

PENGUMUMAN REQUEST FOR INFORMATION (RFI)

Bank Indonesia akan mengadakan Pengadaan dan Pemeliharaan *Software Composition Analysis* sebagai Pengembangan *Application Security Testing* di Bank Indonesia Tahun 2026, dengan ketentuan sebagai berikut:

1. Ruang Lingkup Pekerjaan meliputi:

- a. Melakukan penyediaan *subscription* dengan rincian sebagaimana Lampiran 1.
- b. Melakukan implementasi dengan rincian sebagaimana Lampiran 2.
- c. Melakukan pemeliharaan dengan rincian sebagaimana Lampiran 3.

2. Metode Kerja:

Sebagaimana Lampiran 4.

3. Persyaratan Calon Peserta Pengadaan terdiri dari:

- a. Peserta adalah rekanan Bank Indonesia yang terdaftar pada aplikasi *e-Procurement* dan dalam hal memiliki historis kontrak dengan Bank Indonesia peserta memiliki kinerja secara umum mayoritas baik pada akhir tahun kontrak periode September 2024 sampai dengan September 2026.
- b. Merupakan Perusahaan yang berstatus badan hukum "Perseroan Terbatas" (PT).
- c. Merupakan *business partner* dari Prinsipal OpenText.
- d. Memiliki surat dukungan sebagai *partner* untuk melaksanakan pekerjaan ini yang diterbitkan oleh Prinsipal OpenText.
- e. Memiliki pengalaman dalam melakukan penyediaan *subscription*, implementasi dan pemeliharaan solusi *Software Composition Analysis* (dapat dari beberapa kontrak) paling kurang 1 (satu) pekerjaan pada Juli 2023 s.d Juli 2026 yang dibuktikan dengan bukti kontrak/SPK/PO/SPPP.
- f. Memiliki surat keterangan dari Prinsipal OpenText bahwa *subscription* yang diimplementasikan masih di-*support* selama jangka waktu pelaksanaan pekerjaan.
- g. Merupakan perusahaan yang mempunyai sertifikasi KADIN dengan salah satu klasifikasi sebagai berikut:

Kode	Klasifikasi	Kualifikasi
30011	Alat/peralatan/suku cadang: komputer	Menengah
30501	Teknologi informasi	Menengah
20501	Jasa Teknologi Informasi	Menengah

- h. Memiliki tenaga ahli dengan rincian sebagaimana Lampiran 5.
- i. Menyampaikan surat pernyataan untuk mengikuti pengadaan ini.
 - 1) Perusahaan tidak dinyatakan pailit melalui suatu keputusan pengadilan;
 - 2) Kegiatan usaha perusahaan tidak sedang dihentikan sementara;
 - 3) Orang yang mewakili badan usaha tidak sedang menjalani sanksi pidana dan secara hukum mempunyai kapasitas menandatangani kontrak;

- 4) Memiliki sumber daya manusia, modal, peralatan, dan fasilitas lain yang diperlukan dalam pelaksanaan penyediaan barang dan/atau jasa;
 - 5) Perusahaan tidak sedang dikenakan sanksi oleh Bank Indonesia terkait dengan pelaksanaan Pengadaan sebelumnya di Bank Indonesia;
 - 6) Tidak memiliki hubungan afiliasi dengan peserta lain yang ikut pada pengadaan ini dalam bentuk kesamaan pengurusan dan kepemilikan;
 - 7) Seluruh dokumen yang disampaikan dan/atau diunggah pada aplikasi E-Procurement adalah benar dan merupakan copy dokumen asli.
- j. Memiliki laporan keuangan tahun 2025 yang telah diaudit oleh Kantor Akuntan Publik (KAP) dengan opini minimal wajar dengan pengecualian.
- k. Telah memenuhi kewajiban perpajakan tahun 2025 dengan menyampaikan paling kurang bukti penerimaan yang diterbitkan oleh Dirjen Pajak (DJP) atas pelaporan Surat Pemberitahuan (SPT).

Apabila terdapat perusahaan yang berminat untuk mengikuti pengadaan, maka untuk informasi lebih lanjut dapat menghubungi Bank Indonesia melalui e-mail ahmad_yr@bi.go.id dan rizki_a.i@bi.go.id dengan batas waktu penyampaian RFI ditetapkan mulai tanggal 31 Agustus 2026 sampai dengan 4 September 2026.

Komitmen Integritas

1. Bank Indonesia menjunjung tinggi proses pengadaan yang bersih, bebas dari Korupsi, Kolusi, dan Nepotisme serta pemberitan gratifikasi.
2. Proses pengadaan di Bank Indonesia tidak dipungut biaya apapun.
3. Dalam hal terdapat hal-hal yang bertentangan dengan hal-hal tersebut di atas, harap segera laporkan melalui *whistleblowing system* Bank Indonesia melalui https://www.bi.go.id/wbsbi/add_wbs2.aspx.

Pelaksanaan RFI bukan merupakan bagian dalam proses pengadaan, sehingga Perusahaan yang menyampaikan dokumen pada pelaksanaan RFI tidak serta merta memenuhi prakualifikasi pengadaan ini. Perusahaan baru dapat dinyatakan memenuhi prakualifikasi apabila mendaftar menjadi peserta dan dinyatakan memenuhi kriteria pada proses pengadaan yang dilakukan oleh Bank Indonesia kemudian.

**Divisi *Advisory* dan Persiapan Pengadaan Barang dan
Jasa Strategis dan Kritisal
DEPARTEMEN MANAJEMEN DAN ADVISORY
PENGADAAN**

LAMPIRAN 1. SPESIFIKASI TEKNIS

No.	Product Code	Item Description	Term (Year)	Qty
1	SB-AF124	Fortify Sonatype OEM - Subscription - Fortify Sonatype Lifecycle 1 User Subscription SW E-LTU	2	10
2	SB-AD962	Fortify Sonatype Resell - Subscription-Sonatype - Nexus Repository per User Subscription SW E-LTU	2	10
3	SB-AD963	Fortify Sonatype Resell - Subscription-Sonatype - Firewall Users Subscription SW E-LTU	2	10

LAMPIRAN 2. RUANG LINGKUP IMPLEMENTASI

Ruang lingkup pelaksanaan implementasi adalah sebagai berikut:

1. Lingkup Umum Pekerjaan Implementasi

Rincian lingkup umum adalah sebagai berikut:

- a. Pelaksanaan implementasi dilakukan untuk lingkungan pengembangan aplikasi, sesuai kebutuhan dan kesepakatan dengan Bank Indonesia.
- b. Melakukan instalasi, konfigurasi, dan aktivasi solusi Software Composition Analysis (SCA) yang mencakup kapabilitas analisis komponen perangkat lunak/*open source*, pengelolaan repositori, serta pengamanan penggunaan komponen perangkat lunak pihak ketiga.
- c. Melakukan integrasi solusi SCA dengan sistem *Application Security Testing* eksisting dan ekosistem pengembangan aplikasi Bank Indonesia, termasuk namun tidak terbatas pada *source code repository*, *CI/CD pipeline*, *build tools*, *artifact repository*, serta sistem atau infrastruktur pendukung lainnya yang relevan.
- d. Melakukan pengujian sistem untuk memastikan solusi SCA telah berfungsi dengan kriteria sebagai berikut:

No	Pengujian	Hasil
1.	Tes Fungsionalitas & <i>Health Check</i>	Solusi SCA, Repository Management, dan Firewall berstatus aktif, dapat diakses oleh pengguna yang berwenang, serta beroperasi normal sesuai konfigurasi yang telah disepakati.
2.	Tes Identifikasi Komponen <i>Open Source</i>	Sistem berhasil mengidentifikasi komponen perangkat lunak, termasuk dependensi/dependencies, pustaka/library, paket/package, serta repositori perangkat lunak/software repository yang digunakan dalam proses pengembangan aplikasi.
3.	Tes Deteksi Kerentanan dan/atau Risiko Lisensi	Sistem berhasil mendeteksi kerentanan keamanan, versi komponen yang tidak aman atau tidak lagi didukung, dan/atau potensi risiko lisensi pada komponen perangkat lunak yang digunakan.
4.	Tes <i>Policy Enforcement</i> dan <i>Blocking</i>	Sistem berhasil menerapkan kebijakan keamanan yang disepakati, termasuk memberikan peringatan, rekomendasi perbaikan, atau melakukan pemblokiran terhadap komponen yang memiliki risiko tinggi sesuai <i>policy</i> yang ditetapkan.
5.	Tes Integrasi dengan <i>CI/CD</i> dan <i>Repository</i>	Sistem berhasil terintegrasi dengan <i>pipeline</i> pengembangan dan repositori yang digunakan, sehingga proses analisis komponen dapat dilakukan secara otomatis dalam tahapan pengembangan aplikasi.

- e. Menyusun dokumen pelaksanaan pekerjaan implementasi.

2. Teknis Kegiatan Implementasi

Teknis kegiatan implementasi adalah sebagai berikut:

- 1) Melakukan *assessment* terhadap proses pengembangan aplikasi, ekosistem DevSecOps, *source code repository*, *dependency management*, *artifact repository*, serta pipeline *CI/CD* yang digunakan di Bank Indonesia untuk menentukan arsitektur dan strategi implementasi solusi SCA yang optimal.
- 2) Menyusun rencana dan jadwal implementasi berdasarkan hasil *assessment* yang telah disepakati dengan Bank Indonesia.

- 3) Melakukan instalasi, aktivasi, dan konfigurasi solusi *Software Composition Analysis*, termasuk pengaturan pengguna, role, hak akses, organisasi/proyek aplikasi, serta parameter keamanan yang diperlukan.
- 4) Melakukan konfigurasi Sonatype Lifecycle atau kapabilitas sejenis untuk melakukan analisis terhadap komponen *open source*, identifikasi kerentanan keamanan, risiko lisensi, kualitas komponen, dan rekomendasi mitigasi.
- 5) Melakukan konfigurasi Nexus Repository atau *repository management* untuk mendukung pengelolaan komponen, *package*, *library*, dan *artifact* yang digunakan dalam proses pengembangan aplikasi.
- 6) Melakukan konfigurasi Sonatype Firewall atau kapabilitas sejenis untuk mencegah penggunaan komponen perangkat lunak yang berisiko tinggi sejak tahap awal pengunduhan atau penggunaan dependensi dalam proses pengembangan.
- 7) Melakukan integrasi solusi SCA dengan *tools* pengembangan aplikasi yang digunakan Bank Indonesia, termasuk *source code management*, *CI/CD pipeline*, atau sesuai dengan kesepakatan dengan Bank Indonesia.
- 8) Menyusun dan menerapkan kebijakan keamanan komponen perangkat lunak berdasarkan tingkat risiko, antara lain kerentanan keamanan, tingkat keparahan *vulnerability*, status versi komponen, reputasi komponen, risiko lisensi atau sesuai dengan kesepakatan dengan Bank Indonesia.
- 9) Melakukan pengujian fungsi deteksi, analisis, notifikasi, *reporting*, serta *enforcement policy* untuk memastikan solusi dapat membantu tim pengembang dan tim keamanan dalam mengidentifikasi serta menangani risiko komponen perangkat lunak secara proaktif.
- 10) Melaksanakan *User Acceptance Test* (UAT) bersama unit kerja terkait di Bank Indonesia untuk memastikan seluruh fungsi utama solusi berjalan sesuai kebutuhan dan kriteria keberhasilan yang telah disepakati.
- 11) Memberikan *knowledge transfer* yang komprehensif kepada tim terkait di Bank Indonesia, termasuk tim pengembang aplikasi, DevSecOps, operasional, dan administrator keamanan, terkait penggunaan solusi, pembacaan hasil analisis, pengelolaan *policy*, penanganan temuan, serta mekanisme pelaporan.
- 12) Memastikan seluruh konfigurasi mematuhi standar keamanan informasi Bank Indonesia, termasuk prinsip *least privilege*, pengelolaan akses berbasis peran, *hardening* konfigurasi, serta ketentuan keamanan lain yang berlaku.
- 13) Memastikan seluruh personel yang terlibat dari pihak pelaksana menandatangani *Non-Disclosure Agreement* (NDA) mengingat adanya potensi akses terhadap informasi pengembangan aplikasi, struktur dependensi, repositori, serta data teknis internal Bank Indonesia.
- 14) Menyediakan dukungan teknis selama proses implementasi, pengujian, dan penyelesaian kendala yang muncul sampai solusi dinyatakan dapat digunakan sesuai ruang lingkup pekerjaan.
- 15) Menjaga kebersihan dan ketertiban apabila terdapat aktivitas fisik di lokasi area pekerjaan.

16) Menyusun dan menyerahkan kelengkapan dokumen operasional, meliputi namun tidak terbatas pada:

- a. Dokumen hasil *assessment*;
- b. Dokumen desain implementasi;
- c. Dokumentasi konfigurasi/*as-built configuration*;
- d. Panduan operasional administrator;
- e. Panduan penggunaan untuk tim pengembang;
- f. Panduan pengelolaan *policy*;
- g. Panduan penanganan temuan kerentanan dan risiko lisensi;
- h. Dokumentasi hasil integrasi;
- i. Dokumentasi hasil UAT;
- j. Dokumen *knowledge transfer*

Dokumen kegiatan implementasi disusun dan dicetak rangkap 2 (dua) serta *softcopy* dokumen dapat dikirimkan melalui *email* terlebih dahulu.

LAMPIRAN 3. RUANG LINGKUP PEMELIHARAAN

Ruang lingkup Pekerjaan pemeliharaan meliputi *Preventive Maintenance* (PM), *Corrective Maintenance* (CM) dan Dokumen *Summary Kegiatan* (*Log Book*), dengan uraian sebagai berikut:

1. *Preventive Maintenance* (PM)

PM adalah kegiatan dalam usaha untuk mempertahankan atau menjaga kondisi sistem beroperasi optimal dengan melakukan pemeliharaan dan inspeksi secara berkala setiap 3 (tiga) bulan sekali secara *onsite* di Kantor Pusat Bank Indonesia sesuai dengan jadwal yang ditetapkan dan dibuktikan dengan menyerahkan laporan Pemeliharaan, dengan rincian kegiatan:

a. Melakukan dan membuat laporan kegiatan *health check* dan *assessment* secara berkala terhadap keseluruhan solusi SCA, *repository management*, dan fitur pengamanan komponen perangkat lunak, meliputi:

- 1) *Utility Resource*, mencakup status penggunaan CPU, RAM, disk usage, kapasitas penyimpanan repository, serta resource pendukung lainnya.
- 2) *System Performance*, mencakup kinerja akses aplikasi, proses scanning komponen perangkat lunak, response time sistem, performa repository, serta memastikan tidak terdapat degradasi performa yang berdampak pada proses pengembangan aplikasi.
- 3) *System Availability*, mencakup status ketersediaan layanan, konektivitas antar komponen, status integrasi dengan *source code repository*, *CI/CD pipeline*, atau sistem pendukung lainnya.
- 4) *Security Policy & Analysis Review*, mencakup evaluasi konfigurasi kebijakan/policy, hasil deteksi kerentanan keamanan, risiko lisensi, komponen berisiko tinggi, serta efektivitas mekanisme *enforcement* terhadap penggunaan komponen perangkat lunak/*open source*.
- 5) *Repository Health Check*, mencakup pemeriksaan kondisi *repository*, storage, *cleanup policy*, akses pengguna, hingga potensi penggunaan package/library yang tidak sesuai dengan kebijakan Bank Indonesia.
- 6) *Firewall & Policy Enforcement Check*, mencakup pengecekan fungsi pemblokiran atau peringatan terhadap komponen yang memiliki kerentanan, lisensi tidak sesuai, reputasi buruk, atau tidak memenuhi ketentuan policy yang telah ditetapkan.
- 7) *Vulnerability Database & Component Intelligence Updates*, mencakup pengecekan pembaruan basis data kerentanan, *component intelligence*, *license intelligence*, dan informasi risiko komponen agar proses analisis tetap akurat dan terkini.
- 8) *Patch & Upgrade*, mencakup pelaksanaan *minor patch*, *major upgrade*, pembaruan versi aplikasi, atau pembaruan modul sesuai rekomendasi prinsipal dan persetujuan Bank Indonesia.
- 9) Dokumentasi Inventarisasi, termasuk pencatatan *hostname*, IP Address, URL layanan, versi aplikasi, status *subscription*, jumlah user, daftar integrasi, daftar repository, serta informasi teknis relevan lainnya.

b. Melakukan pencadangan konfigurasi secara berkala sebelum dan sesudah PM untuk memastikan proses pemulihan (*restore*) dapat dilakukan dengan cepat guna meminimalisasi *downtime*.

- c. Menyampaikan informasi terkait perubahan *roadmap* teknologi, pengumuman *End of Life* (EOL), dan *Common Vulnerabilities and Exposures* (CVE) yang berdampak pada versi sistem yang digunakan, beserta rekomendasi mitigasinya.
2. *Corrective Maintenance* (CM)
- CM adalah kegiatan investigasi dan perbaikan untuk mengembalikan kondisi serta fungsi sistem kembali pada keadaan normal berdasarkan:
- a. Hasil pekerjaan PM apabila diketahui adanya kelainan, *error*, atau degradasi performa.
 - b. Laporan insiden atau gangguan pada saat operasional dari Bank Indonesia, meliputi:
 - 1) Melakukan pemeriksaan penyebab gangguan serta melakukan perbaikan/troubleshooting terhadap solusi *SCA*, *repository*, *policy enforcement*, konektivitas, maupun integrasi dengan sistem pengembangan aplikasi.
 - 2) Melakukan koordinasi dan penyampaian informasi perkembangan penanganan (*progress update*) kepada petugas Bank Indonesia secara berkala sampai dengan gangguan dinyatakan selesai.
 - 3) Laporan insiden keamanan atau gangguan operasional (misal: *traffic* sah terblokir / *false positive* masif) dari Bank Indonesia, dengan langkah penanganan:
 - a) Melakukan *troubleshooting* dan investigasi *log* untuk menemukan penyebab utama gangguan (*Root Cause*).
 - b) Instalasi ulang atau upaya-upaya resolusi insiden sistem/solusi dimaksud sesuai tingkat gangguan yang terjadi untuk mengembalikan dan/atau memulihkan kinerja sistem sesuai dengan kebutuhan pada batas waktu sebagaimana didefinisikan dalam *Response Time* dan *Resolution Time* sesuai persetujuan Bank Indonesia.
 - c) Dokumentasi hasil perbaikan dan perubahan konfigurasi yang dilakukan.
 - d) Dokumentasi hasil *Root Cause Analysis* (RCA) beserta rekomendasi dan solusi permanen agar kendala tidak terulang, berikut tindak lanjut pemantauan pasca-perbaikan.
 - c. Apabila Pelaksana Pekerjaan tidak dapat menyelesaikan gangguan, wajib melakukan eskalasi kepada *Support* Prinsipal dan mengawal penyelesaiannya mengacu pada *resolution time*.
 - d. Penyediaan *workaround* atau *hotfix* sementara (apabila *patch* permanen belum tersedia) harus terlebih dahulu mendapatkan izin dan persetujuan dari petugas Bank Indonesia.
 - e. Melakukan usaha preventif berkelanjutan untuk mengurangi kemungkinan timbulnya gangguan berulang.
 - f. Menanggapi laporan gangguan dari Bank Indonesia secara lisan maupun tertulis (email/sistem tiket) sesuai *Service Level Agreement* (SLA) yang dipersyaratkan.
3. Dokumen *summary* kegiatan yang dilakukan selama masa pemeliharaan terdiri dari:
- a. Aktivitas PM setiap 3 (tiga) bulan.
 - b. Aktivitas CM apabila terjadi kendala/gangguan sistem.

- c. Log histori perubahan konfigurasi apabila terjadi modifikasi yang meliputi: aktivasi fitur/fungsi baru, perubahan *policy* kritikal, pembaruan IP Address, dan *upgrade* versi perangkat lunak.

Dokumen disusun dan dicetak dalam rangkap 2 (dua) dan *softcopy* disampaikan setiap 3 (tiga) bulan dan dokumen dapat dikirimkan melalui *email* terlebih dahulu.

LAMPIRAN 4. METODE KERJA

1. Pelaksana Pekerjaan dapat memberikan petunjuk atau saran teknis penggunaan sistem untuk mengatasi kemungkinan terjadinya hambatan dalam pengoperasiannya.
2. Pelaksana Pekerjaan apabila diperlukan oleh Bank Indonesia, dapat diminta bantuannya untuk mendukung dan/atau memberikan konsultasi dalam rangka pengembangan sistem dan aplikasi yang terkait dengan infrastruktur aplikasi.
3. Apabila terjadi keterlambatan dalam Pelaksanaan Pekerjaan, maka akan dikenakan denda sebagai berikut:

a. Pada Tahap Penyediaan *Subscription* dan/atau Implementasi

Apabila jangka waktu pekerjaan penyediaan *subscription* (termasuk penyerahan *subscription confirmation letter* dari Prinsipal) dan/atau implementasi dilampaui tanpa alasan yang dapat diterima oleh Pemberi Tugas, maka Pelaksana Pekerjaan dikenakan denda sebesar 1‰ (satu per mil) dari jumlah biaya penyediaan *subscription* dan implementasi untuk setiap hari keterlambatan, dengan batas maksimum sebesar 5% (lima persen) dari biaya penyediaan *subscription* dan implementasi atau 50 (lima puluh) hari keterlambatan.

b. Pada Tahap Pemeliharaan

Apabila ketentuan pekerjaan pemeliharaan dilampaui tanpa alasan yang dapat diterima oleh Pemberi Tugas, maka Pelaksana Pekerjaan dikenakan sanksi denda keterlambatan sebagai berikut:

1) Pelaksanaan *Preventive Maintenance* (PM)

Apabila jangka waktu pelaksanaan pelaporan PM dilampaui tanpa alasan yang dapat diterima oleh Bank Indonesia, dikenakan denda sebesar 1‰ (satu per mil) dari biaya jasa pemeliharaan per periode untuk setiap hari keterlambatan, dengan batas maksimum sebesar 5% (lima persen) dari biaya jasa pemeliharaan per periode 50 (lima puluh) hari keterlambatan.

2) Pelaksanaan *Corrective Maintenance* (CM)

Apabila jangka waktu penanganan insiden/CM dilampaui tanpa alasan yang dapat diterima, dikenakan denda sebagai berikut:

Komponen SLA	Batas Waktu	Denda
<i>Response Time</i>	>1 jam	2.5% dari harga jasa pemeliharaan per periode.
<i>Resolution Time</i> (RT)	24 jam < RT ≤ 48 jam	2% dari harga jasa pemeliharaan per periode.
	> 48 jam	2 + ((i-1)/2) % dari harga jasa pemeliharaan per periode.

Keterangan:

1. i adalah jumlah hari kalender setelah laporan direspon oleh Pelaksana Pekerjaan, dengan perhitungan i dilakukan pembulatan ke atas.
2. Sebagai contoh:

- Terjadinya gangguan dan laporan telah direspon oleh Pelaksana Pekerjaan pada hari Senin pukul 00.00; dan
- Gangguan diselesaikan pada Rabu pukul 12.15 (60 jam 15 menit setelah laporan direspon oleh Pelaksana Pekerjaan);

Maka cara perhitungan *resolution time* adalah:

- $i = 60 \text{ jam } 15 \text{ menit}$ atau dengan pembulatan ke atas, sehingga nilai $i = 3$;
- $\text{Denda} = (2 + ((3-1)/2))\% \times \text{harga pemeliharaan per termin pembayaran}$.

3. Total nilai maksimal denda keterlambatan untuk seluruh Pekerjaan termasuk *response time* dan *resolution time* adalah 5% (lima persen) dari nilai Total Kontrak.

4. SLA *availability* per bulan adalah 99%. Perhitungan SLA *availability* per bulan untuk pemeliharaan adalah sebagai berikut:

SERVICE LEVEL (SL)	Persentase tingkat pelayanan (operasional) selama 1 bulan
	$\frac{\text{Total jam kerja operasional} - \text{Total jam gangguan}}{\text{Total jam kerja operasional}} \times 100\%$
SERVICE LEVEL RIIL	<i>Service level</i> gangguan yang menjadi tanggung jawab Pelaksana Pekerjaan
RESTITUSI	Potongan pembayaran (dalam %) apabila nilai SL riil berada di bawah komitmen SL dengan rumus di bawah ini:
	$\times \text{biaya jasa pemeliharaan/bulan}$
KOMITMEN SLA	SLA yang dipersyaratkan sesuai tabel persyaratan nilai SLA.

5. Ketentuan Pemberlakuan *Service Level*
 - a. *Downtime* yang menjadi tanggung jawab Pelaksana Pekerjaan (misalnya: salah konfigurasi oleh Pelaksana Pekerjaan, *bug software* yang lambat dieskalasi ke Prinsipal, atau kesalahan operasional oleh Pelaksana Pekerjaan) diperhitungkan sebagai pengurang *availability*.
 - b. *Downtime* tidak diperhitungkan sebagai pengurang *availability* apabila terjadi karena:
 - 1) Pelaksanaan pemeliharaan/perubahan yang direncanakan (*planned maintenance*) dan telah mendapat persetujuan Bank Indonesia.
 - 2) Faktor eksternal dan infrastruktur yang menjadi tanggung jawab Bank Indonesia (misalnya: *Virtual Machine* mati, *storage* penuh dari sisi *host*, gangguan listrik *Data Center*, gangguan jaringan internal yang memutus komunikasi sistem).
 - c. Waktu yang dibutuhkan untuk pengambilan keputusan oleh manajemen Bank Indonesia apabila terjadi *downtime* tidak diperhitungkan sebagai faktor pengurangan *availability* maupun *resolution time*.
 - d. Dalam hal pekerjaan CM tidak dapat diselesaikan dalam waktu SLA, dan/atau menunggu ketersediaan *patch* resmi (RCA) dari Prinsipal yang membutuhkan waktu lebih lama, Pelaksana Pekerjaan wajib menyampaikan status *update* dan menyediakan solusi sementara (*workaround*) agar layanan tetap berjalan.

Pelanggaran SLA ditetapkan oleh Bank Indonesia berdasarkan hasil evaluasi *log* sistem dan laporan insiden yang disepakati bersama dengan Pelaksana Pekerjaan.

LAMPIRAN 5. SPESIFIKASI TENAGA AHLI

Kegiatan	Fungsi	Minimal Kualifikasi	Jumlah	Peran dan Tugas
Implementasi	<i>Project Manager</i>	- S1 - Pengalaman sebagai <i>project manager</i> minimal 5 (lima) tahun. - Memiliki sertifikasi Project Management Professional (PMP) atau <i>Prince 2</i>.	1	- Monitoring Pelaksanaan Implementasi. - Evaluasi Kesesuaian dan Penandatanganan Laporan. - Evaluasi Kesesuaian dan Penandatanganan BAP, BAK dan BAST
	<i>Technical Leader</i>	- S1 - Pengalaman minimal 5 (lima) tahun sebagai <i>Technical Leader</i>. - Memiliki pengalaman implementasi solusi SCA Sonatype minimal 2 (dua) kali dalam 5 (lima) tahun terakhir. - Memiliki sertifikat pelatihan (<i>training completion</i>) dari Prinsipal terkait produk SCA yang ditawarkan, dan/atau sertifikasi profesional lain di bidang keamanan aplikasi/DevSecOps yang masih berlaku.	1	- Melakukan kegiatan implementasi dan konfigurasi - Dokumentasi instalasi, konfigurasi dan testing uji coba
	<i>Technical Engineer</i>	- S1 - Pengalaman minimal 3 (tiga) tahun sebagai <i>Security Engineer/Technical Engineer</i>. - Memiliki pengalaman implementasi solusi SCA Sonatype 1 (satu) kali dalam 3 (tiga) tahun terakhir. - Memiliki sertifikat pelatihan (<i>training completion</i>) dari Prinsipal terkait produk SCA yang ditawarkan, dan/atau sertifikasi profesional lain di bidang keamanan aplikasi/DevSecOps yang masih berlaku.	1	- Melakukan kegiatan implementasi dan konfigurasi - Dokumentasi instalasi, konfigurasi dan testing uji coba
	<i>Technical Writer</i>	- S1 - Pengalaman minimal 3 (tiga) tahun dalam bidang administrasi proyek.	1	- Menyiapkan Laporan - Menyiapkan BAP, BAK, dan BAST - Menyiapkan Tagihan Pembayaran

Pemeliharaan	<i>Technical Leader</i>	• S1 • Pengalaman minimal 5 (lima) tahun sebagai <i>Technical Leader</i>. • Memiliki pengalaman Implementasi dan/atau pemeliharaan SCA Sonatype minimal 2 (dua) kali dalam 5 (lima) tahun terakhir. • Memiliki sertifikat pelatihan (<i>training completion</i>) dari Prinsipal terkait produk SCA yang ditawarkan, dan/atau sertifikasi profesional lain di bidang keamanan aplikasi/DevSecOps yang masih berlaku.	1	• Bertanggung jawab atas pelaksanaan, penyelesaian, dan kualitas keseluruhan pekerjaan pemeliharaan PM/CM. • Melakukan eskalasi dan validasi solusi, memastikan mutu layanan, kepatuhan terhadap <i>standar/best practice</i> teknis, keamanan dan SLA. • Mengelola risiko dan perubahan serta melakukan koordinasi dan orkestrasi dengan pihak Bank Indonesia terkait dan lainnya sehubungan dengan pekerjaan pemeliharaan (PM/CM).
	<i>Technical Engineer (PM/CM)</i>	• S1 • Pengalaman minimal 3 (tiga) tahun sebagai <i>Security Engineer/Technical Engineer</i>. • Memiliki pengalaman melakukan implementasi dan/atau pemeliharaan SCA Sonatype 1 (satu) kali dalam 3 (tiga) tahun terakhir. • Memiliki sertifikat pelatihan (<i>training completion</i>) dari Prinsipal terkait produk SCA yang ditawarkan, dan/atau sertifikasi profesional lain di bidang keamanan aplikasi/DevSecOps yang masih berlaku.	1	• Bertanggung jawab terhadap pelaksanaan dan penyelesaian pekerjaan pemeliharaan (PM/CM). • Bertanggung jawab terhadap menyiapkan Laporan PM/CM. • Berkoordinasi dengan <i>technical leader</i> dalam penyelesaian pekerjaan pemeliharaan (PM/CM).
	<i>Technical Writer</i>	• S1 • Pengalaman minimal 3 (tiga) tahun dalam bidang administrasi proyek	1	• Bertanggung jawab terhadap aspek administrasi pekerjaan, termasuk namun tidak terbatas pada laporan PM dan CM, BAP, BAK, dan BASTserta tagihan pembayaran.

Keterangan:

1. Personel Implementasi dapat merangkap sebagai Personel Pemeliharaan sepanjang memenuhi kualifikasi yang dipersyaratkan.

2. Struktur organisasi pekerjaan dan nama personel yang akan ditugaskan disampaikan pada saat pelaksanaan *Kick-Off Meeting* (KOM) pekerjaan.
3. Setiap tenaga ahli wajib menyampaikan dokumen Surat Pernyataan Menjaga Kerahasiaan Informasi dan Pengamanan Teknologi Informasi kepada Bank Indonesia dengan menggunakan format dari Bank Indonesia disertakan fotokopi KTP.
4. Paling lambat penyampaian Surat Pernyataan Menjaga Kerahasiaan Informasi dan Pengamanan Teknologi Informasi adalah saat KOM pekerjaan.
5. Setiap tenaga ahli wajib mengikuti serta dinyatakan lulus dalam tes *Cybersecurity Awareness* sebagai prasyarat sebelum ditetapkan dan ditugaskan dalam pelaksanaan pekerjaan.
6. Penggantian personel yang sudah ditetapkan dalam KOM harus diinformasikan kepada Bank Indonesia 1 (satu) bulan sebelumnya serta mendapatkan persetujuan dari Bank Indonesia termasuk di dalamnya:
 - a. Kegiatan *handover* pekerjaan kepada personel pengganti.
 - b. Menyediakan surat keterangan penggantian dari perusahaan.
 - c. Surat pernyataan menjaga kerahasiaan informasi dan pengamanan teknologi informasi.
 - d. Surat pernyataan berperilaku baik.
 - e. Personel pengganti mengikuti program induksi dan mengikuti serta dinyatakan lulus dalam tes *Cybersecurity Awareness*.