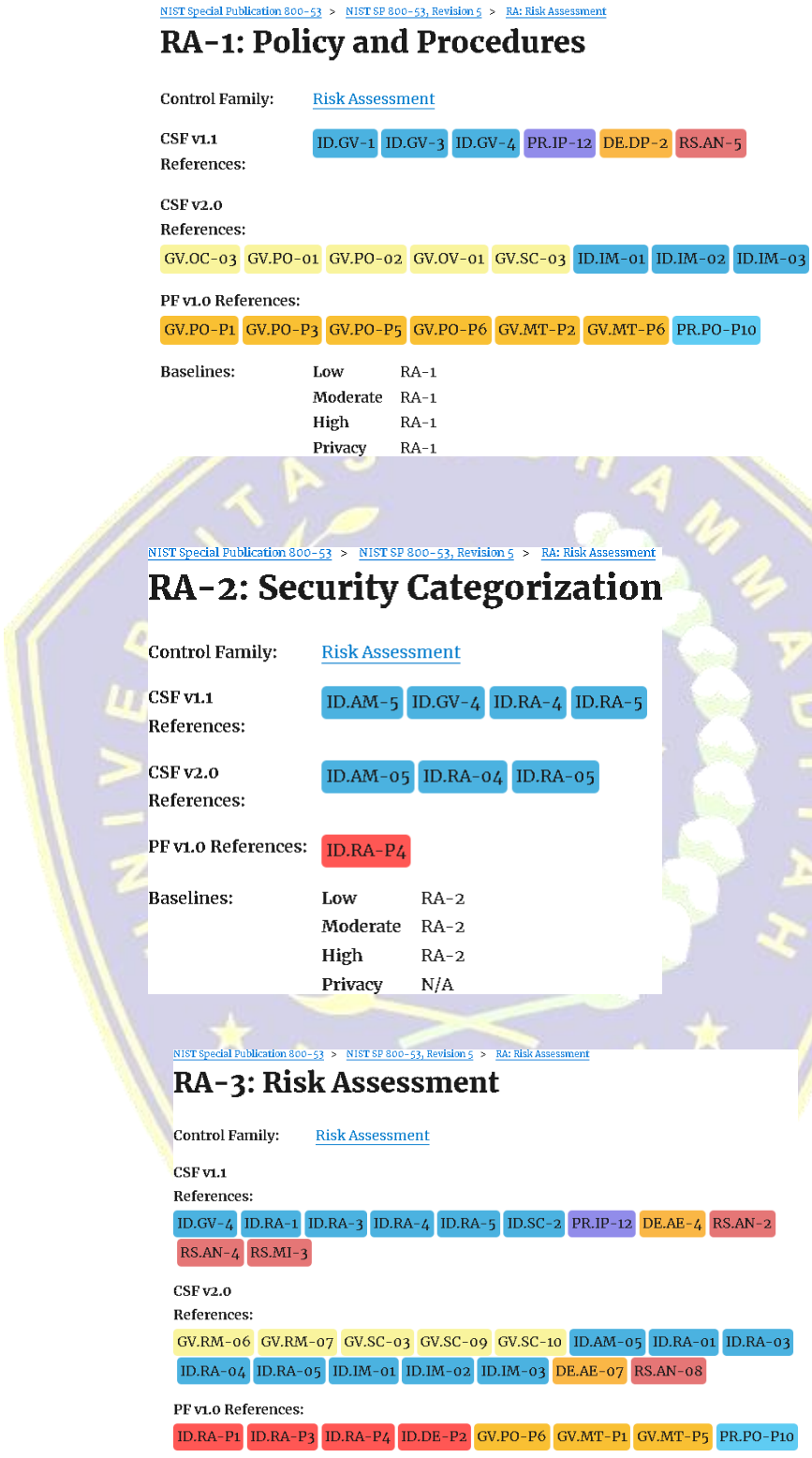
LAMPIRAN

Lampiran 1



NIST Special Publication 800-53 > NIST SP 800-53, Revision 5 > RA: Risk Assessment

RA-1: Policy and Procedures

Control Family: Risk Assessment

CSF v1.1 References: ID.GV-1 ID.GV-3 ID.GV-4 PR.IP-12 DE.DP-2 RS.AN-5

CSF v2.0 References: GV.OC-03 GV.PO-01 GV.PO-02 GV.OV-01 GV.SC-03 ID.IM-01 ID.IM-02 ID.IM-03

PF v1.0 References: GV.PO-P1 GV.PO-P3 GV.PO-P5 GV.PO-P6 GV.MT-P2 GV.MT-P6 PR.PO-P10

Baselines:

Low	RA-1
Moderate	RA-1
High	RA-1
Privacy	RA-1

NIST Special Publication 800-53 > NIST SP 800-53, Revision 5 > RA: Risk Assessment

RA-2: Security Categorization

Control Family: Risk Assessment

CSF v1.1 References: ID.AM-5 ID.GV-4 ID.RA-4 ID.RA-5

CSF v2.0 References: ID.AM-05 ID.RA-04 ID.RA-05

PF v1.0 References: ID.RA-P4

Baselines:

Low	RA-2
Moderate	RA-2
High	RA-2
Privacy	N/A

NIST Special Publication 800-53 > NIST SP 800-53, Revision 5 > RA: Risk Assessment

RA-3: Risk Assessment

Control Family: Risk Assessment

CSF v1.1 References: ID.GV-4 ID.RA-1 ID.RA-3 ID.RA-4 ID.RA-5 ID.SC-2 PR.IP-12 DE.AE-4 RS.AN-2 RS.AN-4 RS.MI-3

CSF v2.0 References: GV.RM-06 GV.RM-07 GV.SC-03 GV.SC-09 GV.SC-10 ID.AM-05 ID.RA-01 ID.RA-03 ID.RA-04 ID.RA-05 ID.IM-01 ID.IM-02 ID.IM-03 DE.AE-07 RS.AN-08

PF v1.0 References: ID.RA-P1 ID.RA-P3 ID.RA-P4 ID.DE-P2 GV.PO-P6 GV.MT-P1 GV.MT-P5 PR.PO-P10

NIST Special Publication 800-53 > NIST SP 800-53, Revision 5 > RA: Risk Assessment

RA-5: Vulnerability Monitoring and Scanning

Control Family: Risk Assessment

CSF v1.1 References: ID.RA-1 PR.IP-12 DE.AE-2 DE.CM-8 DE.DP-4 DE.DP-5 RS.AN-1 RS.MI-3

CSF v2.0 References: GV.SC-10 ID.RA-01 ID.RA-08 ID.IM-01 ID.IM-02 ID.IM-03

PF v1.0 References: PR.PO-P10

Baselines:

Low	RA-5 (2) (11)
Moderate	RA-5 (2) (5) (11)
High	RA-5 (2) (4) (5) (11)

NIST Special Publication 800-53 > NIST SP 800-53, Revision 5 > RA: Risk Assessment

RA-6: Technical Surveillance Countermeasures Survey

Control Family: Risk Assessment

Baselines:

Low	N/A
Moderate	N/A
High	N/A
Privacy	N/A

Previous Version: NIST Special Publication 800-53 Revision 4: RA-6: Technical Surveillance Countermeasures Survey

NIST Special Publication 800-53 > NIST SP 800-53, Revision 5 > RA: Risk Assessment

RA-7: Risk Response

Control Family: Risk Assessment

CSF v1.1 References: ID.RA-6 RS.AN-5 RS.MI-3

CSF v2.0 References: GV.OC-05 GV.RM-01 GV.RM-03 GV.OV-01 GV.OV-02 GV.OV-03 GV.SC-03 GV.SC-09 GV.SC-10 ID.RA-05 ID.RA-06 ID.IM-01 ID.IM-02 ID.IM-03 RS.AN-08

PF v1.0 References: ID.RA-P5

Baselines:

Low	RA-7
Moderate	RA-7
High	RA-7
Privacy	RA-7

NIST Special Publication 800-53 > NIST SP 800-53, Revision 5 > RA: Risk Assessment

RA-8: Privacy Impact Assessments

Control Family: Risk Assessment

CSF v2.0 References: ID.RA-04

PF v1.0 References: ID.RA-P1 ID.RA-P3 ID.RA-P4 ID.RA-P5 ID.DE-P2 GV.PO-P6 GV.MT-P1 GV.MT-P5 CM.PO-P1

Baselines:

Low	N/A
Moderate	N/A
High	N/A
Privacy	RA-8

NIST Special Publication 800-53 > NIST SP 800-53, Revision 5 > RA: Risk Assessment

RA-9: Criticality Analysis

Control Family: Risk Assessment

CSF v1.1 References: ID.AM-5 ID.BE-4 ID.BE-5 ID.RA-4 ID.RM-3

CSF v2.0 References: GV.OC-04 GV.SC-04 GV.SC-07 ID.AM-05 ID.RA-04

PF v1.0 References: ID.BE-P3

Baselines:

Low	N/A
Moderate	RA-9
High	RA-9
Privacy	N/A

NIST Special Publication 800-53 > NIST SP 800-53, Revision 5 > RA: Risk Assessment

RA-10: Threat Hunting

Control Family: Risk Assessment

CSF v1.1 References: ID.RA-2 ID.RA-3

CSF v2.0 References: DE.AE-06 DE.AE-07

Baselines:

Low	N/A
Moderate	N/A
High	N/A
Privacy	N/A

Lampiran 2

RA-1: Kebijakan dan Prosedur	GV.OC-03: Persyaratan hukum, peraturan, dan kontraktual mengenai keamanan siber – termasuk kewajiban privasi dan kebebasan sipil – dipahami dan dikelola	Ex1 : Menentukan proses untuk melacak dan mengelola persyaratan hukum dan peraturan mengenai perlindungan informasi individu (misalnya, Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan, Undang-Undang Privasi Konsumen California, Peraturan Perlindungan Data Umum) Ex2 : Menentukan proses untuk melacak dan mengelola persyaratan kontraktual untuk manajemen keamanan siber informasi pemasok, pelanggan, dan mitra. Ex3 : Menyelaraskan strategi keamanan siber organisasi dengan persyaratan hukum, peraturan, dan kontrak
	GV.PO-01: Kebijakan untuk mengelola risiko keamanan siber ditetapkan berdasarkan konteks organisasi, strategi dan prioritas keamanan siber dan dikomunikasikan dan ditegakkan	Ex1 : Membuat, menyebarluaskan, dan memelihara kebijakan manajemen risiko yang dapat dipahami dan digunakan dengan pernyataan maksud, harapan, dan arahan manajemen. Ex2 : Secara berkala meninjau kebijakan dan proses serta prosedur pendukung untuk memastikan bahwa kebijakan dan prosedur tersebut selaras dengan tujuan dan prioritas strategi manajemen risiko, serta arahan tingkat tinggi dari kebijakan keamanan siber. Ex3 : Memerlukan persetujuan dari manajemen senior atas kebijakan Ex4 : Mengomunikasikan kebijakan manajemen risiko keamanan siber dan mendukung proses serta prosedur di seluruh organisasi Ex5 : Meminta personel untuk mengakui penerimaan kebijakan ketika pertama kali dipekerjakan, setiap tahun, dan setiap kali kebijakan diperbarui.

	GV.PO-02: Kebijakan untuk mengelola risiko keamanan siber ditinjau, diperbarui, dikomunikasikan, dan ditegakkan untuk mencerminkan perubahan dalam persyaratan, ancaman, teknologi, dan misi organisasi.	Contoh 1 : Memperbarui kebijakan berdasarkan tinjauan berkala atas hasil manajemen risiko keamanan siber untuk memastikan bahwa kebijakan dan proses serta prosedur pendukung mampu menjaga risiko pada tingkat yang dapat diterima. Contoh 2 : Memberikan garis waktu untuk meninjau perubahan pada lingkungan risiko organisasi (misalnya, perubahan risiko atau tujuan misi organisasi), dan mengomunikasikan pembaruan kebijakan yang direkomendasikan. Ex3 : Memperbarui kebijakan untuk mencerminkan perubahan dalam persyaratan hukum dan peraturan Contoh 4 : Memperbarui kebijakan untuk mencerminkan perubahan teknologi (misalnya, adopsi kecerdasan buatan) dan perubahan bisnis (misalnya, akuisisi bisnis baru, persyaratan kontrak baru)
	GV.OV-01: Hasil strategi manajemen risiko keamanan siber ditinjau untuk menginformasikan dan menyesuaikan strategi dan arah	1st : Risiko Pihak Pertama Ex1 : Mengukur seberapa baik strategi manajemen risiko dan hasil risiko telah membantu para pemimpin dalam membuat keputusan dan mencapai tujuan organisasi. Ex2 : Periksa apakah strategi risiko keamanan siber yang menghambat operasi atau inovasi harus disesuaikan
	GV.SC-03: Manajemen risiko rantai pasokan keamanan siber diintegrasikan ke dalam manajemen risiko siber dan perusahaan, penilaian risiko, dan proses perbaikan	Ex1 : Mengidentifikasi area keselarasan dan tumpang tindih dengan keamanan siber dan manajemen risiko perusahaan Ex2 : Menetapkan perangkat kontrol terpadu untuk manajemen risiko keamanan siber dan manajemen risiko rantai pasokan keamanan siber Ex3 : Mengintegrasikan manajemen risiko rantai pasokan keamanan siber ke dalam proses perbaikan Ex4 : Meningkatkan risiko keamanan siber yang material dalam rantai pasokan ke manajemen senior, dan mengatasinya di tingkat manajemen risiko perusahaan 3 : Risiko Pihak Ketiga

	ID.IM-01: Perbaikan diidentifikasi dari evaluasi	Ex1 : Melakukan penilaian mandiri terhadap layanan penting yang mempertimbangkan ancaman dan TTP saat ini Ex2 : Berinvestasilah dalam penilaian pihak ketiga atau audit independen atas efektivitas program keamanan siber organisasi untuk mengidentifikasi area yang memerlukan perbaikan. Ex3 : Mengevaluasi kepatuhan terhadap persyaratan keamanan siber terpilih secara terus-menerus melalui cara otomatis
	ID.IM-03: Peningkatan diidentifikasi dari pelaksanaan proses, prosedur, dan aktivitas operasional.	Ex1 : Melaksanakan sesi pembelajaran kolaboratif dengan para pemasok Ex2 : Meninjau kebijakan, proses, dan prosedur keamanan siber setiap tahun untuk mempertimbangkan pelajaran yang didapat Ex3 : Gunakan metrik untuk menilai kinerja keamanan siber operasional dari waktu ke waktu
RA-2: Kategorisasi Keamanan	ID.AM-05: Aset diprioritaskan berdasarkan klasifikasi, kekritisan, sumber daya, dan dampak pada misi	Ex1 : Tentukan kriteria untuk memprioritaskan setiap kelas aset Ex2 : Terapkan kriteria prioritas pada aset Ex3 : Melacak prioritas aset dan memperbaruinya secara berkala atau ketika terjadi perubahan signifikan pada organisasi
	ID.RA-04: Dampak potensial dan kemungkinan ancaman yang mengeksploitasi kerentanan diidentifikasi dan dicatat	Contoh 1 : Pemimpin bisnis dan praktisi manajemen risiko keamanan siber bekerja sama untuk memperkirakan kemungkinan dan dampak skenario risiko dan mencatatnya dalam daftar risiko. Contoh 2 : Hitung dampak potensial terhadap bisnis dari akses tidak sah ke komunikasi, sistem, dan data organisasi yang diproses di dalam atau oleh sistem tersebut.
	ID.RA-05: Ancaman, kerentanan, kemungkinan, dan dampak digunakan untuk memahami risiko inheren dan menginformasikan prioritas respons risiko.	Ex1 : Mengembangkan model ancaman untuk lebih memahami risiko terhadap data dan mengidentifikasi respons risiko yang tepat Contoh 2 : Prioritaskan alokasi sumber daya dan investasi keamanan siber berdasarkan perkiraan kemungkinan dan dampaknya

RA-3: Penilaian Risiko	GV.RM-06: Metode standar untuk menghitung, mendokumentasikan, mengkategorikan, dan memprioritaskan risiko keamanan siber ditetapkan dan dikomunikasikan	Ex1 : Menetapkan kriteria untuk menggunakan pendekatan kuantitatif terhadap analisis risiko keamanan siber, dan menentukan rumus probabilitas dan paparan. Ex2 : Membuat dan menggunakan templat (misalnya, daftar risiko) untuk mendokumentasikan informasi risiko keamanan siber (misalnya, deskripsi risiko, paparan, penanganan, dan kepemilikan) Ex3 : Menetapkan kriteria untuk memprioritaskan risiko pada tingkat yang tepat dalam perusahaan Ex4 : Gunakan daftar kategori risiko yang konsisten untuk mendukung pengintegrasian, penggabungan, dan perbandingan risiko keamanan siber.
	GV.RM-07: Peluang strategis (yaitu, risiko positif) dicirikan dan dimasukkan dalam diskusi risiko keamanan siber organisasi	Ex1 : Menetapkan dan mengomunikasikan panduan dan metode untuk mengidentifikasi peluang dan memasukkannya ke dalam diskusi risiko (misalnya, analisis kekuatan, kelemahan, peluang, dan ancaman [SWOT]) Ex2 : Mengidentifikasi sasaran pengembangan dan mendokumentasikannya Ex3 : Hitung, dokumentasikan, dan prioritaskan risiko positif di samping risiko negatif
	GV.SC-09: Praktik keamanan rantai pasokan diintegrasikan ke dalam program keamanan siber dan manajemen risiko perusahaan, dan kinerjanya dipantau sepanjang siklus hidup produk dan layanan teknologi.	Ex1 : Kebijakan dan prosedur memerlukan catatan asal usul untuk semua produk dan layanan teknologi yang diperoleh Ex2 : Secara berkala memberikan laporan risiko kepada para pemimpin tentang bagaimana komponen yang diperoleh terbukti tidak dirusak dan autentik. Ex3 : Berkomunikasi secara berkala di antara manajer risiko keamanan siber dan personel operasi mengenai perlunya memperoleh patch, pembaruan, dan pemutakhiran perangkat lunak hanya dari penyedia perangkat lunak yang sah dan tepercaya.Ex4 : Meninjau kebijakan untuk memastikan bahwa kebijakan tersebut mengharuskan personel pemasok yang disetujui untuk melakukan pemeliharaan pada produk

		pemasok. Ex5 : Kebijakan dan prosedur memerlukan pengecekan terhadap peningkatan perangkat keras penting untuk mengetahui adanya perubahan yang tidak sah
	GV.SC-10: Rencana manajemen risiko rantai pasokan keamanan siber mencakup ketentuan untuk aktivitas yang terjadi setelah berakhirnya kemitraan atau perjanjian layanan.	Ex1 : Menetapkan proses untuk mengakhiri hubungan kritis baik dalam keadaan normal maupun buruk Ex2 : Menetapkan dan menerapkan rencana untuk dukungan pemeliharaan akhir masa pakai komponen dan keusangan Ex3 : Verifikasi bahwa akses pemasok ke sumber daya organisasi dinonaktifkan segera ketika tidak lagi diperlukan Ex4 : Verifikasi bahwa aset yang berisi data organisasi dikembalikan atau dibuang dengan benar tepat waktu, terkendali, dan aman. Ex5 : Mengembangkan dan melaksanakan rencana untuk mengakhiri atau mentransisikan hubungan pemasok yang memperhitungkan risiko keamanan dan ketahanan rantai pasokan Ex6 : Mengurangi risiko terhadap data dan sistem yang disebabkan oleh pemutusan hubungan kerja dengan pemasok Ex7 : Mengelola risiko kebocoran data yang terkait dengan pemutusan hubungan kerja dengan pemasok
	ID.AM-05: Aset diprioritaskan berdasarkan klasifikasi, kekritisan, sumber daya, dan dampak pada misi	Ex1 : Tentukan kriteria untuk memprioritaskan setiap kelas aset Ex2 : Terapkan kriteria prioritas pada aset Ex3 : Melacak prioritas aset dan memperbaruinya secara berkala atau ketika terjadi perubahan signifikan pada organisasi

	ID.RA-01: Kerentanan dalam aset diidentifikasi, divalidasi, dan dicatat	Ex1 : Gunakan teknologi manajemen kerentanan untuk mengidentifikasi perangkat lunak yang tidak ditambal dan salah konfigurasi. Ex2 : Menilai arsitektur jaringan dan sistem untuk kelemahan desain dan implementasi yang memengaruhi keamanan siber Ex3 : Meninjau, menganalisis, atau menguji perangkat lunak yang dikembangkan organisasi untuk mengidentifikasi kerentanan desain, pengkodean, dan konfigurasi default. Ex4 : Menilai fasilitas yang menyimpan aset komputasi penting untuk mengetahui kerentanan fisik dan masalah ketahanan Ex5 : Memantau sumber intelijen ancaman siber untuk mendapatkan informasi tentang kerentanan baru dalam produk dan layanan Ex6 : Meninjau proses dan prosedur untuk menemukan kelemahan yang dapat dimanfaatkan untuk mempengaruhi keamanan siber.
	ID.IM-01: Perbaikan diidentifikasi dari evaluasi	Ex1 : Melakukan penilaian mandiri terhadap layanan penting yang mempertimbangkan ancaman dan TTP saat ini Ex2 : Berinvestasilah dalam penilaian pihak ketiga atau audit independen atas efektivitas program keamanan siber organisasi untuk mengidentifikasi area yang memerlukan perbaikan. Ex3 : Terus mengevaluasi kepatuhan terhadap persyaratan keamanan siber terpilih melalui cara otomatis
	ID.IM-03: Peningkatan diidentifikasi dari pelaksanaan proses, prosedur, dan aktivitas operasional.	Ex1 : Melaksanakan sesi pembelajaran kolaboratif dengan pemasok Ex2 : Meninjau kebijakan, proses, dan prosedur keamanan siber setiap tahun untuk mempertimbangkan pelajaran yang didapat Ex3 : Gunakan metrik untuk menilai kinerja keamanan siber operasional dari waktu ke waktu

	DE.AE-07: Intelijen ancaman siber dan informasi kontekstual lainnya diintegrasikan ke dalam analisis	Ex1 : Menyediakan umpan intelijen ancaman cyber secara aman ke teknologi deteksi, proses, dan personel x2 : Menyediakan informasi dari inventaris aset ke teknologi deteksi, proses, dan personel secara aman Ex3 : Memperoleh dan menganalisis pengungkapan kerentanan secara cepat untuk teknologi organisasi dari pemasok, vendor, dan penasihat keamanan pihak ketiga
	RS.AN-08: Besarnya insiden diperkirakan dan divalidasi	Ex1 : Meninjau target potensial lain dari insiden tersebut untuk mencari indikator kompromi dan bukti persistensi Ex2 : Menjalankan alat secara otomatis pada target untuk mencari indikator kompromi dan bukti persistensi
RA-5: Pemantauan dan Pemindaian Kerentanan	GV.SC-10: Rencana manajemen risiko rantai pasokan keamanan siber mencakup ketentuan untuk aktivitas yang terjadi setelah berakhirnya kemitraan atau perjanjian layanan.	Ex1 : Menetapkan proses untuk mengakhiri hubungan kritis baik dalam keadaan normal maupun buruk Ex2 : Menetapkan dan menerapkan rencana untuk dukungan pemeliharaan akhir masa pakai komponen dan keusangan Ex3 : Verifikasi bahwa akses pemasok ke sumber daya organisasi dinonaktifkan segera ketika tidak lagi diperlukan Ex4 : Verifikasi bahwa aset yang berisi data organisasi dikembalikan atau dibuang dengan benar tepat waktu, terkendali, dan aman. Ex5 : Mengembangkan dan melaksanakan rencana untuk mengakhiri atau mentransisikan hubungan pemasok yang memperhitungkan risiko keamanan dan ketahanan rantai pasokan Ex6 : Mengurangi risiko terhadap data dan sistem yang disebabkan oleh pemutusan hubungan kerja dengan pemasok Ex7 : Mengelola risiko kebocoran data yang terkait dengan pemutusan hubungan kerja dengan pemasok

	ID.RA-08: Proses untuk menerima, menganalisis, dan menanggapi pengungkapan kerentanan ditetapkan	Ex1 : Melakukan pembagian informasi kerentanan antara organisasi dan pemasoknya dengan mengikuti aturan dan protokol yang ditetapkan dalam kontrak. Ex2 : Menetapkan tanggung jawab dan memverifikasi pelaksanaan prosedur untuk memproses, menganalisis dampak, dan menanggapi ancaman, kerentanan, atau pengungkapan insiden keamanan siber oleh pemasok, pelanggan, mitra, dan organisasi keamanan siber pemerintah.
RA-7: Respon Risiko	GV.OC-05: Hasil, kemampuan, dan layanan yang diandalkan oleh organisasi dipahami dan dikomunikasikan	Ex1 : Buat inventaris ketergantungan organisasi pada sumber daya eksternal (misalnya, fasilitas, penyedia hosting berbasis cloud) dan hubungannya dengan aset organisasi dan fungsi bisnis. Ex2 : Mengidentifikasi dan mendokumentasikan ketergantungan eksternal yang merupakan titik kegagalan potensial bagi kemampuan dan layanan penting organisasi, dan membagikan informasi tersebut dengan personel yang sesuai.
	GV.RM-01: Tujuan manajemen risiko ditetapkan dan disetujui oleh pemangku kepentingan organisasi	Ex1 : Memperbarui tujuan manajemen risiko keamanan siber jangka pendek dan jangka panjang sebagai bagian dari perencanaan strategis tahunan dan ketika terjadi perubahan besar Ex2 : Menetapkan tujuan yang terukur untuk manajemen risiko keamanan siber (misalnya, mengelola kualitas pelatihan pengguna, memastikan perlindungan risiko yang memadai untuk sistem kontrol industri) Ex3 : Para pemimpin senior menyetujui tujuan keamanan siber dan menggunakannya untuk mengukur dan mengelola risiko dan kinerja.
	GV.RM-03: Aktivitas dan hasil manajemen risiko keamanan siber dimasukkan dalam proses manajemen risiko perusahaan	Ex1 : Menggabungkan dan mengelola risiko keamanan siber bersama dengan risiko perusahaan lainnya (misalnya, kepatuhan, keuangan, operasional, peraturan, reputasi, keselamatan) Ex2 : Melibatkan manajer risiko keamanan siber dalam perencanaan manajemen risiko perusahaan

		Ex3 : Menetapkan kriteria untuk meningkatkan risiko keamanan siber dalam manajemen risiko perusahaan
	GV.OV-03: Kinerja manajemen risiko keamanan siber organisasi dievaluasi dan ditinjau untuk penyesuaian yang diperlukan	Ex1 : Meninjau indikator kinerja utama (KPI) untuk memastikan bahwa kebijakan dan prosedur di seluruh organisasi mencapai tujuan Ex2 : Meninjau indikator risiko utama (KRI) untuk mengidentifikasi risiko yang dihadapi organisasi, termasuk kemungkinan dan dampak potensial Ex3 : Mengumpulkan dan mengomunikasikan metrik tentang manajemen risiko keamanan siber dengan pimpinan senior
	GV.SC-03: Manajemen risiko rantai pasokan keamanan siber diintegrasikan ke dalam manajemen risiko keamanan siber dan perusahaan, penilaian risiko, dan proses perbaikan	Ex1 : Mengidentifikasi area keselarasan dan tumpang tindih dengan keamanan siber dan manajemen risiko perusahaan Ex2 : Menetapkan perangkat kontrol terpadu untuk manajemen risiko keamanan siber dan manajemen risiko rantai pasokan keamanan siber Ex3 : Mengintegrasikan manajemen risiko rantai pasokan keamanan siber ke dalam proses perbaikan Ex4 : Meningkatkan risiko keamanan siber yang material dalam rantai pasokan ke manajemen senior, dan mengatasinya di tingkat manajemen risiko perusahaan

	GV.SC-10: Rencana manajemen risiko rantai pasokan keamanan siber mencakup ketentuan untuk aktivitas yang terjadi setelah berakhirnya kemitraan atau perjanjian layanan.	Ex1 : Menetapkan proses untuk mengakhiri hubungan kritis baik dalam keadaan normal maupun buruk Ex2 : Menetapkan dan menerapkan rencana untuk dukungan pemeliharaan akhir masa pakai komponen dan keusangan Ex3 : Verifikasi bahwa akses pemasok ke sumber daya organisasi dinonaktifkan segera ketika tidak lagi diperlukan Ex4 : Verifikasi bahwa aset yang berisi data organisasi dikembalikan atau dibuang dengan benar tepat waktu, terkendali, dan aman. Ex5 : Mengembangkan dan melaksanakan rencana untuk mengakhiri atau mentransisikan hubungan pemasok yang memperhitungkan risiko keamanan dan ketahanan rantai pasokan Ex6 : Mengurangi risiko terhadap data dan sistem yang disebabkan oleh pemutusan hubungan kerja dengan pemasok Ex7 : Mengelola risiko kebocoran data yang terkait dengan pemutusan hubungan kerja dengan pemasok
	ID.RA-06: Respon risiko dipilih, diprioritaskan, direncanakan, dilacak, dan dikomunikasikan	Ex1 : Terapkan kriteria rencana pengelolaan kerentanan untuk memutuskan apakah akan menerima, mentransfer, memitigasi, atau menghindari risiko. Ex2 : Terapkan kriteria rencana manajemen kerentanan untuk memilih kontrol kompensasi guna mengurangi risiko Ex3 : Melacak kemajuan implementasi respons risiko (misalnya, rencana tindakan dan tonggak sejarah [POA&M], daftar risiko, laporan detail risiko) Ex4 : Menggunakan temuan penilaian risiko untuk menginformasikan keputusan dan tindakan respons risiko Ex5 : Mengomunikasikan respons risiko yang direncanakan kepada pemangku kepentingan yang terkena dampak berdasarkan urutan prioritas

	ID.IM-03: Peningkatan diidentifikasi dari pelaksanaan proses, prosedur, dan aktivitas operasional.	Ex1 : Melaksanakan sesi pembelajaran kolaboratif dengan para pemasok Ex2 : Meninjau kebijakan, proses, dan prosedur keamanan siber setiap tahun untuk mempertimbangkan pelajaran yang didapat Ex3 : Gunakan metrik untuk menilai kinerja keamanan siber operasional dari waktu ke waktu
	RS.AN-08: Besarnya insiden diperkirakan dan divalidasi	Ex1 : Meninjau target potensial lain dari insiden tersebut untuk mencari indikator kompromi dan bukti persistensi Ex2 : Menjalankan alat secara otomatis pada target untuk mencari indikator kompromi dan bukti persistens
RA-8: Penilaian Dampak Privasi	ID.RA-04: Dampak potensial dan kemungkinan ancaman yang mengeksploitasi kerentanan diidentifikasi dan dicatat	Contoh 1 : Pemimpin bisnis dan praktisi manajemen risiko keamanan siber bekerja sama untuk memperkirakan kemungkinan dan dampak skenario risiko dan mencatatnya dalam daftar risiko. Contoh 2 : Hitung dampak potensial terhadap bisnis dari akses tidak sah ke komunikasi, sistem, dan data organisasi yang diproses di dalam atau oleh sistem tersebut. Ex3 : Menjelaskan dampak potensial dari kegagalan berjenjang pada sistem
RA-9: Analisis Kekritisan	GV.OC-04: Sasaran, kemampuan, dan layanan penting yang diandalkan atau diharapkan oleh pemangku kepentingan dari organisasi dipahami dan dikomunikasikan	Ex1 : Menetapkan kriteria untuk menentukan kekritisan kemampuan dan layanan sebagaimana dilihat oleh pemangku kepentingan internal dan eksternal. Ex2 : Menentukan (misalnya, dari analisis dampak bisnis) aset dan operasi bisnis yang penting untuk mencapai tujuan misi dan dampak potensial dari kerugian (atau kerugian sebagian) dari operasi tersebut. Ex3 : Menetapkan dan mengomunikasikan tujuan ketahanan (misalnya, tujuan waktu pemulihan) untuk memberikan kemampuan dan layanan penting dalam berbagai kondisi operasi (misalnya, saat diserang, selama pemulihan, operasi normal)

	GV.SC-04: Pemasok diketahui dan diprioritaskan berdasarkan kekritisannya	Ex1 : Mengembangkan kriteria untuk kekritisan pemasok berdasarkan, misalnya, sensitivitas data yang diproses atau dimiliki oleh pemasok, tingkat akses ke sistem organisasi, dan pentingnya produk atau layanan terhadap misi organisasi. Ex2 : Mencatat semua pemasok, dan memprioritaskan pemasok berdasarkan kriteria kekritisan
RA-10: Perburuan Ancaman	DE.AE-06: Informasi tentang kejadian buruk diberikan kepada staf dan alat yang berwenang	Ex1 : Menggunakan perangkat lunak keamanan siber untuk membuat peringatan dan memberikannya ke pusat operasi keamanan (SOC), penanggap insiden, dan alat respons insiden. Ex2 : Penanggap insiden dan personel berwenang lainnya dapat mengakses temuan analisis log setiap saat Ex3 : Secara otomatis membuat dan menetapkan tiket di sistem tiket organisasi ketika jenis peringatan tertentu terjadi Ex4 : Membuat dan menetapkan tiket secara manual di sistem tiket organisasi ketika staf teknis menemukan indikator kompromi
	DE.AE-07: Intelijen ancaman siber dan informasi kontekstual lainnya diintegrasikan ke dalam analisis	Ex1 : Menyediakan umpan intelijen ancaman cyber secara aman ke teknologi deteksi, proses, dan personel Ex2 : Menyediakan informasi dari inventaris aset ke teknologi deteksi, proses, dan personel secara aman Ex3 : Memperoleh dan menganalisis pengungkapan kerentanan secara cepat untuk teknologi organisasi dari pemasok, vendor, dan penasihat keamanan pihak ketiga

Lampiran 3

KATEGORI (RA)	FUNGSI SESUAI NIST	PERTANYAAN KUESIONER	RATA-RATA SKOR (1-5)	RESPONDEN
RA-1: Kebijakan dan Prosedur	GV.OC-03: Persyaratan hukum, peraturan, dan kontraktual mengenai keamanan siber – termasuk kewajiban privasi dan kebebasan sipil – dipahami dan dikelola	Apakah kampus memahami dan mengikuti aturan hukum dan kontrak yang berhubungan dengan keamanan data dan privasi?	4,00	IT
	GV.PO-01: Kebijakan untuk mengelola risiko keamanan siber ditetapkan berdasarkan konteks organisasi, strategi dan prioritas keamanan siber dan dikomunikasikan dan ditegakkan	Apakah kampus sudah memiliki kebijakan tertulis untuk mengelola risiko keamanan siber, dan apakah kebijakan itu sudah disosialisasikan serta diperbarui secara rutin?	3,33	IT
	GV.OV-01: Hasil strategi manajemen risiko keamanan siber ditinjau untuk menginformasikan dan menyesuaikan strategi dan arah	Apakah hasil evaluasi keamanan siber digunakan untuk memperbaiki strategi dan arah kebijakan kampus?	3,67	IT
	GV.SC-03: Manajemen risiko rantai pasokan keamanan siber diintegrasikan ke	Apakah kampus menilai dan mengelola risiko	3,33	IT

	dalam manajemen risiko siber dan perusahaan, penilaian risiko, dan proses perbaikan	keamanan dari pihak luar (seperti vendor atau penyedia layanan), termasuk setelah kerja sama selesai?		
	ID.IM-01: Perbaikan diidentifikasi dari evaluasi	Apakah kampus secara rutin mencari hal-hal yang bisa diperbaiki dari evaluasi dan pelaksanaan operasional keamanan siber?	3,67	IT
RA-2: Kategorisasi Keamanan	ID.AM-05: Aset diprioritaskan berdasarkan klasifikasi, kekritisan, sumber daya, dan dampak pada misi	Apakah kampus bisa menentukan mana aset atau sistem yang paling penting dan butuh perlindungan lebih?	3,79	DOSEN & MHS
	ID.RA-04: Dampak potensial dan kemungkinan ancaman yang mengeksploitasi kerentanan diidentifikasi dan dicatat	Apakah kampus mencatat ancaman dan kelemahan yang mungkin terjadi dan dampaknya terhadap sistem yang ada?	3,33	IT
	ID.RA-05: Ancaman, kerentanan, kemungkinan, dan dampak digunakan untuk memahami risiko inheren dan menginformasika	Apakah kampus menggunakan informasi ancaman, kelemahan, dan dampaknya untuk	4,33	IT

	n prioritas respons risiko.	menentukan prioritas dalam mengurangi risiko?		
RA-3: Penilaian Risiko	GV.RM-06: Metode standar untuk menghitung, mendokumentasikan, mengkategorikan, dan memprioritaskan risiko keamanan siber ditetapkan dan dikomunikasikan	Apakah kampus memiliki cara yang jelas dan standar untuk mengukur serta menentukan tingkat risiko keamanan siber?	4,67	IT
	GV.SC-10: Rencana manajemen risiko rantai pasokan keamanan siber mencakup ketentuan untuk aktivitas yang terjadi setelah berakhirnya kemitraan atau perjanjian layanan.	Apakah keamanan dari pemasok atau vendor dipantau sepanjang kerja sama dan setelahnya?	3,83	DOSEN & MHS
	ID.RA-01: Kerentanan dalam aset diidentifikasi, divalidasi, dan dicatat	Apakah kampus secara rutin memeriksa dan mencatat kelemahan pada sistem yang digunakan?	4,00	IT
	DE.AE-07: Intelijen ancaman siber dan informasi kontekstual lainnya diintegrasikan ke dalam analisis	Apakah kampus menggunakan informasi dari luar tentang ancaman siber untuk menganalisis dan	4,00	IT

		meningkatkan keamanannya?		
	RS.AN-08: Besarnya insiden diperkirakan dan divalidasi	Apakah kampus rutin menilai seberapa besar dampak dari insiden keamanan yang mungkin terjadi?	4,00	IT
	ID.RA-08: Proses untuk menerima, menganalisis, dan menanggapi pengungkapan kerentanan ditetapkan	Apakah kampus memiliki prosedur untuk menerima dan menangani laporan kelemahan sistem dari pihak lain?	3,67	IT
RA-7: Respon Risiko	GV.OC-05: Hasil, kemampuan, dan layanan yang diandalkan oleh organisasi dipahami dan dikomunikasikan	Apakah kampus mengetahui dan menyampaikan dengan jelas layanan penting yang harus terus berjalan untuk mendukung tujuan kampus?	3,82	DOSEN & MHS
	GV.RM-01: Tujuan manajemen risiko ditetapkan dan disetujui oleh pemangku kepentingan organisasi	Apakah kampus memiliki tujuan pengelolaan risiko keamanan yang jelas dan disetujui oleh pihak terkait?	3,78	DOSEN & MHS

	GV.RM-03: Aktivitas dan hasil manajemen risiko keamanan siber dimasukkan dalam proses manajemen risiko perusahaan	Apakah kegiatan dan hasil dari pengelolaan risiko siber ikut dimasukkan dalam perencanaan risiko kampus secara keseluruhan?	3,67	IT
	GV.OV-03: Kinerja manajemen risiko keamanan siber organisasi dievaluasi dan ditinjau untuk penyesuaian yang diperlukan	Apakah performa pengelolaan risiko keamanan siber dievaluasi secara rutin untuk perbaikan?	4,33	IT
	ID.RA-06: Respon risiko dipilih, diprioritaskan, direncanakan, dilacak, dan dikomunikasikan	Apakah kampus memiliki cara yang jelas untuk menangani risiko keamanan siber dan menyampaikan tindakannya kepada pihak terkait?	4,67	IT
RA-9: Analisis Kekritisan	GV.OC-04: Sasaran, kemampuan, dan layanan penting yang diandalkan atau diharapkan oleh pemangku kepentingan dari organisasi dipahami dan dikomunikasikan	Apakah kampus bisa menentukan mana pemasok atau vendor yang paling baik dan dapat mengatasi risiko keamanan kampus?	3,77	DOSEN & MHS

RA-10: Perburuan Ancaman	DE.AE-06: Informasi tentang kejadian buruk diberikan kepada staf dan alat yang berwenang	Apakah kampus memiliki prosedur agar informasi tentang insiden keamanan disampaikan ke staf dan pihak berwenang tepat waktu?	4,00	IT

Nama	Responden	Apakah kampus bisa menentukan mana aset atau sistem yang paling penting dan butuh perlindungan lebih?	Apakah keamanan dari pemasok atau vendor dipantau sepanjang kerja sama dan setelahnya?	Apakah kampus mengetahui dan menyampaikan dengan jelas layanan penting yang harus terus berjalan untuk mendukung tujuan kampus?	Apakah kampus memiliki tujuan pengelolaan risiko keamanan yang jelas dan disetujui oleh pihak terkait?	Apakah kampus bisa menentukan mana pemasok atau vendor yang paling baik dan dapat mengatasi risiko keamanan kampus?
Hidayatin Sholikha	Mahasiswa	Netral	Setuju	Setuju	Setuju	Setuju
Juan Fahmi Ilyasa El Rachman	Mahasiswa	Sangat Setuju	Sangat Setuju	Sangat Setuju	Sangat Setuju	Sangat Setuju
Dewi	Mahasiswa	Setuju	Setuju	Setuju	Netral	Netral
Fatihah Farah Dhiya'	Mahasiswa	Sangat Setuju	Sangat Setuju	Sangat Setuju	Sangat Setuju	Sangat Setuju
AMMAR AL GHAZY	Mahasiswa	Sangat Tidak Setuju	Sangat Tidak Setuju	Tidak Setuju	Sangat Setuju	Sangat Setuju
Iqbal p	Mahasiswa	Setuju	Netral	Setuju	Setuju	Setuju
Muhammad wildan arafif	Mahasiswa	Setuju	Setuju	Setuju	Setuju	Setuju
dhea nur savira	Mahasiswa	Setuju	Setuju	Setuju	Setuju	Setuju
Nely	Mahasiswa	Netral	Netral	Netral	Netral	Netral
Enik	Mahasiswa	Setuju	Setuju	Setuju	Netral	Netral
ck	Mahasiswa	Netral	Setuju	Setuju	Netral	Setuju
Ob	Mahasiswa	Netral	Netral	Setuju	Netral	Sangat Setuju
Nopal	Mahasiswa	Setuju	Netral	Setuju	Setuju	Setuju

Muhammad Ridho Jundiansyah	Mahasiswa	Tidak Setuju	Tidak Setuju	Tidak Setuju	Tidak Setuju	Tidak Setuju
A. Farid Susanto	Mahasiswa	Setuju	Setuju	Sangat Setuju	Sangat Setuju	Setuju
ahmad fatkhul mubin	Mahasiswa	Setuju	Setuju	Setuju	Sangat Tidak Setuju	Sangat Tidak Setuju
Azra Maulana Firmansyah	Mahasiswa	Sangat Setuju	Sangat Setuju	Sangat Setuju	Sangat Setuju	Sangat Setuju
Miftakhul Khasanah	Mahasiswa	Sangat Setuju	Sangat Setuju	Sangat Setuju	Setuju	Setuju
ayu	Mahasiswa	Setuju	Setuju	Sangat Setuju	Setuju	Setuju
Imam Hanafi	Mahasiswa	Setuju	Setuju	Setuju	Setuju	Setuju
Tsalits Wildan Hamid	Mahasiswa	Sangat Setuju	Sangat Setuju	Setuju	Netral	Setuju
Fadilla Fairozun Ni'mah	Mahasiswa	Setuju	Setuju	Setuju	Setuju	Setuju
Bagus Dwi Jauhari	Mahasiswa	Netral	Netral	Netral	Netral	Netral
Aurora Sabrina Elhawa	Mahasiswa	Netral	Setuju	Netral	Setuju	Setuju
Hamka Lukmanul	Mahasiswa	Netral	Setuju	Netral	Netral	Netral

Hakim Adhani						
M. Cita Prasetya Agam	Mahasiswa	Setuju	Setuju	Setuju	Setuju	Setuju
Zufar Faiil Haq	Mahasiswa	Sangat Setuju	Sangat Setuju	Sangat Setuju	Setuju	Sangat Setuju
Dimas surya	Mahasiswa	Setuju	Netral	Netral	Setuju	Sangat Setuju
Ahmad Abdullah Fahmi	Mahasiswa	Setuju	Netral	Netral	Netral	Netral
Heri Ardiansyah	Dosen	Netral	Netral	Netral	Netral	Netral
Gelora habibie wicaksono	Mahasiswa	Setuju	Setuju	Setuju	Setuju	Setuju
Nia Putri	Mahasiswa	Netral	Netral	Netral	Netral	Netral
alif rachman rasyid	Mahasiswa	Sangat Setuju	Tidak Setuju	Setuju	Tidak Setuju	Netral
Abdul Muiz	Mahasiswa	Sangat Setuju	Sangat Setuju	Sangat Setuju	Sangat Setuju	Sangat Setuju
M. Kamal Al Ibad	Mahasiswa	Setuju	Setuju	Setuju	Setuju	Setuju
Angga Risdianto Wijaya Putra	Mahasiswa	Setuju	Setuju	Netral	Setuju	Setuju
DinorA	Mahasiswa	Setuju	Setuju	Netral	Setuju	Setuju
Fiqrul Labib Abdullah	Mahasiswa	Setuju	Netral	Setuju	Setuju	Setuju

Fachdiya Risfi Adriyani	Mahasiswa	Netral	Setuju	Netral	Netral	Netral
tiyas	Mahasiswa	Netral	Netral	Netral	Netral	Netral
mohammad izzul haq putra	Mahasiswa	Setuju	Setuju	Netral	Setuju	Netral
nila dwi noor rositah	Mahasiswa	Setuju	Setuju	Setuju	Setuju	Setuju
Mutsna Sa Yu Zakka	Mahasiswa	Netral	Setuju	Tidak Setuju	Tidak Setuju	Netral
Ahmad lathif aditya	Mahasiswa	Setuju	Setuju	Setuju	Setuju	Setuju
Muhammad Rifqi syafik	Mahasiswa	Netral	Netral	Netral	Netral	Netral
Mada Mercylina	Mahasiswa	Sangat Setuju	Setuju	Sangat Setuju	Setuju	Sangat Setuju
Faridhatun Nurfaidah	Mahasiswa	Netral	Netral	Netral	Netral	Netral
syauqi mubarok ilahi	Mahasiswa	Setuju	Setuju	Setuju	Setuju	Setuju
ryan	Dosen	Sangat Setuju	Sangat Setuju	Setuju	Sangat Setuju	Setuju
Ayu Fidayanti	Mahasiswa	Netral	Setuju	Netral	Setuju	Netral
Riza Nur Fitriani	Mahasiswa	Setuju	Setuju	Setuju	Setuju	Setuju
Dwi putra	Mahasiswa	Netral	Setuju	Setuju	Setuju	Netral

alvinsyah						
Muhammad Boby Bachtiar Putra	Mahasiswa	Netral	Netral	Netral	Netral	Netral
Rohmatul Badiyah	Mahasiswa	Netral	Setuju	Netral	Sangat Setuju	Setuju

Responden: Bayu Anugrah (Staff IT)

Pertanyaan	Jawaban
Apakah kampus memahami dan mengikuti aturan hukum dan kontrak yang berhubungan dengan keamanan data dan privasi?	Sangat Setuju
Apakah kampus sudah memiliki kebijakan tertulis untuk mengelola risiko keamanan siber, dan apakah kebijakan itu sudah disosialisasikan serta diperbarui secara rutin?	Setuju
Apakah hasil evaluasi keamanan siber digunakan untuk memperbaiki strategi dan arah kebijakan kampus?	Sangat Setuju
Apakah kampus menilai dan mengelola risiko keamanan dari pihak luar (seperti vendor atau penyedia layanan), termasuk setelah kerja sama selesai?	Setuju
Apakah kampus secara rutin mencari hal-hal yang bisa diperbaiki dari evaluasi dan pelaksanaan operasional keamanan siber?	Setuju
Apakah kampus mencatat ancaman dan kelemahan yang mungkin terjadi dan dampaknya terhadap sistem yang ada?	Setuju
Apakah kampus menggunakan informasi ancaman, kelemahan, dan dampaknya untuk menentukan prioritas dalam mengurangi risiko?	Setuju
Apakah kampus memiliki cara yang jelas dan standar untuk mengukur serta menentukan tingkat risiko keamanan siber?	Setuju
Apakah kampus secara rutin memeriksa dan mencatat kelemahan pada sistem yang digunakan?	Setuju
Apakah kampus menggunakan informasi dari luar tentang ancaman siber untuk menganalisis dan meningkatkan keamanannya?	Netral
Apakah kampus rutin menilai seberapa besar dampak dari insiden keamanan yang mungkin terjadi?	Setuju
Apakah kampus memiliki prosedur untuk menerima dan menangani laporan kelemahan sistem dari pihak lain?	Setuju
Apakah kegiatan dan hasil dari pengelolaan risiko siber ikut dimasukkan dalam perancanangan risiko kampus secara keseluruhan?	Netral
Apakah performa pengelolaan risiko keamanan siber dievaluasi secara rutin untuk perbaikan?	Setuju
Apakah kampus memiliki cara yang jelas untuk menangani risiko keamanan siber dan menyampaikan tindakannya kepada pihak terkait?	Setuju

Apakah kampus memiliki prosedur agar informasi tentang insiden keamanan disampaikan ke staf dan pihak berwenang tepat waktu?	Setuju

Responden: M. Nurul Ihsan (Staff IT)

Pertanyaan	Jawaban
Apakah kampus memahami dan mengikuti aturan hukum dan kontrak yang berhubungan dengan keamanan data dan privasi?	Sangat Setuju
Apakah kampus sudah memiliki kebijakan tertulis untuk mengelola risiko keamanan siber, dan apakah kebijakan itu sudah disosialisasikan serta diperbarui secara rutin?	Sangat Setuju
Apakah hasil evaluasi keamanan siber digunakan untuk memperbaiki strategi dan arah kebijakan kampus?	Sangat Setuju
Apakah kampus menilai dan mengelola risiko keamanan dari pihak luar (seperti vendor atau penyedia layanan), termasuk setelah kerja sama selesai?	Sangat Setuju
Apakah kampus secara rutin mencari hal-hal yang bisa diperbaiki dari evaluasi dan pelaksanaan operasional keamanan siber?	Sangat Setuju
Apakah kampus mencatat ancaman dan kelemahan yang mungkin terjadi dan dampaknya terhadap sistem yang ada?	Sangat Setuju
Apakah kampus menggunakan informasi ancaman, kelemahan, dan dampaknya untuk menentukan prioritas dalam mengurangi risiko?	Sangat Setuju
Apakah kampus memiliki cara yang jelas dan standar untuk mengukur serta menentukan tingkat risiko keamanan siber?	Sangat Setuju
Apakah kampus secara rutin memeriksa dan mencatat kelemahan pada sistem yang digunakan?	Sangat Setuju
Apakah kampus menggunakan informasi dari luar tentang ancaman siber untuk menganalisis dan meningkatkan keamanannya?	Sangat Setuju
Apakah kampus rutin menilai seberapa besar dampak dari insiden keamanan yang mungkin terjadi?	Sangat Setuju
Apakah kampus memiliki prosedur untuk menerima dan menangani laporan kelemahan sistem dari pihak lain?	Sangat Setuju
Apakah kegiatan dan hasil dari pengelolaan risiko siber ikut dimasukkan dalam perancanangan risiko kampus	Sangat Setuju

secara keseluruhan?	
Apakah performa pengelolaan risiko keamanan siber dievaluasi secara rutin untuk perbaikan?	Sangat Setuju
Apakah kampus memiliki cara yang jelas untuk menangani risiko keamanan siber dan menyampaikan tindakannya kepada pihak terkait?	Sangat Setuju
Apakah kampus memiliki prosedur agar informasi tentang insiden keamanan disampaikan ke staf dan pihak berwenang tepat waktu?	Sangat Setuju

Responden: Moch Fattahur Razzaq (Staff IT)

Pertanyaan	Jawaban
Apakah kampus memahami dan mengikuti aturan hukum dan kontrak yang berhubungan dengan keamanan data dan privasi?	Tidak Setuju
Apakah kampus sudah memiliki kebijakan tertulis untuk mengelola risiko keamanan siber, dan apakah kebijakan itu sudah disosialisasikan serta diperbarui secara rutin?	Sangat Tidak Setuju
Apakah hasil evaluasi keamanan siber digunakan untuk memperbaiki strategi dan arah kebijakan kampus?	Sangat Tidak Setuju
Apakah kampus menilai dan mengelola risiko keamanan dari pihak luar (seperti vendor atau penyedia layanan), termasuk setelah kerja sama selesai?	Sangat Tidak Setuju
Apakah kampus secara rutin mencari hal-hal yang bisa diperbaiki dari evaluasi dan pelaksanaan operasional keamanan siber?	Tidak Setuju
Apakah kampus mencatat ancaman dan kelemahan yang mungkin terjadi dan dampaknya terhadap sistem yang ada?	Sangat Tidak Setuju
Apakah kampus menggunakan informasi ancaman, kelemahan, dan dampaknya untuk menentukan prioritas dalam mengurangi risiko?	Setuju
Apakah kampus memiliki cara yang jelas dan standar untuk mengukur serta menentukan tingkat risiko keamanan siber?	Sangat Setuju
Apakah kampus secara rutin memeriksa dan mencatat kelemahan pada sistem yang digunakan?	Netral

Apakah kampus menggunakan informasi dari luar tentang ancaman siber untuk menganalisis dan meningkatkan keamanannya?	Setuju
Apakah kampus rutin menilai seberapa besar dampak dari insiden keamanan yang mungkin terjadi?	Tidak Setuju, Setuju
Apakah kampus memiliki prosedur untuk menerima dan menangani laporan kelemahan sistem dari pihak lain?	Tidak Setuju
Apakah kegiatan dan hasil dari pengelolaan risiko siber ikut dimasukkan dalam perancanangan risiko kampus secara keseluruhan?	Netral
Apakah performa pengelolaan risiko keamanan siber dievaluasi secara rutin untuk perbaikan?	Setuju
Apakah kampus memiliki cara yang jelas untuk menangani risiko keamanan siber dan menyampaikan tindakannya kepada pihak terkait?	Sangat Setuju
Apakah kampus memiliki prosedur agar informasi tentang insiden keamanan disampaikan ke staf dan pihak berwenang tepat waktu?	Netral