan ke auditor untuk diperiksa atau diungkap sebagai bahan diskusi dan kegiatan audit lain, termasuk data dan informasi yang bersifat rahasia dan konfidensial.

Kedua dokumen tersebut bisa jadi terpisah, misalnya bila diperlukan untuk membuat NDA bagi masing-masing personel audit yang terlibat, bukan hanya satu atas nama media organisasi pelaksana audit. Perjanjian kerja sama cukup satu untuk masing-masing pihak.

PKS ini setidaknya harus mencantumkan informasi berikut:

- Identitas kedua belah pihak yaitu nama auditor dan auditi, alamat, serta kontak masing-masing.
- Tujuan audit yaitu untuk apa audit tersebut dilakukan.
- Ruang lingkup audit keamanan digital untuk media bisa dibagi menjadi dua, yaitu auditor sebagai pelaksana audit dan auditi sebagai pihak yang diaudit.
- Ruang lingkup audit mencakup apa saja yang mau diaudit. Misalnya, profil, risiko dan ancaman, kapasitas media, aset-aset digital, dan sumber daya manusia.
- Metode untuk melakukan audit. Biasanya mencakup wawancara, diskusi terfokus, pemindaian situs web, observasi kantor, dan lain-lain.
- Periode yaitu berapa lama audit akan dilaksanakan dan dari tanggal berapa hingga tanggal berapa. Proses audit biasanya memerlukan waktu setidaknya tiga bulan.
- Hak dan kewajiban masing-masing pihak baik auditor dan media yang diaudit. Misalnya, kewajiban bagi media untuk memberikan

informasi yang diperlukan dan kewajiban auditor untuk bekerja secara profesional.

- Kerahasiaan data yaitu jaminan bahwa auditor tidak akan membocorkan data dan informasi media kepada pihak lain.
- Informasi tambahan termasuk kemungkinan perubahan periode kerja jika audit tidak selesai selama periode yang sudah disepakati.

NDA ini setidaknya harus mencantumkan informasi berikut:

- Identitas kedua belah pihak yaitu nama auditor dan organisasi, alamat, dan kontak masing-masing.
- Hak dan kewajiban masing-masing pihak baik auditor dan auditi, misalnya, kewajiban bagi organisasi untuk memberikan informasi yang diperlukan dan kewajiban auditor untuk bekerja secara profesional.
- Kerahasiaan data yaitu jaminan bahwa auditor tidak akan membocorkan data dan informasi organisasi kepada pihak lain.
- Penyelesaian Sengketa merupakan bagian dalam Perjanjian Kerahasiaan untuk membantu memastikan kerahasiaan data tetap terjaga apabila terjadi perselisihan atau perbedaan pendapat antara kedua belah pihak.

1.2.2 Pengumpulan Informasi

Guna membantu media dalam memastikan adanya PKS atau NDA, modul ini menyediakan lampiran format perjanjian termasuk memuat informasi yang wajib tercantum di dalamnya.

Dalam tahap ini, auditor mengumpulkan berbagai informasi umum terkait media, sebagai bahan awal untuk menggali lebih dalam media yang akan diaudit. Berbagai hal yang ditemukan saat pencarian informasi ini dapat mengarah ke usulan kegiatan yang relevan pada sesi pertemuan awal. Eksekusi kegiatannya disesuaikan dengan jadwal kegiatan audit.

Informasi yang dikumpulkan dapat berupa situs-situs web, penyedia surel, dan media sosial. Umumnya, informasi tersebut tersedia secara publik, sehingga proses pengumpulan bisa dilakukan secara mandiri. Termasuk di dalamnya, aktivitas atau kegiatan di luar produksi konten berita.

1.2.3 Penyusunan Jadwal

Setelah PKS ditandatangani kedua belah pihak, auditor harus menyiapkan tahapan dan jadwal pelaksanaan audit. Kesepakatan tahapan dan jadwal ini berguna sebagai acuan bagi kedua belah pihak terutama dalam persiapan waktu dan apa saja dokumen yang perlu disiapkan organisasi yang akan diaudit.

Contoh tahapan dan dokumen tersebut bisa dilihat dalam tabel berikut, tetapi bisa disesuaikan dengan kondisi nyata pada saat pertemuan awal dengan auditi:

Tabel 1: Tahapan dan kebutuhan dalam persiapan audit keamanan digital

Tahapan	Kebutuhan
1. Perencanaan dan Persiapan	Perjanjian kerahasiaan, alur kerja dan formulir penilaian yang disepakati kedua belah pihak
2. Penilaian Keamanan Perangkat	Formulir penilaian, jadwal wawancara staf
3. Penilaian Keamanan Website	Daftar website media, termasuk subdomainnya jika ada
4. Penilaian Keamanan Jaringan	Admin jaringan
5. Pemetaan Risiko dan Mitigasi	Informasi tentang nama SSID dan kata sandinya.
6. Penilaian Kebijakan Keamanan	Penemuan kerentanan dan rencana aksi
7. Penyusunan SOP Keamanan Digital	Kebijakan dan SOP Keamanan Digital untuk organisasi
8. Penyusunan Laporan Akhir	Laporan audit, pemindaian, dan hasil wawancara & SOP Keamanan Digital

1.2.4 Pertemuan Awal

Setelah adanya PKS dan jadwal audit, perlu semacam *kick-off meeting* atau pertemuan awal. Dalam pertemuan awal tersebut auditor akan berkenalan dengan pihak auditi secara tatap muka langsung (luring) ataupun daring.

Dalam pertemuan awal ini tim auditor akan berkenalan dengan pihak manajemen auditi dan juga beberapa staf dengan maksud menjelaskan proses audit yang akan dilakukan. Beberapa hal yang perlu dijelaskan auditor dalam pertemuan ini yaitu:

- Berapa lama proses audit akan berjalan dari mulai pembuatan NDA hingga penyusunan laporan. Biasanya dalam rentang wak-

tu tiga bulan, tetapi bisa lebih lama dan bisa lebih cepat sesuai dengan kebutuhan audit.
- Siapa saja yang akan dilibatkan dalam proses audit ini. Misalnya siapa saja yang perlu diwawancarai, seberapa lama waktu untuk wawancara, apa saja yang perlu disiapkan, hingga kemungkinan terhubung dengan pihak ketiga jika dibutuhkan
- Bagaimana proses audit akan dilakukan, apa metodenya, kebutuhan data untuk audit, luring atau daring, dll.

Pertemuan ini diharapkan bisa memberikan gambaran secara keseluruhan proses audit yang akan dijalankan, sehingga pihak auditor dan auditi bisa saling bekerja sama dalam prosesnya sehingga semua berjalan dengan lancar.

1.2.5 Persiapan Auditor

Agar nantinya audit berjalan dengan baik, auditor perlu juga secara mandiri menyiapkan dan memastikan beberapa hal, termasuk:

- Peralatan bantu audit sudah tersedia dan siap dipakai (perangkat keras, perangkat lunak, daftar periksa, maupun alat bantu lain)
- Rencana perjalanan, akomodasi, transportasi, dan logistik lain yang diperlukan saat audit.

Pada kondisi tertentu ketika melakukan audit terhadap organisasi dengan risiko tingkat tinggi, perlu juga persiapan manajemen risiko yang baik.

Auditor juga perlu menginformasikan beberapa hal yang perlu disiapkan pihak auditi, yaitu:

- Profil organisasi, termasuk kegiatan dan struktur media.

- Aset digital apa saja yang akan diaudit, termasuk situs web, data, media sosial, dan infrastruktur media.
- Personel yang terlibat dalam proses audit, termasuk pimpinan umum, staf IT, dan atau staf lain yang relevan.

1.3 Catatan

Tahapan persiapan ini bagian penting dalam kegiatan audit keamanan digital perusahaan media. Dukungan dan persetujuan dari pimpinan atau pembuat kebijakan di media akan sangat membantu seluruh proses audit. Menurut hasil laporan evaluasi SAFETAG oleh Purpose+motion, 95% auditor dan auditi merasakan bahwa partisipasi manajemen merupakan suatu hal yang penting dalam keberhasilan proses audit. Hal ini senada dengan pengalaman-pengalaman SAFEnet.

Apabila proses audit dilakukan oleh pihak ketiga atau eksternal, perusahaan media wajib mempersiapkan perjanjian kerjasama agar proses audit memiliki acuan dan akuntabilitas antar para pihak.

1.4 Keluaran

Keluaran dari tahapan ini adalah:

- Perjanjian dengan organisasi yang akan diaudit, mencakup ruang lingkup, linimasa, kebijakan kerahasiaan, dan nomor kontak.
- Daftar periksa perangkat (keras dan lunak) untuk mendukung pelaksanaan audit.

1.5 Acuan

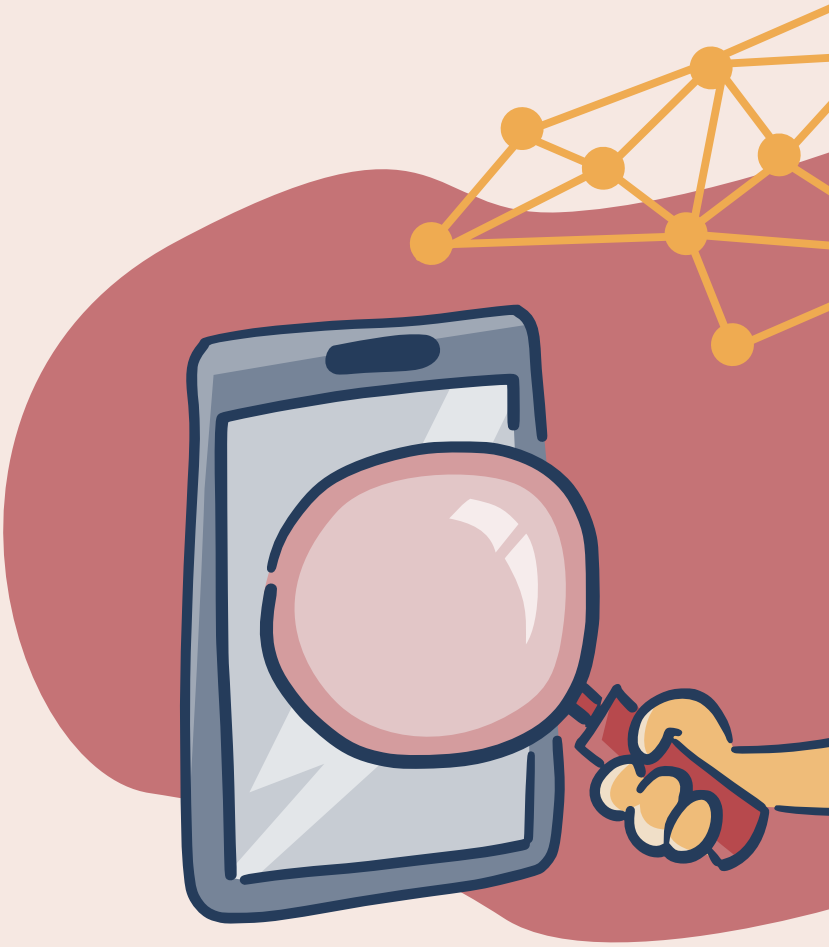
Informasi lebih lanjut terkait persiapan dan perencanaan audit adalah:

- Assessment Plan https://safetag.org/activities/assessment_plan
- Confidentiality Agreement https://safetag.org/activities/confidentiality_agreement
- Incident Response and Emergency Contact https://safetag.org/activities/incident_response
- Regional Context Research https://safetag.org/activities/regional_context_research
- Technical Context Research https://safetag.org/activities/technical_context_research
- Audit Timeline and Planning https://safetag.org/activities/safetag_audit_timeline
- Incident Response https://safetag.org/activities/incident_response/



BAGIAN B

PELAKSANAAN



2. Penilaian Risiko dan Ancaman

2.1 Ringkasan

Penilaian risiko dan ancaman merupakan bagian paling penting dalam audit keamanan digital, termasuk untuk media daring. Tujuan rangkaian aktivitas penilaian risiko guna mengumpulkan informasi yang cukup untuk mengidentifikasi dan menilai berbagai risiko yang dihadapi suatu media dan aktor terkait sehingga mereka dapat mengambil tindakan secara strategis.

Secara garis besar, proses ini mencakup tiga tahap, yaitu analisis isu dan program, analisis kerentanan, dan analisis ancaman. Berdasarkan tiga tahapan tersebut akan ditemukan tingkat risiko sebagai hasil perpaduan antara kemungkinan dan dampak. Risiko dinilai dengan membandingkan ancaman terhadap suatu media dengan kerentanannya dan kapasitasnya untuk merespons atau memitigasi ancaman yang muncul.

Ringkasnya, tingkat risiko sama dengan kemungkinan dikalikan dampak (tingkat risiko = kemungkinan x dampak). Sebagai contoh, jika kemungkinan terjadinya tinggi dan dampaknya juga tinggi, maka tingkat risikonya jelas tinggi. Sebaliknya, jika kemungkinan terjadinya rendah dan dampaknya juga rendah, maka tingkat risikonya juga rendah.

Kemungkinan adalah seberapa besar sebuah serangan atau insiden keamanan digital bisa atau akan terjadi. Dampak adalah seberapa besar kerugian yang akan terjadi pada media tersebut jika serangan atau insiden keamanan digital terjadi. Sebagai perbandingan, serangan terhadap situs web dalam bentuk DDoS atau *deface* tentu lebih besar dampaknya terhadap media daring yang sepenuhnya bergantung pada situs web dibandingkan intimidasi daring terhadap jurnalisnya.

2.2 Tahapan

Proses analisis risiko dan ancaman dibagi menjadi tiga tahap, yaitu Analisis Isu dan Program, Analisis Kerentanan, dan Analisis Ancaman. Proses ini juga dilengkapi dengan perangkat penilaian risiko PAKEM DIRI yang mencakup pemeriksaan laptop, ponsel, identitas, dan komunikasi. Secara empiris, tingkat risiko tersebut dipengaruhi tiga faktor utama, yaitu:

- Sensitifnya isu yang dikerjakan,
- Penggunaan teknologi digital, dan
- Kapasitas keamanan digital.

Penggunaan teknologi digital terkait erat dengan aktivitas. Sementara sensitivitas isu terkait dengan isu dan program yang media kerjakan atau fokuskan. Adapun, kapasitas media bisa dinilai dari tiga komponen, masing-masing: proses (termasuk kebijakan), orang (sumber daya manusia), dan platform (teknologi yang digunakan).

2.2.1 Analisis Isu dan Program

Tahap ini merupakan proses menggali lebih dalam apa isu dan program utama sebuah media. Proses ini juga memaparkan profil, aktivitas, aktor, dan kapasitas suatu media. Contohnya apa saja kegiatan yang dilakukan media untuk mencapai tujuannya. Lembaga media, khususnya yang bergerak dengan isu sensitif, rentan mengalami dan menjadi target lebih intens. Misalnya, media yang mengadvokasi isu Papua bisa jadi lebih rentan terhadap ancaman dibandingkan media yang membahas hobi atau olahraga.

Terkait profil media, pertanyaan yang perlu digali termasuk:

- Bagaimana profil media?
- Apakah media sudah terverifikasi dan tercatat di Dewan Pers?

- Bagaimana struktur di media?
- Apa tugas dan fungsi masing-masing dalam struktur tersebut?

Sensitivitas Isu

Dalam konteks isu yang dikerjakan, temuan SAFEnet menunjukkan sensitivitas isu berpengaruh terhadap tingkat risiko dan bentuk serangan yang mungkin terjadi. Meskipun tidak spesifik membahas isu dan program media, analisis berikut bisa menjadi acuan untuk menentukan sejauh mana sebuah media memiliki tingkat risiko berdasarkan isu yang mereka liput atau publikasikan.

Tabel 2: Risiko dan bentuk serangan digital terhadap OMS berdasarkan isu yang dikerjakan.

Latar Belakang	Serangan halus (non-teknis)	Serangan Kasar (teknis)	Keterangan
Papua	▪ Trolling ▪ Sextortion ▪ Impersonasi ▪ Intimidasi	▪ DDoS Attack ▪ Pemutusan kabel Internet ▪ Robocall ▪ Zoom Bombing ▪ Pencurian laptop	
Lingkungan	▪ Doxing ▪ Intimidasi	▪ Peretasan situs web ▪ Pengambilalihan akun	
LGBTQ	▪ NCII ▪ Impersonasi ▪ Online Exhibitionism ▪ Trolling	▪ Peretasan akun media sosial ▪ Peretasan akun pesan ringkas	▪ Terkait erat dengan KBGO
Jurnalis	▪ Doxing ▪ Trolling	▪ DDoS Attack ▪ Peretasan Akun	
Demokrasi dan HAM		▪ Pengambilalihan Akun Instagram dan WhatsApp	
Perempuan	▪ Impersonasi		▪ Relatif lebih rendah risikonya

Sumber: Sudah Rentan, Kurang Waspada Pula. (SAFEnet, 2022).

Aktivitas

Aktivitas atau kegiatan adalah tindakan dan proses yang disepakati oleh seluruh elemen media untuk menghasilkan karya jurnalistik, baik yang terkait redaksi maupun bisnis. Kegiatan ini terutama yang dilakukan media untuk mencapai tujuannya. Misalnya, produksi dan penyebaran konten berita, advokasi isu publik, atau diskusi di dalam atau luar kantor media, hingga penggalangan dana. Bentuk-bentuk aktivitas sebuah media juga berpengaruh terhadap tingkat risiko keamanan digitalnya.

Meskipun sebagian besar pekerjaan media berproses pada produksi berita, kegiatan lain tetap berkelindan dengan keamanan digital. Mulai dari penggunaan teknologi saat mencari sumber informasi, liputan ke lapangan, produksi, penyebaran, hingga diskusi terkait konten yang diterbitkan. Semakin tinggi ketergantungan pemanfaatan teknologi digital pada sebuah media, maka semakin tinggi tingkat risikonya. Penting bagi media untuk mendetilkan pemanfaatan teknologi pada setiap aktivitas yang mereka lakukan.



Model bisnis sebuah media juga menjadi bagian yang perlu diketahui auditor. Karena penyampaian informasi mengenai model bisnis seperti menggelar kegiatan pelatihan dan pihak media mengumpulkan data pribadi peserta, menggelar kegiatan dengan kelompok minoritas, hingga memanfaatkan *programmatic ads*.

Pertanyaan yang perlu dijawab terkait aktivitas media bisa mencakup:

- Apa saja isu berisiko yang disoroti?
- Apa saja program selain produksi konten berita?
- Siapa sasaran utama program tersebut?
- Apa saja kegiatan dan isu penerima manfaat programnya?

Berikut contoh dari identifikasi risiko dan ancaman terkait aktivitas atau kegiatan media yang disajikan dalam format tabel. Setiap media bisa memiliki penilaian yang berbeda, tergantung kegiatannya.

Tabel 3: Bentuk risiko dan ancaman digital yang potensial terjadi terhadap media menurut kegiatannya.

Kegiatan	Risiko dan Ancaman
Pengelolaan dan kampanye media sosial	▪ Peretasan ▪ Pengambilalihan akun ▪ Phishing ▪ Persekusi daring
Aktivitas daring pada kantor	▪ Penyadapan ▪ Pengawasan ilegal
Komunikasi Internal	▪ Peretasan ▪ Penyadapan ▪ Pengambilalihan akun
Pengelolaan Website	▪ Injeksi SQL ▪ Serangan DDoS ▪ Peretasan ▪ Impersonasi Web ▪ Malvertising ▪ Kebocoran data
Pengumpulan Data	▪ Kebocoran data ▪ Kehilangan data ▪ Perusakan data

Aktor

Dalam konteks analisis risiko dan ancaman, yang dimaksud dengan aktor di sini adalah semua pihak yang berpotensi untuk melakukan

serangan digital maupun berperan terhadap pengamanan keamanan digital. Pihak-pihak tersebut bisa berupa individu maupun organisasi. Namun, dalam proses analisis risiko dan ancaman, pemetaan difokuskan pada aktor yang potensial menjadi seteru atau penyerang.

Pemetaan aktor bisa dilakukan berdasarkan isu yang dikerjakan sebuah media disertai dengan kapasitas mereka masing-masing maupun kemungkinan mereka melakukan serangan. Sebagai contoh, jika sebuah media mengerjakan liputan terkait dengan korban bisnis tambang, maka aktor-aktor yang berpotensi melakukan serangan adalah perusahaan tambang atau dalam skala tertentu juga negara.

Pada dasarnya aktor-aktor tersebut terbagi menjadi tiga jenis utama, yaitu negara, swasta, dan publik. Setiap jenis aktor memiliki potensi dan kapasitas berbeda-beda sebagai seteru. Semakin detail penjelasan tiap aktor akan semakin mudah memetakan potensi dan kapasitas mereka. Aktor negara, misalnya, bisa didetailkan lagi apakah kepolisian, militer, kementerian, dan seterusnya. Begitu pula dengan swasta, apakah perusahaan tambang, pelaku bisnis kecil, dan lain-lain.



Kapasitas melakukan serangan terkait dengan sumber daya yang mereka miliki. Katakanlah, jika media meliput korban penangkapan sewenang-wenang, maka mereka berpotensi mengalami serangan dari kepolisian yang tentu memiliki unit siber lebih canggih dibandingkan pelaku bisnis. Selain kapasitas, potensi juga bisa dilihat dari riwayat aktor dalam melakukan serangan digital di waktu-waktu lain.

Pertanyaan terkait pelaku ancaman bisa termasuk:

- Apakah bisa diketahui siapa pelaku ancaman dan serangan tersebut?
- Teknik apa yang mereka gunakan?
- Apakah mereka menargetkan kerentanan media saat ini?

- Apakah mereka menargetkan media serupa atau hanya menyasar media yang diaudit?
- Apa saja metode yang digunakan oleh pelaku ancaman untuk menyerang media serupa?
- Apakah pelaku ancaman saat ini mempunyai keinginan untuk melakukan serangan terhadap media ini?
- Apakah media merupakan target ancaman prioritas bagi pelaku ancaman?

Kapasitas

Penilaian kapasitas keamanan digital mencakup tiga komponen, yaitu proses (termasuk kebijakan), orang (sumber daya manusia), dan platform (teknologi yang digunakan). Dalam bahasa Inggris, biasanya disebut 3P, yaitu *process, people, and platform*. Istilah tersebut tetap bisa digunakan jika lebih memudahkan.

- **Proses:** Komponen proses bertujuan memeriksa ada tidaknya sebuah kebijakan untuk memastikan proses kerjanya berlangsung dengan aman. Sasaran utama audit ini adalah level pimpinan. Kebijakan ini tidak harus secara spesifik terkait keamanan digital, tetapi bisa juga terkait pengelolaan data dan informasi atau pengamanan situs web dan media sosial. Lalu, jika terdapat kebijakan, apakah diterapkan dengan konsisten dan diperbarui secara berkala? Penting juga melihat apakah terdapat penanggung jawab untuk memastikan keamanan semua proses. Selain penanggung jawab juga perlu melihat kebijakan pimpinan terkait alokasi biaya dan kemauan untuk memberikan contoh bagi stafnya.

- **Sumber daya manusia:** Komponen sumber daya manusia ini mencakup ketersediaan dan keterampilan staf media untuk menjalankan proses produksi, penyebaran konten berita, hingga

memengaruhi perubahan termasuk pendanaan, jaringan, serta proses dan kebijakan kelembagaan. Sasaran utama pemeriksaan ini di level staf. Pertanyaan yang perlu dijawab termasuk: Apakah jurnalis atau staf mendapatkan pelatihan yang memadai untuk mengenali dan merespons ancaman? Apakah staf memiliki keterampilan dan pengetahuan yang diperlukan untuk penerapan keamanan yang efektif? Penting untuk mengingat bahwa sumber daya manusia meliputi semua orang yang terhubung dengan suatu organisasi media, termasuk jurnalis, desainer, staf sekretariat redaksi, dewan pengurus/pengawas, admin media sosial, bahkan bagian logistik.

- **Platform:** Komponen platform mencakup perangkat yang digunakan media dan semua stafnya. Sasaran utama pemeriksaan adalah perangkat. Penilaian terkait dengan penggunaan dan pemilihan teknologi untuk membantu seluruh proses tersebut. Apakah teknologi yang digunakan memadai dan terus diperbarui? Apakah menggunakan sistem operasi terbaru? Apakah terdapat aplikasi bajakan? Penggalian informasi mengenai kualitas teknologi perangkat keras dan perangkat lunak yang digunakan akan berpengaruh terhadap tingkat keamanan sebuah media.



2.2.2 Analisis Kerentanan

Kerentanan adalah celah keamanan pada media yang dapat dieksploitasi pihak lain. Misalnya, ketiadaan kebijakan keamanan bakal menyulitkan pemimpin atau pengambil kebijakan di media untuk menerapkan mitigasi keamanan. Alasannya, karena tidak ada sebuah acuan yang dapat dijadikan pegangan atau panduan.

Langkah ini serupa *medical check up* untuk mengetahui apakah seseo-

rang menderita penyakit tertentu dan seberapa parah. Langkah ini sangat penting karena mengidentifikasi masalah dan potensi masalah yang belum tentu disadari keberadaannya oleh media, sehingga sangat boleh jadi perlu auditor dari luar untuk memeriksanya.

Analisis kerentanan dilakukan untuk mengetahui paparan ancaman, titik lemah, dan cara-cara lain untuk memengaruhi media. Contohnya isu yang dikerjakan, praktik mitigasi yang belum dilakukan, dan sejauh mana ketergantungannya pada teknologi digital. Kerentanan lain, yang lebih teknis misalnya, pemanfaatan *plugin* yang tidak diperbarui dapat menimbulkan celah pada keamanan situs web media.

Berikut contoh beberapa kerentanan yang biasa ditemukan saat audit adalah:

- Penggunaan sistem operasi dan atau program bajakan pada laptop staf,
- Tidak ada pencadangan data pada laptop dan ponsel staf,
- Kata sandi yang terlalu mudah ditebak karena identik dengan pengguna, misalnya, nama dan tahun pembuatan akun,
- Sistem pengelolaan konten (CMS) dan *plugin* situs web yang tidak diperbarui, dan
- Berbagi hosting (*shared hosting*) situs web dengan situs web lain.

Kerentanan di atas hanya sekadar contoh. Kerentanan lain bisa ditemukan lebih lanjut pada saat audit.

2.2.3 Analisis Ancaman

Analisis ancaman adalah proses mengidentifikasi apa saja serangan potensial dan dampaknya bagi media. Identifikasi itu perlu menyertakan riwayat ancaman yang pernah terjadi terhadap media. Untuk memu-

dahkan analisis ancaman digital terhadap media daring, auditor bisa menggunakan komponen dan pertanyaan berikut:

Risiko dan Ancaman Digital

- Apa saja risiko dan ancaman serangan digital yang mungkin terjadi?
- Seberapa besar kemungkinan dan intensitasnya?
- Apa saja riwayat serangan yang pernah terjadi?
- Jika pernah terjadi, bagaimana dampaknya? Bagaimana penanganannya?

Semua proses tanya jawab tersebut bisa dilakukan melalui wawancara secara tatap muka maupun secara daring. Namun, metode yang paling baik adalah melalui diskusi terfokus secara langsung bersama semua staf media.

Semua temuan dalam wawancara itu dapat dimasukkan dalam matriks dengan variabel kemungkinan dan dampak. Hal ini dapat membantu auditor dalam memetakan tingkat risiko. Sebagai ilustrasi, matriks di bawah ini dapat dijadikan acuan, tetapi identifikasi ancaman ini bisa jadi berbeda-beda bagi setiap media.

Kemungkinan Tinggi, Dampak Rendah ▪ Penyadapan ▪ Pengawasan ilegal ▪ Kebocoran data ▪ Serangan Malware ▪ Ransomware	Kemungkinan Tinggi, Dampak Tinggi ▪ Peretasan ▪ Pengambilalihan akun ▪ Serangan DDOS ▪ Persekusi daring ▪ Pengancaman ▪ Phising
Kemungkinan Rendah, Dampak Rendah ▪ Injeksi Iklan ▪ Komentar Spam	Kemungkinan Rendah, Dampak Tinggi ▪ Malvertising

2.2.4 PAKEM DIRI

PAKEM DIRI merupakan singkatan dari Penilaian Keamanan Digital Mandiri. Metode penilaian keamanan digital ini dikembangkan SAFEnet untuk mengetahui tingkat risiko di level individu staf dan bersifat kuantitatif.

Penilaian mengacu pada pengaturan keamananempat komponen, yaitu laptop, ponsel, identitas, dan komunikasi. Terdapat 50 pertanyaan tertutup dengan jawaban "Ya" dan "Tidak". Setiap pertanyaan mewakili sebuah kondisi yang harus dijawab secara jujur, sesuai kondisi yang ada. Oleh karena itu, hasil PAKEM DIRI sangat bergantung pada kejujuran pengisinya.

Penilaian tiap individu lalu dikumpulkan dan dijadikan penilaian keamanan digital di tingkat organisasi atau perusahaan media dengan cara mendapatkan nilai rata-rata. Nilai rata-rata tersebut akan menunjukkan tingkat risiko di level organisasi yang terbagi menjadi lima kondisi, mulai dari rentang tingkat risiko sangat rendah hingga risiko sangat tinggi.

Formulir PAKEM DIRI dan petunjuk pengisiannya terdapat dalam lampiran panduan ini.

2.3 Catatan

Penilaian risiko dan ancaman maupun tingkat risiko adalah aktivitas yang bersifat subjektif. Tidak ada hitungan pasti ala matematika dalam penilaian tingkat risiko. Oleh karena itu, auditor tidak perlu khawatir dengan hasil yang subjektif. Meskipun demikian, hasil penilaian risiko, ancaman, dan tingkat risiko tersebut harus disertai dengan penjelasan berdasarkan temuan-temaun audit mencakup analisis isu dan program, kegiatan, hingga kapasitas sebagaimana telah disebutkan di atas.

Tahapan penilaian risiko dan ancaman ini memerlukan dukungan, parti-

sipasi, serta keterbukaan dari tingkat pimpinan sebagai pengambil keputusan hingga seluruh staf media. Pengumpulan informasi oleh auditor pada tahapan ini akan membantu proses audit dan penyusunan laporan audit.

2.4 Keluaran

Berdasarkan penilaian ini hasil yang akan didapatkan adalah sebagai berikut:

- Data pemetaan risiko pada jaringan dan perangkat organisasi yang diaudit.
- Daftar pemetaan risiko dari program dan kegiatan inti organisasi.
- Pemetaan ancaman dalam bentuk tabel dan matriks

2.5 Acuan

Informasi lebih lanjut terkait penilaian risiko dan ancaman adalah:

- Process Mapping and Risk Modeling https://safetag.org/methods/risk_modeling
- Threat Assessment https://safetag.org/methods/threat_assessment
- Process Mapping https://safetag.org/activities/process_mapping_activity/
- Risk Modeling Using the Pre-Mortem Strategy https://safetag.org/activities/pre_mortum_risk_assessment_activity/
- Creating a Risk Matrix https://safetag.org/activities/risk_matrix/
- Sensitive Data https://safetag.org/activities/sensitive_data/
- Self Doxing https://safetag.org/activities/self_doxing/
- Guiding Questions for High-Risk Organisations https://safetag.org/activities/interviews_highrisk/

- Threat Identification https://safetag.org/activities/threat_identification/
- Threat Interaction https://safetag.org/activities/threat_interaction/
- Regional Context Research https://safetag.org/activities/regional_context_research/
- Assessing Legal Threats https://safetag.org/activities/assessing-legal-threats/

3. Penilaian Aset & Data

3.1 Ringkasan



Setiap organisasi media, apa pun isunya, kemungkinan besar mengelola data sensitif atau pribadi. Namun, data tersebut sering tersebar di berbagai perangkat dengan tingkat keamanan yang berbeda, sehingga berisiko tercecer atau disalahgunakan. Karena itu, penting untuk mengelompokkan data, mengetahui lokasinya, cara penyimpanannya, tingkat keamanannya, tujuan dan pihak yang menerima data, serta siapa saja yang memiliki akses. Semua ini harus terorganisir dengan baik.

Selain aspek penyimpanan, pada tahapan ini auditor juga menilai tanggung jawab organisasi dalam mengelola data, serta risiko kebocoran atau penyalahgunaan yang mungkin terjadi selama proses pengumpulan, pemrosesan, dan penggunaan data.

Tujuan utama dari tahapan ini, yaitu:

- Memetakan data sensitif organisasi — apa, di mana disimpan, bagaimana ditransfer, dan siapa yang memiliki akses. Hal ini penting agar auditor dapat merekomendasikan solusi penyimpanan yang lebih aman sesuai dengan risiko dan alur kerja organisasi.
- Menemukan kerentanan terhadap penyalahgunaan data dan aset.

- Memberikan rekomendasi untuk melindungi data dan aset digital sesuai temuan audit.

3.2 Tahapan

Secara garis besar, tahapan dalam penilaian aset dan data termasuk memahami konsep keamanan data dan informasi, menilai kepatuhan terhadap regulasi, memetakan aset digital, serta mendaftar media sosial dan pengamanannya.

3.2.1 Memahami Keamanan Sistem Informasi

Untuk bisa melakukan audit terkait penilaian aset dan data, seorang auditor perlu memahami konsep keamanan komunikasi dan informasi yang biasa disebut Konsep CIA. Konsep ini terdiri dari tiga pilar utama dalam keamanan sistem informasi, yaitu *confidentiality* (kerahasiaan), *integrity* (keutuhan) dan *availability* (ketersediaan).

- Kerahasiaan berarti data dan informasi tersebut hanya bisa diakses orang yang berhak. Contohnya pesan pribadi di ponsel di mana hanya penerima dan pengirim yang boleh membacanya. Orang lain tidak boleh tahu isinya. Dalam konteks pengamanan situs web media, kerahasiaan ini adalah akses masuk dashboard situs web sehingga hanya pengguna tertentu yang bisa mengaksesnya. Untuk itu perlu ada mekanisme akses tertentu seperti penggunaan nama pengguna dan kata sandi.

  Cara menjaga kerahasiaan adalah dengan menggunakan password, enkripsi data, serta mengontrol akses, seperti siapa boleh mengedit atau melihat data/informasi apa.

- Keutuhan berarti data harus tetap akurat dan tidak berubah tanpa izin. Contohnya jika ada pesan yang diubah, tapi dila-

kukan orang yang tidak memiliki hak untuk itu. Perubahan data perlu untuk dideteksi untuk menghindari perubahan yang tidak diinginkan.

Cara menjaga keutuhan data adalah dengan menggunakan *hashing* (mengecek apakah data berubah) dan menggunakan kontrol versi data. Gunakan data cadangan yang dipakai untuk memulihkan jika terjadi kerusakan data.

- Ketersediaan berarti data harus bisa diakses atau tersedia saat dibutuhkan. Contohnya, saat kita membuka suatu halaman di situs web, maka data di situs web tersebut harus tersedia agar bisa diakses. Jika ternyata peladennya tumbang (*down*), maka saat itu data tidak tersedia.

  Cara menjaga adalah dengan infrastruktur yang baik, cadangan data untuk pemulihan dan proteksi keamanan dari serangan DDoS.

3.2.2 Menilai Kepatuhan terhadap Regulasi

Paling tidak ada dua regulasi yang berpengaruh dalam kegiatan yang dilakukan organisasi media yaitu UU No 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan UU No 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP).

Dalam UU PDP ini mengatur bagaimana data pribadi harus dikumpulkan, digunakan, disimpan, dan dilindungi oleh siapa pun yang memproses data, termasuk organisasi media. Beberapa hal yang perlu diperhatikan terkait UU PDP yaitu:

- **Pengumpulan Data:** Saat media melakukan wawancara, survei, atau investigasi, sering kali mereka mengumpulkan data pribadi

(nama, kontak, opini, dll). UU PDP mewajibkan persetujuan eksplisit dari subjek data sebelum data dikumpulkan atau dipublikasikan.

- **Penggunaan dan Penyimpanan:** Data digital yang dikumpulkan harus disimpan secara aman. Organisasi media wajib menjamin tidak ada kebocoran atau penyalahgunaan, termasuk dari pihak ketiga.

- **Hak Subjek Data:** Orang yang datanya dikumpulkan berhak mengetahui, mengakses, membetulkan, bahkan meminta penghapusan data mereka. Ini memengaruhi bagaimana media menyusun kebijakan pengelolaan data.

- **Kategori Data Sensitif:** Data seperti latar belakang politik, kesehatan, agama, atau orientasi seksual dianggap sangat sensitif. Media harus sangat berhati-hati jika ingin mengungkapkannya.

UU KIP ini menjamin hak publik untuk mengakses informasi yang dikuasai badan publik, termasuk organisasi media milik pemerintah atau yang mendapat dana publik.

Beberapa hal yang perlu diperhatikan terkait UU KIP yaitu:

- **Kewajiban Transparansi:** Jika organisasi media menerima dana dari APBN/APBD atau merupakan bagian dari lembaga publik, mereka wajib membuka informasi tertentu ke publik (seperti laporan keuangan, program kerja, atau struktur organisasi).

- **Batasan Informasi yang Dikecualikan:** Meski harus terbuka, ada informasi yang dikecualikan (misalnya yang menyangkut keamanan negara atau data pribadi). Di sinilah media harus menyeimbangkan antara keterbukaan dan perlindungan data pribadi.

- **Peran Ganda Media:** Media juga bertugas mengawasi keterbukaan informasi badan publik lain. Dalam konteks ini, mereka menjadi pengguna UU KIP sekaligus bisa jadi subjeknya.

Aspek-aspek yang perlu diperhatikan media terkait kepatuhan terhadap regulasi yang relevan dengan pengelolaan data dan informasi bisa dilihat pada tabel di bawah.

Pada saat media berupaya memenuhi kewajiban terhadap dua regulasi tersebut, auditor dapat memeriksa kerentanan pada pemanfaatan teknologinya pada beberapa aspek seperti:

Tabel 4: Aspek yang perlu diperhatikan media terkait kepatuhan terhadap regulasi

Aspek	Penyesuaian
Privasi vs Transparansi	Menjaga data pribadi narasumber, tetapi tetap mendorong transparansi publik
Etika Jurnalistik	Memastikan peliputan tidak melanggar UU PDP, terutama saat mengungkap identitas individu
Pengelolaan Data Internal	Menerapkan kontrol akses, enkripsi, dan SOP penghapusan data
Penerapan Hak Subjek Data	Siap menghadapi permintaan klarifikasi, koreksi, atau penghapusan data

- Menyediakan dan Memberikan Informasi: Badan publik wajib menyediakan, memberikan, dan/atau menerbitkan informasi yang berada di bawah kewenangannya kepada pemohon informasi, kecuali informasi yang dikecualikan sesuai ketentuan.
- Membangun Sistem Informasi dan Dokumentasi: Badan publik membangun dan mengembangkan sistem untuk mengelola informasi secara baik dan efisien sehingga mudah diakses.

- Mengumumkan Informasi Berkala: Badan publik wajib mengumumkan informasi secara berkala paling singkat enam bulan sekali, dalam bentuk yang mudah dijangkau dan dipahami masyarakat.

Beberapa aspek di atas apabila memanfaatkan teknologi digital seperti tertaut dengan portal media, penting diaudit agar tidak menambah kerentanan media.

3.2.3 Memetakan Aset Digital

Aset digital adalah segala bentuk informasi atau konten yang disimpan dalam format digital dan memiliki nilai bagi individu, organisasi, atau sistem. Secara sederhana aset digital bisa diartikan barang berharga dalam bentuk digital, bisa berupa file, data, akun, atau sistem.

Contoh aset digital:

- **Dokumen penting:** laporan keuangan, kontrak, proposal
- **Basis data:** data anggota, donatur, klien, atau penerima manfaat
- **Konten media:** foto, video, desain, materi kampanye
- **Akun dan kredensial:** email organisasi, akun media sosial, akun layanan cloud
- **Perangkat lunak & sistem:** website, CMS, aplikasi internal
- **Perangkat keras:** komputer (meja atau bergerak), router, kamera, NAS, peladen.

Data Sensitif dan Privat

Seiring waktu, data dan metadata organisasi media, termasuk milik anggotanya, bisa menjadi sulit dikelola. Hal ini terutama jika staf menggunakan layanan pihak ketiga seperti Google Drive, OneDrive, atau Dropbox. Penggunaan layanan ini merupakan hal wajar, tapi penting

untuk mencatat secara jelas di mana data disimpan dan siapa saja yang memiliki akses.

Pengaturan dan peninjauan hak akses harus dilakukan secara berkala, baik pada layanan pihak ketiga maupun platform yang dikelola langsung oleh organisasi, seperti situs web atau *Network Attached Storage* (NAS). Pengelolaan hak akses yang baik memungkinkan pembatasan akses yang tepat untuk mencegah data diakses oleh pihak yang tidak berwenang.

Daftar Pertanyaan:

- Data apa yang dianggap penting dan harus tersedia secara publik?
- Apakah ada pencadangannya (*back up*) pada data tersebut?
- Apa saja data yang dianggap privat atau rahasia organisasi?
- Bagaimana lembaga menentukan siapa yang bisa mengakses data tersebut?
- Adakah orang yang tidak punya wewenang untuk mengakses data tersebut, tetapi bisa mengaksesnya?
- Apakah staf sudah punya kriteria apa yang termasuk dalam data sensitif?
- Data apa saja yang bisa diakses staf untuk melakukan pekerjaannya?
- Dari mana data tersebut berasal?
- Apa yang Anda lakukan terhadap data yang tidak diperlukan atau digunakan?

Risiko Penyalahgunaan Data

Organisasi media perlu mengidentifikasi risiko dan dampak jika ada data organisasi yang hilang atau bocor. Langkah ini dilakukan untuk memastikan organisasi memahami cara mengelola data. Langkah pertama adalah memetakan seluruh data yang dimiliki, lalu meng-

klasifikasikannya berdasarkan tingkat kepentingan atau sensitivitasnya.

Organisasi media juga perlu merefleksikan potensi risiko, seperti: apa akibatnya jika data hilang atau disalahgunakan? Berapa besar upaya yang telah dilakukan untuk mengumpulkan data tersebut? Jika rusak atau hilang, apakah data masih bisa dipulihkan, dan berapa besar sumber daya (waktu, tenaga, biaya) yang dibutuhkan untuk pemulihannya?

Saat tahapan ini dilakukan, auditor biasanya menemui penggunaan layanan pihak ketiga. Organisasi sangat mungkin menyimpan data atau bergantung terhadap layanan tersebut. Perlu pengecekan juga tentang Syarat dan Ketentuan serta Kebijakan Privasi layanan tersebut, sebagai bahan identifikasi risiko pada organisasi. Di berbagai organisasi penggunaan atau kebergantungan terhadap platform atau layanan pihak ketiga sering terjadi. Selain kebijakan terkait, perlu juga melihat rekam jejak bagaimana layanan tersebut merespon jika ada insiden keamanan atau kebijakan privasi mereka.

Beberapa langkah yang bisa dilakukan dalam mengidentifikasi risiko:

- Identifikasi data apa saja yang dikumpulkan oleh organisasi
- Mengelompokkan data yang terkumpul berdasar tempat penyimpanannya. Tempat ini bisa berupa ruang fisik maupun digital. Misalnya, catatan pada buku yang tersimpan di suatu tempat, maupun informasi data pribadi dalam fail/dokumen di penyimpanan awan atau perangkat penyimpanan seperti flashdisk.
- Klasifikasikan informasi yang terkandung dalam data tersebut. Apakah isinya memuat hal sensitif, pribadi, atau privat? Sensitivitas kepentingan data ini bisa dibagi menjadi tiga kelompok: tinggi, sedang, dan rendah.
- Pikirkan konsekuensi dan kemungkinan penyalahgunaan yang mungkin muncul.

3.2.4 Mendaftar Media Sosial & Pengelolaannya

Informasi kredensial media sosial dan website juga menjadi data sensitif bagi organisasi media, apalagi jika media tersebut mempunyai kanal media sosial yang juga dikelola dengan baik. Untuk itu perlu adanya pengelolaan yang baik pula terhadap aset digital yang dimiliki organisasi termasuk di dalamnya aset media sosial.

Langkah yang perlu dilakukan dalam tahap ini yaitu auditor perlu mendapatkan hasil pemetaan media sosial apa saja yang dimiliki oleh organisasi dan bagaimana mereka mengelolanya, terutama dalam keamanannya.

Berikut tabel yang bisa digunakan sebagai informasi daftar media sosial yang digunakan organisasi:

Tabel 5: Daftar media sosial yang dikelola media

No	Platform	Akun	Tautan	Pengikut / Pelanggan	Pengamanan

Daftar Pertanyaan :

- Apa saja akun media sosial yang dimiliki?
- Apa media sosial yang paling aktif diukur dari jumlah pengikut atau pelanggan serta intensitas unggahannya?
- Bagaimana pengamanan masing-masing akun tersebut dinilai

dari, antara lain, kekuatan kata sandi dan penggunaan 2FA atau bahkan MFA?
- Siapa saja yang punya akses terhadap media sosial?
- Siapa saja yang memiliki informasi login media sosial?
- Bagaimana media sosial tersebut dijalankan/dikelola? Apakah menggunakan perangkat khusus? Berapa banyak admin?
- Bagaimana pengelolaan kredensial login media sosial organisasi?
- Tantangan apa yang sering terjadi dalam pengelolaan media sosial?
- Apakah admin sudah memahami cara memulihkan akun media sosial secara mandiri?

3.3 Catatan

Metode penilaian aset dan data bisa dilakukan dalam tiga bentuk, yaitu wawancara, observasi jarak jauh, atau pengisian tabel. Wawancara dilakukan secara langsung terhadap penanggung jawab media sosial auditi, termasuk menanyakan pengamanannya. Observasi bisa dilakukan secara jarak jauh, tetapi tetap perlu menanyakan ke auditi terkait pengamanannya. Adapun pengisian tabel bisa dilakukan sendiri oleh auditi.

Data hasil penilaian harus ditangani dengan sangat aman. Termasuk memastikan transfer data menggunakan saluran terenkripsi dan menjaga privasi informasi selama proses berlangsung.

3.4 Keluaran

Hasil dari penilaian ini biasanya mencakup:

- Pemetaan lengkap aset digital termasuk di mana berada, siapa yang mengaksesnya dan menyimpan, layanan pihak ketiga yang digunakan.

- Penilaian sensitivitas dan identifikasi risiko jika terjadi kehilangan atau akses oleh pihak yang tidak berwenang.
- Rekomendasi mitigasi berupa sistem penyimpanan aman, pengelolaan hak akses, data dan media sosial atau kebijakan pencadangan data.

3.5 Acuan

- Contoh tabel Penilaian Aset Digital
- Risk of Data Lost and Found https://safetag.org/activities/data_lost_and_found/
- Assessing Usage of Cloud Services https://safetag.org/activities/cloud_services/
- The Impacts of a Lost Device https://safetag.org/activities/impact_lost_device/
- The Impacts of a “Found” Device https://safetag.org/activities/impact_found_device/



4. Pemetaan Infrastruktur & Jaringan

4.1 Ringkasan

Setelah memetakan dan menilai aset data, proses berikutnya adalah memetakan infrastruktur dan jaringan digital. Infrastruktur ini adalah fondasi yang menentukan bagaimana organisasi media mengakses, mengirim, dan menyimpan data, sehingga melindunginya adalah sebuah keharusan.

Untuk memahaminya, kita dapat menggunakan analogi sebuah bangunan. Sebelum mengamankan bangunan, kita perlu tahu aset berharga apa saja yang terdapat di dalamnya. Sama halnya juga dengan data atau informasi organisasi. Selanjutnya, kita harus memahami arsitektur bangunan tersebut dari tata letak sampai strukturnya, yang dalam konteks digital berarti memahami arsitektur yang berupa perangkat keras dan perangkat lunak yang digunakan dalam kerja-kerja digital organisasi.

Langkah terpenting kemudian adalah memetakan semua akses seperti titik masuk dan keluar pada bangunan itu, seperti pintu, jendela, dan gerbang, yang setara dengan peladen (*server*), aplikasi pendukung web, *port* jaringan, dan titik akses lainnya pada infrastruktur digital.

Kemudian, untuk dapat memeriksa apakah terdapat celah pada akses

masuk infrastruktur digital ini, pemindaian yang meliputi dari situs web dan jaringan baik eksternal seperti, layanan/aplikasi web pendukung, layanan surel, DNS, maupun jaringan internal seperti Wi-Fi perlu dilakukan.

Setelah memetakan infrastruktur dan asetnya, kita akan memeriksa apakah terdapat celah atau kerentanan. Melalui semua proses tersebut, auditor dapat menilai apakah penerapan keamanan infrastruktur saat ini cukup melindungi organisasi atau tidak.

4.2 Tahapan

4.2.1 Observasi Infrastruktur



Memastikan keamanan infrastruktur bisa diawali dengan mengenali kondisi jaringan, aplikasi, layanan pihak ketiga yang digunakan media. Selain itu, perlu juga melakukan pendataan aset digital, melengkapi tahapan pada bagian sebelumnya, yang dimiliki organisasi, utamanya terkait perangkat.

Dengan mengenali perangkat apa saja yang terhubung dalam jaringan internal. Kemudian, mengidentifikasi layanan organisasi apa saja yang bisa diakses dengan atau tanpa jaringan internal. Kemudian, melihat bagaimana kondisi pengaturan keamanan perangkat atau layanan terkait. Bisa menjadi tolok ukur untuk melakukan pemetaan dan pemindaian kerentanan lebih lanjut.

Umumnya, beberapa perangkat jaringan yang terdapat dalam suatu organisasi seperti:

- *Router*
- *Network printer*
- *Access point Wi-Fi*

- *NAS (LAN file storage/file sharing)*
- *Network projector* (yang tersambung melalui Wi-Fi)
- *Modem broadband*
- *Smart TV*
- Mikrotik
- Jaringan internet yang terhubung dalam domain.

Perangkat selain jaringan yang mungkin menyimpan data sensitif, termasuk:

- Perangkat desktop, laptop, dan mobile
- Kamera
- Mesin fotokopi (mungkin memilik diska penyimpanan).

Lalu, terkait perangkat lunak yang digunakan dapat berupa:

- Layanan produktivitas atau kolaborasi seperti Google Workspace, Microsoft, atau yang lainnya
- Aplikasi komunikasi (WhatsApp, Signal, dsb.)
- Aplikasi pengolah dokumen
- Situs web
- Layanan surel (termasuk layanan email pihak ketiga).

Pemilihan perangkat keras dan lunak sangat memengaruhi cara kerja organisasi media. Penting untuk memahami keuntungan dan kerugian dari setiap pilihan, seperti menggunakan aplikasi berbayar versus sumber terbuka (*open-source*), memilih produk dari negara tertentu, atau menggunakan layanan *big tech*.

Saat mempertimbangkan perangkat atau layanan pihak ketiga, setidaknya ada tiga faktor utama yang perlu dievaluasi. Kebijakan (layanan dan privasi), kepatuhan terhadap standar industri, dan rekam jejak penyedia layanan. Menganalisis ketiga faktor ini akan membantu memetakan potensi ancaman dengan lebih jelas. Sebagai contoh, saat memilih aplikasi

komunikasi pesan ringkas untuk grup antara Signal dan WhatsApp, Signal jelas lebih unggul jika prioritas utamanya adalah privasi pengguna. Begitu juga dengan pilihan layanan surel, apakah terdapat fitur enkripsi secara bawaan atau tidak serta layanan yang digunakan apakah memiliki kebijakan privasi yang menghargai pengguna.

Setelah itu, pendataan aset infrastruktur IT adalah langkah lanjutan yang cukup penting bagi organisasi media. Mengingat data dan informasi penting diakses melalui jaringan internal atau eksternal, perlindungan aset digital harus dimulai dari langkah dasar: mengidentifikasi dan memetakan semua perangkat keras yang dapat mengakses atau terhubung ke dalam infrastruktur tersebut. Tanpa inventarisasi yang jelas, sulit untuk melindungi dan mengelola aset digital secara efektif.

Umumnya, pendataan atau inventarisasi aset sebaiknya mencakup beberapa hal berikut.

- **Nama Aset/Nama Perangkat:** Deskripsi yang jelas (misalnya, "Laptop Merk P Model QR," "Printer X model ABC").
- **Pengguna aset:** Nama staf yang saat ini menggunakan aset tersebut.
- **Lokasi:** Lokasi fisik aset (misalnya, "Kantor," "Kerja Jarak Jauh - Rumah [Nama Staf]").
- **Pengamanan:** Metode pengamanan yang digunakan. Misalnya, kata sandi kuat dan 2FA.
- **Spesifikasi:** Detail teknis utama (misalnya, CPU, RAM, ukuran Penyimpanan, nomor model).
- **Tanggal Pembelian:** Kapan aset tersebut dibeli.

4.2.2 Pemindaian Situs Web

Pada tahap ini auditor mencari kemungkinan celah keamanan dalam perangkat, layanan, aplikasi, dan jaringan organisasi dengan menguji

dan membandingkannya dengan berbagai sumber (pangkalan data kerentanan, informasi vendor/layanan, dan investigasi/temuan audit).

Dalam melakukan pemindaian kerentanan, perlu kita bedakan mengenai asesmen kerentanan dan uji penetrasi. Asesmen kerentanan lebih bersifat menyeluruh, sedangkan uji penetrasi lebih mendalam. Kedua hal tersebut juga memiliki tujuan berbeda. Asesmen kerentanan bertujuan untuk melihat sejauh mana kerentanan dapat muncul atau potensial bersarang pada suatu sistem organisasi. Di sisi lain, Uji Penetrasi lebih berfungsi untuk memverifikasi suatu kerentanan dan memiliki tujuan yang spesifik.

Dalam proses pemindaian kerentanan, penggunaan aplikasi non-teknis dapat dimanfaatkan, tetapi penggunaan aplikasi harus didasarkan pada pemahaman tentang batasan, lingkup, dan konsekuensi dari pemindaian oleh aplikasi atau layanan pihak ketiga terkait, terutama jika berbasis web. Sebagai contoh, penggunaan aplikasi layanan pihak ketiga tidak dapat memindai sedalam dan sejauh aplikasi teknis khusus. Penggunaannya hanya sebatas memindai pada permukaannya saja. Untuk mendapatkan pemindaian yang lebih komprehensif, perlu menggunakan aplikasi khusus, seperti Burp Suite, Nessus, Nuclei atau beberapa aplikasi alternatif lainnya. Namun, penggunaan aplikasi tersebut memerlukan kapasitas pemahaman dan keahlian teknis yang lebih mendalam.

Menyigi Situs Web

Menyigi situs web (*website footprinting*) merupakan sebuah proses menelusuri dan menemukan segala sesuatu mengenai suatu situs web atau domain, termasuk informasi berupa peladennya, teknologi yang digunakan, dan data lainnya yang mungkin berguna bagi penyerang. Kata *footprinting* sendiri mengacu pada istilah teknis dalam dunia komputer terkait proses untuk memperoleh informasi mengenai suatu sistem atau jaringan.

Penggunaan alat pindai layanan pihak ketiga sebagai langkah awal dapat dilakukan untuk mengumpulkan informasi mengenai suatu situs web, yang kemudian berguna untuk memulai Pemindaian Kerentanan. Untuk memetakan infrastruktur sebuah domain, seperti peladen e-mail, detail peladen, dan layanan terkait lainnya, dapat menggunakan tools seperti DNSDumpster, Censys, atau SecurityTrails. Sementara itu, untuk mengidentifikasi teknologi dan aplikasi spesifik yang digunakan sebuah situs web, dapat menggunakan Wappalyzer atau BuiltWith.

Beberapa rekomendasi layanan berbasis web untuk menunjang praktik ini tercantum di bawah. Untuk opsi yang lebih luas, silakan mengacu pada lampiran.

- Wappalyzer: https://www.wappalyzer.com/
- DNSDumpster: https://dnsdumpster.com/

Data yang dikumpulkan menjadi modal utama sebagai informasi untuk menyesuaikan langkah selanjutnya. Misalnya, penggunaan situs web berbasis WordPress perlu menyesuaikan alat pemindai yang digunakan menjadi WPScan atau WPSec. Kemudian situs web secara *custom* atau tidak memanfaatkan CMS populer, perlu melakukan pemindaian dari sisi aplikasi web dan API-nya (*Application Programming Interface*). Selain itu, informasi terkait layanan atau aplikasi apa saja yang termuat dalam peladen, seperti, email, web panel, bisa menjadi catatan untuk melakukan pemindaian lebih lanjut.

Pemeriksaan melalui layanan pihak ketiga berikut dapat membantu tahapan proses ini.

- Mengidentifikasi Target dengan menentukan domain atau situs web yang akan diuji.
- Menggunakan BuiltWith atau Wappalyzer untuk mengenali teknologi pendukung aplikasi web yang digunakan.

- Menggunakan DNSDumpster atau SecurityTrails untuk memetakan infrastrukturnya.

Pemindaian Kerentanan

Pemindaian situs web dilakukan untuk melihat postur keamanan situs web beserta aplikasi pendukungnya. Selain itu, pengecekan terhadap temuan kerentanan perlu untuk memastikan situs web tidak terinfeksi dan bukan merupakan suatu *false positive*.

Beberapa aplikasi atau layanan yang dapat digunakan untuk memindai kerentanan, sebagai berikut.

- WPScan: https://wpscan.com/
- WPSec: https://wpsec.com/
- Sucuri SiteCheck: https://sitecheck.sucuri.net/
- UpGuard Web Scan: https://webscan.upguard.com/
- SSLabs Test https://www.ssllabs.com/ssltest/.
- Zed Attack Proxy (ZAP), Nessus, atau Burp Suite
- Daftar aplikasi pemindai kerentanan OWASP: https://owasp.org/www-community/Vulnerability_Scanning_Tools

Beberapa aspek pertanyaan yang bisa dipertimbangkan dalam menilai keamanan situs web adalah:

Tabel 6: Aspek untuk menilai keamanan sebuah situs web

No.	Pertanyaan	Jawaban (Ya/Tidak)	Catatan/Temuan
1	Apakah situs-situs web organisasi telah mengimplementasikan protokol HTTPS (TLS/SSL) dengan baik?		
2	Apakah situs web terdaftar pada daftar hitam?		
3	Apakah hasil pemindaian menunjukan kerentanan?		
4	Apakah kondisi pengamanan infrastruktur surel organisasi telah menerapkan praktik terbaik?		
5	Apakah situs web beserta aplikasi pendukungnya rutin diperbarui?		

Pemindaian melalui layanan pihak ketiga berikut bisa membantu beberapa tahapan proses ini.

- Menggunakan WPSec atau WPScan (jika relevan) untuk memindai kerentanan website yang berbasis pada WordPress.
- Menggunakan Sucuri SiteCheck untuk melakukan pemindaian situs web dan memeriksa daftar hitam.
- Menggunakan SSLabs untuk memeriksa pengaturan SSL/TLS.
- Menggunakan UpGuard Web mencari kerentanan.
- Jika memiliki kemampuan lebih teknis lakukan *penetration test* dan verifikasi kerentanan.
- Membuat laporan berdasarkan temuan dari pengujian sebelumnya.

4.2.3 Pemetaan Jaringan (Wi-Fi)

Penggunaan jaringan internal dalam kantor biasanya digunakan untuk mengakses dan mengelola internet atau intranet, printer, kamera pengawas, dan NAS. Router atau modem yang berasal dari penyedia layanan internet (ISP) biasanya merupakan pusat perangkat utama yang mengkoordinir semua perangkat yang terhubung dalam jaringan. Dengan demikian, mengamankan gerbang utama ini (modem) merupakan suatu keharusan. Memastikan pengaturan bawaan sudah diubah, meliputi, tetapi tidak terbatas pada penggunaan akun bawaan, pengaturan *firewall*, pemisahan jaringan menjadi langkah yang perlu dipenuhi. Jika tidak demikian, besar kemungkinan akan menyebabkan dan mengekspos segala perangkat yang terhubung dalam suatu jaringan sehingga menjadi lebih rentan.

Untuk memudahkan pemetaan jaringan dan infrastruktur sebuah media, daftar periksa berikut bisa membantu.

Tabel 7: Daftar periksa pemetaan infrastruktur dan jaringan sebuah media

Komponen	Temuan	Kegiatan
Perangkat komputer atau Laptop	Amati penggunaan sistem operasi dan aplikasi perangkat staf, orisinal atau tidak? Bagaimana kondisi perangkat? Tempatnya di mana? Pada saat jam kerja berakhir apakah perangkat dibawa pulang atau ditinggal?	Pengamatan
	Amati bagaimana para staf menjaga perangkatnya. Apakah ditinggal begitu saja saat ditinggalkan atau dikunci? Apa saja pengamanannya?	Pengamatan

Sistem Operasi	Amati atau tanya sistem Operasi apa saja yang digunakan oleh staf. Apakah sistem operasinya berlisensi sah atau tidak?	Pengamatan/Pengecekan Perangkat
Wi-Fi Kantor	Apakah nama SSID dan kata sandinya diberitahukan secara terbuka atau tidak. Misalnya, di dinding atau ditulis di papan?	Pengamatan
	Jika nama SSID dan kata sandi tidak terbuka, mintalah kepada staf di kantor tersebut.	Meminta akses
	Cari informasi apa layanan jasa Internet yang digunakan lewat platform speedtest.net, fast.com, atau whoer.net.	Pengujian dengan platform
	Setelah menemukan layanan jasa internet yang digunakan, lakukan percobaan masuk pada router sebagai admin Wi-Fi tersebut. Gunakan nama pengguna dan kata sandi bawaan (default), yang biasanya tersedia secara luas di mesin pencari. Jika masih terdapat penggunaan akun bawaan catat sebagai temuan.	Pengujian dengan percobaan akses.
	Jika bisa masuk sebagai admin Wi-Fi kantor mitra, catat sebagai temuan penting karena risikonya sangat tinggi.	Pengujian dengan mengakses dasbor router
	Ambil gambar untuk semua temuan, seperti nama SSID dan kata sandi yang ditempel, posisi jeroan admin Wi-Fi lembaga, dan informasi lain-lain yang relevan.	Dokumentasi

	Tanyakan informasi pendukung lain, termasuk kapan kata sandi diganti terakhir kali, bagaimana pengaturan SSID-nya, apakah ada admin yang memantau penggunaannya, dst.	Wawancara & Pengamatan
Local Area Network (LAN)	Tanyakan apakah kantor memakai LAN atau tidak. Jika memakai, siapa saja yang bisa mengakses? Apakah tamu bisa langsung mengakesnya juga?	Wawancara & Pengamatan
Router	Tanyakan di mana letak *router*. Perhatikan apakah bisa diakses orang lain dengan mudah atau tidak.	Wawancara & Pengamatan
Media Penyimpanan	Apakah lembaga memiliki media penyimpanan terpusat, seperti server atau NAS? Jika punya, di mana posisinya? Siapa saja yang bisa mengakses ruangan ataupun jaringannya, lokal atau bisa dari jarak jauh?	Wawancara & Pengamatan
Jaringan	Jika menggunakan pihak ketiga untuk mengatur WIFI, LAN, NAS, dsb, siapa pihak ketiga tersebut? Bagaimana statusnya (konsultan atau seperti apa?) Apa latar belakang pihak ketiga tersebut? Adakah narahubung dari staf kantor untuk transfer informasi atau pengetahuan dari konsultan?	Wawancara
Perangkat terhubung	Melakukan pemindaan dengan aplikasi atau melalui dasbor router untuk memastikan perangkat terhubung dikenali.	Pengujian dengan aplikasi Fing atau Nmap

Kamera Pengawas	Perhatikan apakah kantor memiliki kamera pengawas (CCTV)? Berapa? Bagaimana penempatannya?	Pengamatan
Keamanan Fisik Lain	Ada beberapa hal lain yang juga perlu diperhatikan. Meskipun bukan termasuk keamanan digital, tetapi aspek-aspek berikut berpengaruh juga pada keamanan digital, yaitu lingkungan sekitar, pagar kantor, pengaturan ruangan, penanggung jawab keamanan, posisi duduk, dan lain-lain.	

Tahapan yang dapat dilakukan sebagai acuan pada bagian ini adalah:

- Memeriksa apakah terdapat pembagian dan pemisah jaringan antara pengguna internal dan eksternal.
- Mengidentifikasi penyedia jasa internet yang digunakan beserta merk dan model router.
- Memeriksa penggunaan akun bawan router, dengan mencari informasi dari mesin pencari atau https://www.routerpasswords.com/.
- Mengidentifikasi perangkat yang terhubung dari Router atau aplikasi Fing.

Daftar pertanyaan yang bisa diajukan untuk mengetahui keamanan Wi-Fi bisa dilihat dalam tabel di bawah.

Tabel 8: Daftar pertanyaan untuk memeriksa keamanan Wi-Fi

No.	Pertanyaan	Ya/Tidak	Catatan/ Temuan
1	Apakah tahu cara mengakses halaman admin router?		
2	Apakah masih memakai kredensial bawaan atau *default*?		
3	Siapa yang bisa mengakses halaman admin dari router?		
4	Apakah menggunakan Mikrotik atau perangkat pengatur layanan jaringan?		
5	Apakah ada layanan yang tersedia dalam jaringan yang tidak diberi tahu oleh staf organisasi?		
6	Apa sistem operasi, atau layanan/aplikasi yang digunakan organisasi? Apakah ada hal tidak umum, berbeda, atau belum diperbarui mengenai layanan atau sistem operasi yang dijalankan?		
7	Apakah semua perangkat jaringan dan non-jaringan telah diperbarui ke versi terbaru?		
8	Apakah ada kebijakan penggunaan password yang kuat dan diterapkan secara konsisten?		
9	Apakah ada firewall yang melindungi jaringan dari akses yang tidak sah?		
10	Apakah ada backup data yang dilakukan secara teratur?		
11	Apakah karyawan diberi pelatihan keamanan secara cukup?		
12	Apakah ada kebijakan penggunaan yang jelas untuk perangkat pribadi yang terhubung ke jaringan organisasi?		

4.3 Catatan

Pemetaan jaringan dan infrastruktur sebuah media memerlukan adanya kunjungan langsung ke kantor media tersebut. Oleh karena itu, observasi menjadi faktor penting untuk mendapatkan hasil pemetaan secara lebih akurat.

Selama observasi tersebut, auditor juga perlu memetakan dan menganalisis keamanan fisik kantor, termasuk lingkungan kantor, kamera pengawas, pengaturan tempat kerja, hingga penempatan router.

4.4 Keluaran



Berdasarkan penilaian ini hasil yang akan didapatkan adalah sebagai berikut:

- Data hasil pemindaan domain beserta dengan subdomain-nya dan Informasi DNS
- Informasi penggunaan layanan web dan pengamanan surel
- Data hasil pemindaan kerentanan pada aplikasi web
- Data hasil pengecekan Penguji Sertifikat TLS

4.5 Acuan

- Network Scanning https://safetag.org/activities/network_scanning
- Network Access https://safetag.org/activities/network_access
- Network Traffic Analysis https://safetag.org/activities/traffic_analysis
- Remote Network and User Device Assessment https://safetag.org/activities/remote_network_device_assessment
- Router Based Attacks https://safetag.org/activities/router_attacks

- VoIP Security Assessment https://safetag.org/activities/voip_assessment
- Wireless Range Mapping https://safetag.org/activities/wireless_range_mapping
- Monitor Open Wireless Traffic https://safetag.org/activities/monitor_open_wireless_traffic
- Vulnerability Scanning https://safetag.org/activities/vulnerability_scanning/
- Vulnerability Research https://safetag.org/activities/vulnerability_research/
- Website Footprinting https://safetag.org/activities/web_footprint/
- Web Vulnerability Assessment https://safetag.org/activities/web_vulnerability_assessment/
- VoIP Security Assessment https://safetag.org/activities/voip_assessment/
- Check Config Files https://safetag.org/activities/check_config_files/
- Router Based Attacks https://safetag.org/activities/router_attacks/

BAGIAN B

PELAPORAN



5. Penyusunan Laporan

5.1 Ringkasan

Tahap akhir dari proses audit adalah penyusunan laporan. Setelah seluruh informasi terkumpul—terkait tujuan audit, lingkup kerja, kapasitas organisasi, serta hasil identifikasi risiko, ancaman, pengelolaan data, aset, jaringan, dan kebijakan—auditor menyusun rekomendasi berdasarkan temuan-temuan tersebut. Laporan harus disusun secara akurat, jelas, dan konstruktif.

Bentuk laporan yang umum adalah daftar temuan disertai rekomendasi perbaikan. Waktu yang dibutuhkan untuk perbaikan bervariasi. Jika dalam rencana audit awal telah dirancang pemeriksaan ulang (re-audit), maka waktu pelaksanaannya harus mempertimbangkan estimasi durasi perbaikan tersebut.

Penulisan laporan perlu memerhatikan target audiens, agar mudah dipahami. Karena pembaca laporan disampaikan pada pihak manajemen organisasi yang bisa berasal dari latar belakang non-teknis, maka hindari istilah teknis yang sulit untuk dijelaskan. Jika istilah teknis harus digunakan, sertakan penjelasan singkatnya.

Inti laporan adalah agar pesan auditor tersampaikan dengan baik, serta rekomendasi dapat diterapkan oleh organisasi. Bahasa dan gaya penulisan disesuaikan dengan kebutuhan organisasi—beberapa mungkin menginginkan laporan yang mendalam, sementara lainnya hanya memerlukan ringkasan eksekutif.

Organisasi juga harus memahami bahwa menjaga keamanan digital organisasi perlu dilakukan secara terus menerus karena merupakan proses berkelanjutan. Perubahan perangkat keras, perangkat lunak, serta taktik serangan akan terus muncul, sehingga audit keamanan idealnya dilakukan secara berkala, minimal setahun sekali, sebagai bagian dari manajemen keamanan IT.

Secara umum, laporan berisi rangkuman seluruh kegiatan audit. Namun, jika terdapat aspek teknis dalam proses audit, seperti hasil pemindaian kerentanan, maka lampiran teknis perlu disertakan. Lampiran ini dapat mencakup data dari alat asesmen, seperti jenis dan lokasi kerentanan pada situs web atau jaringan organisasi.

5.2 Tahapan

Pada prinsipnya, penyusunan laporan terdiri dari dua tahapan, yaitu penulisan dan penyampaian laporan. Penulisan laporan dilakukan berdasarkan semua temuan audit yang dibuat secara terstruktur agar memudahkan auditi untuk mendapatkan informasi penting terkait substansi audit. Adapun penyampaian laporan dilakukan agar auditi bisa mendapatkan informasi secara langsung dengan auditor sekaligus membuaka ruang untuk diskusi selama penyampaian tersebut.

5.2.1 Penyusunan Laporan

Secara garis besar, substansi laporan audit terdiri dari penjelasan tentang audit, profil organisasi, temuan, dan rekomendasi. Kerangka laporan dari tiap bagian tersebut bisa dilihat pada struktur berikut:

1. Halaman Depan

- Nama Organisasi
- Judul Laporan Audit

- Waktu Audit (bulan dan tahun)
- Nama Auditor

2. Pengantar

- Latar Belakang
- Tujuan Audit
- Ruang Lingkup Audit
- Metodologi

3. Profil Organisasi

- Deskripsi singkat organisasi
- Struktur teknis dasar (jika relevan)
- Kapasitas tim internal

4. Temuan

- Risiko & Ancaman
- Kapasitas
- Aset Digital
- Jaringan & Infrastruktur

5. Rekomendasi

- Kebijakan
- Pengelolaan Data & Aset Digital
- Jaringan & Infrastrukur

6. Penutup

7. Lampiran Teknis

5.2.2 Penyampaian Laporan

Penyampaian laporan melalui pemaparan dapat dilakukan sebagai langkah terakhir setelah penyampaian laporan audit secara tertulis. Tahapan ini biasanya dilakukan secara jarak jauh karena kemudahan waktunya. Penyampaian laporan ini sebaiknya dihadiri oleh manajemen organisasi yang bisa mengambil keputusan terkait hasil audit, terutama terkait dengan rekomendasi.

Pertemuan ini memaparkan atau memberikan informasi relevan mengenai serangkaian langkah apa saja yang telah dilalui dalam proses audit, temuan-temuan yang ada dan juga rekomendasi yang sudah dituliskan auditor.

Tahap ini merupakan waktu yang tepat bagi organisasi yang diaudit untuk menanyakan segala hal terkait keseluruhan rangkaian proses audit ataupun hal lain yang memerlukan tindak lanjut. Untuk itu sebaiknya laporan tertulis sudah lebih dulu dibaca oleh pihak manajemen organisasi.

5.3 Catatan

Menyusun rekomendasi dari temuan audit adalah tahap krusial yang menentukan apakah hasil audit akan benar-benar bermanfaat bagi organisasi. Rekomendasi harus bisa ditindaklanjuti, dipahami, dan disesuaikan dengan kapasitas organisasi.

Beberapa hal yang perlu diperhatikan dalam menyusun rekomendasi:

- Tautkan rekomendasi dengan hasil temuan
- Buatlah rekomendasi yang sifatnya spesifik, bukan umum
- Sesuaikan dengan kapasitas organisasi yang diaudit (pertimbangkan ketersediaan SDM teknis, tingkat pemahaman terhadap IT dan pendanaan)

- Buat skala prioritas berdasarkan risiko (prioritas tinggi, sedang dan rendah)
- Tambahkan juga estimasi jangka waktu (jangka waktu panjang, menengah atau jangka pendek)

5.4 Keluaran

- Laporan audit secara tertulis berikut rekomendasinya
- Penjadwalan penyampaian laporan dan diskusi hasil audit

5.5 Acuan

- Template Laporan Audit
- Roadmap Development https://safetag.org/activities/roadmap_development/
- Resource Identification https://safetag.org/activities/identify_useful_resources/
- Report Creation https://safetag.org/activities/report_creation/

Daftar Istilah

2FA	Autentikasi dua langkah. Metode keamanan yang memerlukan dua bentuk verifikasi berbeda (misalnya, sandi + kode SMS) untuk mengakses akun.
Asesmen Kerentanan	Proses sistematis untuk mengidentifikasi, mengukur, dan memprioritaskan kelemahan keamanan dalam sistem, jaringan, atau aplikasi.
Auditi	Pihak, organisasi, sistem, atau proses yang sedang menjalani pemeriksaan (audit).
Auditor	Orang atau tim yang bertanggung jawab melakukan pemeriksaan (audit) keamanan secara independen.
CISA	Sertifikasi profesional oleh Information Systems Audit and Control Association (ISACA) yang diakui secara global
DDoS Attack	Distributed Denial of Service Attack. Serangan yang membanjiri target (peladen atau situs web) dengan lalu lintas internet dari banyak sumber sehingga situs web tidak dapat diakses.
Doxing	Tindakan menyebarkan informasi identitas pribadi atau rahasia seseorang di internet tanpa izin, seringkali dengan tujuan jahat.
Enkripsi	Proses mengubah informasi (data) menjadi kode rahasia (*ciphertext*) untuk mencegah akses oleh pihak yang tidak berwenang. Hanya penerima dengan kunci dekrip yang dapat membukanya.
Exhibitionism	Perilaku seseorang yang secara eksplisit memamerkan atau menyebarkan konten seksual dirinya kepada orang lain tanpa persetujuan.

Ekstranet	Jaringan privat yang diperluas untuk memungkinkan akses aman ke operasi atau data organisasi oleh pihak luar tertentu (misalnya, mitra bisnis, pemasok, pelanggan).
Hardware	Perangat keras. Komponen fisik dan nyata dari sistem komputer atau perangkat, seperti media penyimpanan, memori, atau monitor.
Impersonasi	Tindakan berpura-pura menjadi orang lain, seringkali untuk tujuan menipu atau memperoleh informasi (termasuk penipuan identitas).
Impersonasi Web	Tindakan membuat situs web palsu yang meniru situs web resmi (misalnya bank atau layanan populer) untuk mencuri kredensial pengguna; mirip dengan *phishing*.
Injeksi SQL	*Structured Query Language Injection*. Kerentanan yang terjadi ketika penyerang memasukkan kode SQL berbahaya ke kolom input untuk memanipulasi basis data aplikasi web.
Intimidasi	Tindakan mengancam, menakut-nakuti, atau memaksakan kehendak kepada seseorang (daring maupun luring).
ISACA	Information Systems Audit and Control Association. Asosiasi profesional global untuk tata kelola, kontrol, dan keamanan teknologi informasi.
Kebocoran data	Insiden keamanan di mana data sensitif, terlindungi, atau rahasia disalin, ditransmisikan, dilihat, dicuri, atau digunakan oleh individu yang tidak berwenang.
Kredensial	Informasi untuk membuktikan identitas saat mengakses sistem, seperti nama pengguna (*username*) dan kata sandi (*password*).
LAN	*Local Area Network*. Jaringan komputer yang menghubungkan perangkat dalam area geografis terbatas, seperti rumah, kantor, atau gedung sekolah.

Malvertising	Penggunaan iklan daring yang sah untuk mendistribusikan *malware* (perangkat lunak jahat) atau mengarahkan pengguna ke situs web berbahaya.
MFA	Autentikasi Multi-Faktor. Konsep yang sama dengan 2FA, tetapi dapat mencakup lebih dari dua faktor verifikasi.
NAS	*Network Attached Storage*. Perangkat penyimpanan data khusus yang terhubung ke jaringan dan memungkinkan akses data dari beberapa pengguna dan perangkat.
NCII	*Non-Consensual Intimate Imagery*. Penyebaran gambar atau video intim seseorang tanpa persetujuan mereka.
NDA	*Non-Disclosure Agreement*. Perjanjian kerahasiaan hukum antara dua pihak yang mencegah informasi rahasia diungkapkan.
Peladen (*server*)	Program atau perangkat komputer yang menyediakan layanan atau sumber daya untuk program atau perangkat lain, yang dikenal sebagai klien.
Pemutusan kabel Internet	Serangan fisik yang menargetkan kabel serat optik atau infrastruktur jaringan lain untuk memutuskan koneksi internet wilayah luas.
Pengambilalihan akun	Serangan digital di mana penyerang mendapatkan akses ke akun pengguna dan mengambil kendali penuh atasnya.
Pengawasan ilegal	Pemantauan atau pengumpulan informasi tentang seseorang atau sekelompok orang secara diam-diam dan tanpa dasar hukum atau persetujuan.
Peretasan	Tindakan mendapatkan akses tidak sah ke sistem komputer atau jaringan, seringkali dengan tujuan jahat.
Peretasan situs web	Serangan yang bertujuan memodifikasi tampilan, konten, atau fungsi situs web tanpa izin pemiliknya.

SAFEnet	Southeast Asia Freedom of Expression Network. Organisasi masyarakat sipil di Indonesia yang berfokus di isu hak-hak digital.
SAFETAG	Security Auditing Framework and Evaluation Template for The Advocacy Group. Kerangka kerja audit keamanan yang disesuaikan untuk organisasi masyarakat sipil dan kelompok advokasi.
Sextortion	Pemerasan yang dilakukan dengan mengancam akan menyebarkan gambar, video, atau informasi bersifat seksual atau intim tentang korban.
Software	Perangkat Lunak. Program dan data yang digunakan untuk mengoperasikan komputer dan menjalankan tugas-tugas spesifik (lawan dari hardware).
SSID	Service Set Identifier. Nama jaringan nirkabel (Wi-Fi) untuk mengidentifikasi dan menyambungkan ke jaringan tersebut.
Tingkat keparahan	Ukuran dampak atau risiko dari suatu kerentanan atau insiden keamanan (misalnya, rendah, sedang, tinggi, kritis).
Trolling	Tindakan meunggah komentar yang memprovokasi, mengganggu, atau memprovokasi di media sosial dengan tujuan memicu reaksi emosional.
Uji Penetrasi	*Penetration Test (Pentest)*. Upaya melakukan serangan secara etis pada sistem atau jaringan untuk menemukan kerentanan keamanan yang dapat dieksploitasi.
Website footprinting	Proses pengumpulan informasi (jejak) pasif tentang situs web target dan infrastrukturnya sebelum melakukan serangan.
Zoom Bombing	Gangguan terhadap panggilan konferensi video (biasanya di Zoom) dengan menyajikan konten yang menyinggung atau mengganggu.

FORMAT PKS

Berikut adalah contoh format Perjanjian Kerja Sama yang mencakup NDA antara auditor dan auditi. Secara struktur dan substansi bisa disesuaikan dengan kondisi di lapangan. Dokumen bisa diunduh di s.id/format-pks

SURAT PERJANJIAN KERJA SAMA

Nomor: 123/ADM/BULAN/TAHUN

Yang bertanda tangan di bawah ini, masing-masing :

Nama	:
Jabatan	:
Alamat Kantor	:
Telepon	:
Email	:

Dalam perjanjian ini bertindak untuk dan atas nama [ORGANISASI/NAMA INDIVIDU AUDITOR], selanjutnya disebut PIHAK PERTAMA.

Nama	:
Jabatan	:
Alamat Kantor	:
Telepon	:
Email	:

Dalam perjanjian ini bertindak untuk dan atas nama [MEDIA YANG DIAUDIT], selanjutnya disebut sebagai PIHAK KEDUA.

Selanjutnya PIHAK PERTAMA dan PIHAK KEDUA secara bersama-sama disebut PARA PIHAK.

Secara sadar PARA PIHAK telah bersepakat untuk membuat Perjanjian Kerja Sama dalam rangka [TUJUAN KERJA SAMA] dengan ketentuan sebagai berikut:

Pasal 1
Lingkup Kerja Sama

Lingkup kerja sama PARA PIHAK dalam Perjanjian Kerja Sama ini adalah:

a) Pelaksanaan audit keamanan digital,
b) Penyusunan kebijakan dan panduan keamanan digital,
c) Pelatihan keamanan digital, serta
d) Pendampingan pelaksanaan kebijakan dan panduan keamanan digital.

Pasal 2
Jangka Waktu Perjanjian

Perjanjian ini dilaksanakan selama (BERAPA) bulan pada TANGGAL MULAI HINGGA TANGGAL SELESAI.

Pasal 3
Hak dan Kewajiban

- PIHAK PERTAMA berkewajiban untuk melakukan audit keamanan digital meliputi kebijakan dan praktik oleh PIHAK KEDUA;
- PIHAK PERTAMA berkewajiban untuk menyusun Laporan Hasil Audit Keamanan Digital yang mencakup pelaksanaan, metode, temuan, dan rekomendasi untuk peningkatan keamanan digital PIHAK KEDUA;
- PIHAK PERTAMA berhak mendapatkan informasi dan data yang diperlukan dalam pekerjaan ini dari PIHAK KEDUA;

- PIHAK PERTAMA berhak mendapatkan dukungan dari PIHAK KEDUA untuk bisa menyelesaikan semua pekerjaan dalam Perjanjian Kerja Sama ini;
- PIHAK KEDUA berkewajiban untuk memberikan informasi dan data kepada PIHAK PERTAMA untuk menyelesaikan semua pekerjaan dalam Perjanjian Kerja Sama ini;
- PIHAK KEDUA berkewajiban untuk berkoordinasi secara internal agar staf-staf PIHAK KEDUA yang diperlukan dalam pekerjaan ini bisa bersedia dan bisa bekerja sama dalam proses audit oleh PIHAK PERTAMA; dan
- PIHAK KEDUA berhak mendapatkan hasil pekerjaan yang dilakukan PIHAK PERTAMA, sesuai dengan jadwal yang disepakati.

Pasal 4
Mekanisme Koordinasi

Mekanisme koordinasi dalam Perjanjian Kerja Sama ini dibagi dalam dua jalur, yaitu:

- Untuk proses administrasi dan perjanjian kerja, PIHAK KEDUA bisa berkoordinasi dengan PIHAK PERTAMA; dan
- Untuk proses komunikasi dan koordinasi dalam menyelesaikan lingkup pekerjaan, maka PIHAK PERTAMA menunjuk Tim Auditor untuk langsung berkoordinasi dengan Pemimpin Redaksi PIHAK KEDUA.

Pasal 5
Kerahasiaan Data

PIHAK PERTAMA dilarang menggunakan dan mengungkapkan rahasia organisasi seperti keuangan, data pribadi, keamanan, dan sebagainya milik PIHAK KEDUA; kecuali diperintahkan oleh pihak yang berwenang, seperti Pengadilan, Kepolisian atau instansi-instansi Pemerintah/Non Pemerintah yang resmi di mata Hukum Indonesia.

Pengungkapan untuk keperluan di atas harus mendapat persetujuan tertulis oleh PIHAK KEDUA, dalam format yang dibuat dan dikeluarkan oleh PIHAK KEDUA. Pelarangan ini akan terus berlaku walaupun perjanjian ini telah berakhir.

Pasal 7
Amendemen

Apabila ada suatu perubahan yang belum diatur sebelumnya dalam kesepakatan PARA PIHAK atau belum diatur dalam surat perjanjian ini maka akan dimusyawarahkan lebih lanjut oleh para pihak dan hasil dari musyawarah tersebut akan dituangkan dalam addendum yang tak terpisahkan dari perjanjian ini.

Perjanjian ini dibuat dalam dua rangkap dan ditandatangani PARA PIHAK sebagai bukti persetujuan atas isi perjanjian kerja sama ini.

KOTA, TANGGAL

PIHAK I PIHAK II

DAFTAR PIRANTI & APLIKASI

Berikut ini daftar fungsi layanan pengujian pihak ketiga yang dapat digunakan.

Alat	Kategori	Fungsi Utama	Tingkat Kesulitan
BuiltWith/ Waaplyzer (free)	Pembaca Teknologi Website	Mengidentifikasi teknologi yang digunakan dalam membangun situs web	Mudah
DNSDumpster (free)	Pencari Subdomain dan Informasi DNS	Mencari informasi jaringan pada suato domain, seperti subdomain, IP alamat, dan informasi DNS lainnya	Mudah
SecurityTrails (freemium)	Pencari Subdomain dan Informasi DNS	Menyediakan data tentang infrastruktur digital. Serupa dengan DNSDumpster, tetapi menawarkan fitur yang lebih lengkap	Mudah
Censys (freemium)	Pencari infrastruktur peladen	Menemukan dan mengawasi peladen yang terhubung dalam jaringan internet	Mudah
MxToolbox: MX Lookup Tool (free)	Alat periksa infrastruktur surel	Mengidentifikasi pengaturan surel	Mudah
WPScan (free)	Pembaca Kerentanan Umum	Mengidentifikasi kerentanan yang spesifik pada platform WordPress	Mudah ke Sedang
Sucuri Sitecheck (free)	Pembaca Kerentanan Umum	Mengidentifikasi kerentanan umum pada suatu situs web	Mudah
UpGuard (freemium)	Pemantau Keamanan dan Kepatuhan	Mengidentifikasi kerentanan umum pada suatu situs web	Mudah

SSL Labs (free)	Penguji Pengaturan SSL/TLS	Menganalisis konfigurasi SSL/TLS pada sebuah server web	Mudah
ZAP, Nessus, Burp Suite	Pemindai kerentanan menyeluruh dan mendalam	Melakukan pindai terhadat aplikasi dan jaringan web	Sulit

TABEL DAFTAR ASET

Berikut format tabel Daftar Aset media. Dokumen bisa diunduh dari s.id/daftar-aset

Lembaga :
Tanggal :

No	Media Sosial	Akun	Tautan	Follower / Subscriber	Pengamanan
1	Twitter				Contoh: pakai 2FA, password dg kalimat sandi, dst.

PANDUAN PENILAIAN KEAMANAN DIGITAL MANDIRI (PAKEM DIRI)

Versi: Oktober 2025

PAKEM DIRI adalah metode penilaian keamanan digital secara mandiri yang sedang dikembangkan SAFEnet untuk menilai tingkat risiko keamanan digital secara personal. Dokumen bisa diunduh di s.id/pakem-diri

Nama :
Tanggal :

Petunjuk Pengisian:

Jawablah berdasarkan perilaku Anda sehari-hari. Jika Anda memilih Ya, masukkan angka 1. Jika Tidak, masukkan angka 0. Hasil akhir akan menunjukkan tingkat risikonya.

KEAMANAN PERANGKAT

Kriteria Keamanan	Ya / Tidak
Memisahkan laptop untuk bekerja dan pribadi	
Menggunakan sistem operasi (OS) orisinal, bukan bajakan	
Menggunakan program atau aplikasi orisinal, bukan bajakan	

Mengunci layar (kata sandi, PIN, atau biometrik) untuk membuka perangkat	
Mengaktifkan firewall	
Melakukan enkripsi media penyimpan	
Mematikan fungsi lokasi pada laptop	
Melakukan pencadangan (*back up*) secara berkala, setidaknya sebulan sekali	
Membersihkan berkas dan aplikasi yang sudah tidak digunakan secara berkala	
Menggunakan antivirus dan pembersih (*cleaner*)	
Memperbarui (*update*) sistem operasi dan aplikasi jika ada pembaruan	
Menghapus riwayat penggunaan Wi-Fi secara rutin	

KEAMANAN PONSEL

Kriteria Keamanan Ponsel	Ya / Tidak
Memisahkan ponsel untuk bekerja atau hal sensitif dengan ponsel untuk keperluan pribadi	
Melindungi ponsel secara fisik yaitu dengan menggunakan pelindung luar (*casing*) dan atau pelindung layar (*screen guard*)	
Melindungi ponsel dengan kunci (password, PIN, pola, atau biometrik) agar tidak mudah diakses orang lain	
Mengaktifkan penguncian otomatis jika tidak digunakan dalam waktu tertentu, misalnya 1 menit atau 5 menit	
Memperbarui sistem operasi (OS) dan aplikasi jika tersedia	
Mengganti nama ponsel dengan nama lain agar tidak mudah dikenali	
Menonaktifkan Bluetooth dan Wi-Fi jika tidak sedang digunakan	
Memasang (*install*) aplikasi hanya dari sumber resmi	
Menonaktifkan lokasi pada ponsel kecuali jika digunakan	
Keluar (*logout*) dari aplikasi email jika tidak digunakan dalam waktu lama, misalnya satu minggu	
Memeriksa sejauh mana akses setiap aplikasi terhadap data di ponsel	

Memeriksa apa saja perangkat lain (misalnya laptop) yang terhubung untuk aplikasi pesan ringkas di ponsel, seperti Whatspaa, Telegram dan Wire	
Menggunakan peramban yang tidak merekam aktivitas penggunanya, seperti Firefox Focus, Brave, dan Ducduckgo	
Melakukan pencadangan data (*back up*) secara berkala, misalnya sebulan sekali	
Mengaktifkan enkripsi pada ponsel agar tidak bisa dibuka dari perangkat lain tanpa izin pemilik	
Memasang aplikasi mesin pencari yang aman, seperti Brave dan DuckDuckGo	
Menggunakan antivirus untuk mendeteksi jika ada perangkat berbahaya (*malware*) di ponsel	
Memeriksa secara berkala aplikasi dan berkas apa saja yang sudah tidak digunakan dan menghapusnya jika tidak diperlukan	
Menghapus riwayat Wi-Fi pada ponsel agar tidak meninggalkan jejak digital	

KEAMANAN AKUN

Kriteria Keamanan	Ya / Tidak
Membedakan antara akun pribadi, seperti untuk belanja dengan akun pekerjaan	
Membatasi mengunggah identitas personal seperti keluarga, tanggal lahir, alamat, dan semacamnya	
Membuat password yang kompleks dan kuat	
Membuat password berbeda-beda untuk setiap aset digital yang dimiliki	
Mencatat password di aplikasi pengelola password seperti KeePass atau Bitwarden	
Mengganti password secara berkala setidaknya enam bulan sekali	
Menggunakan metode 2FA untuk memperkuat keamanan perangkat maupun aset-aset digital lainnya	

KEAMANAN KOMUNIKASI

Kriteria Keamanan	Ya / Tidak
Menggunakan koneksi pribadi, misalnya *tethering* dari ponsel sendiri atau Wi-Fi kantor/rumah, pada saat berinternet	
Menggunakan VPN ketika mengakses Wi-Fi publik	
Menghindari penggunaan informasi sensitif dan personal ketika menggunakan Wi-Fi publik	
Menggunakan peramban aman, seperti Brave dan Firefox, untuk mengurangi jejak digital saat berselancar	
Menghapus riwayat data dan kukis di peramban secara berkala	
Menggunakan aplikasi pesan terenkripsi, misalnya Signal atau Wire, sebagai grup resmi pekerjaan	
Menggunakan surel terenkripsi untuk berkomunikasi tentang hal-hal sensitif	
Menggunakan mesin pencari yang lebih menghargai privasi	
Menggunakan layanan terenkripsi, seperti BigBlueBotton dan Jitsi, untuk panggilan video	
Menggunakan layanan *cloud* terenkripsi dan bisa dikunci, seperti Proton Dive dan Mega, untuk berbagi berkas	

Mewaspadai dan berhati-hati terhadap surel atau pranala dari pengirim yang tidak dikenal	
Memeriksa keamanan pranala atau berkas di database malware seperti virustotal dan urlscan.io	

NILAI TOTAL	**0.00**

Cara Menghitung

Berikut adalah penjelasan nilai akhir yang diperoleh:

- 1 - 20 = tingkat risiko sangat tinggi
- 21 – 40 = tingkat risiko tinggi
- 41 - 60 = tingkat risiko sedang
- 61 – 80 = tingkat risiko rendah
- 81 – 100 = tingkat risiko sangat rendah

Untuk menggunakan PAKEM DIRI atau berkonsultasi lebih lanjut silakan hubungi SAFEnet di info@safenet.or.id atau Hotline +62817-9323-375.

Panduan ini merupakan acuan dalam melaksanakan audit keamanan digital untuk media, khususnya media daring. Materi panduan mencakup landasan teoritis dan praktis bagaimana sebuah audit keamanan digital media sebaiknya dilakukan, termasuk memahami konsep, tujuan, dan tahapan kerjanya.

SAFEnet

Jalan Gita Sura III Nomor 55 Peguyangan Kaja
Denpasar, Bali 80123

Telepon : +62 817 9323375
Surel: info@safenet.or.id
Twitter & Instagram: @safenetvoice
Situs web: safenet.or.id