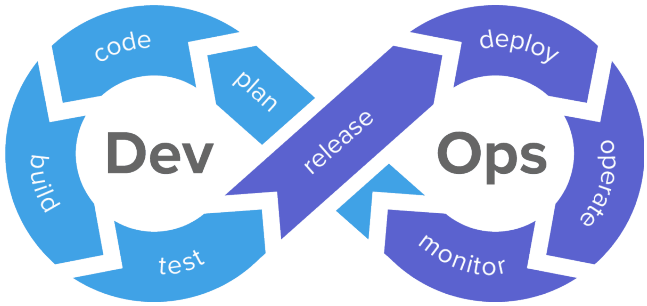
Domaine : Systèmes d'Information et télécommunication **Entité émettrice :** DSIT-DDL **Nature du document :** Directive (DIR)		**Id. Rte :** RTE_2024_0645183_2 **Id. métier** :
Version 2.0 **Statut** Approuvé **Accessibilité** Interne RTE	**Note prescriptive sur les règles de qualité des développements pour les applications DSIT**	**Date d'approbation** 06 Oct 2025 **Prescriptif** **Date d'applicabilité :** 01 Sep 2024
Destinataire(s) pour Action DSIT-CORSN, DSIT-DESIGN, DSIT-DPCM, DSIT-DPOI, DSIT-DPOSE, DSIT-DPCO, DSIT-DDL **Destinataires pour Information** PISSIN		**Rédacteur(s)** SEBASTIEN MURGEY **Vérificateur(s)** VINCENT BOUSQUET **Approbateur(s)** VALERIE VAGAGGINI
Document(s) de référence		

Rte - Réseau de Transport d'Électricité
7C, place du Dôme
Immeuble window
92073 PARIS LA DEFENSE CEDEX

1 Contexte et objectifs

Les standards SI se sont, sur les 10 dernières années, rapprochés des processus de qualité de l'industrie en intégrant des notions de contrôle et d'amélioration continue. Cela répond aussi bien à des enjeux de cybersécurité qu'à une réduction des coûts d'exploitation.
Les DSI ont donc créé une nouvelle organisation dite DEV-OPS fluidifiant le processus de mise en production sans pour autant réduire le niveau d'exigences en termes de qualité.

RTE a, en 2017, créé une équipe dédiée à la gestion du processus DEV-OPS et son outillage. Parmi ces outils, la solution SonarQube permet de vérifier, en amont de chaque mise en production, plusieurs métriques de qualité sur le code des applications. Cette dernière est la plus utilisée dans le domaine digital (près de 95% des DSI l'ont implémenté[1]).



RTE, à l'instar d'autres entreprises, est de plus en plus sujet à des attaques cyber et la sécurité de l'exploitation SI est une co-responsabilité entre les infrastructures SI et le développement des applications SI.

Pour garantir et mesurer le niveau attendu de qualité et de sécurité des développements réalisés par RTE, SonarQube propose des indicateurs essentiels autour de 4 thèmes : la sécurité, la maintenabilité, la fiabilité et la couverture de tests. Ces indicateurs offrent une vision de la qualité du code mais ne se substituent pas aux différents audits (de sécurité par exemple) qui restent nécessaires aux applications critiques pour éprouver leurs limites (de performance, de volumétrie, de sécurité etc…).

Cette note décrit les critères de qualité prescriptifs à suivre et appliquer pour les applications DSIT ; Il définit également le périmètre d'applicabilité de ces critères et la progressivité dans leur implémentation au sein des processus SI RTE.

Une note d'application est également disponible sur DOKI qui définit certaines modalités de mise en pratique de ces prescriptions.

2 Prescriptions sur la qualité des applications

2.1 Critères prescriptifs Sonar

Les critères de qualité suivants deviennent prescriptifs progressivement à partir de novembre 2024 :

- **Sécurité** : une note de A sur le backend et le frontend, à compter du **01/11/2024**
- **Couverture de code par les tests** : un pourcentage de couverture minimum de 60% sur le backend seul, à compter du **01/03/2025**
- **Maintenabilité** : une note de A sur le backend et le frontend, à compter du **01/09/2025**

Pour les projets open source, ces critères de qualité seront définis dans le cadre de la gouvernance du projet en veillant à leur cohérence avec les prescriptions internes.

Ces critères pourront être amenés à évoluer. Au-delà de ces premières prescriptions, d'autres critères sont recommandés. La liste complète de ces critères est présentée dans la note d'application. Il est conseillé à tous les projets de tendre vers le respect de cette barrière de qualité plus large afin d'être prêts pour les futurs élargissements de cette prescription.

2.2 Applications concernées

L'ensemble des applications sous le pilotage de la DSIT (application industrialisée) sont concernées par la présente note. En revanche, des dérogations pourront être accordées (temporairement où de façon permanente) en fonction de la nature du projet, et de son historique.

Il est rappelé que toute nouvelle application développée par la DSIT doit obligatoirement s'inscrire dans le processus d'intégration continu DevOps RTE pour s'assurer de sa qualité.

2.3 Evolution de la prescription

Le calendrier d'évolution des prescriptions sera revu annuellement par DDL et DESIGN pour validation par le CODIR DSIT.

Il faut noter que l'objectif reste de poursuivre l'extension du périmètre de prescription, et de la surface d'analyse notamment pour ce qui touche à l'éco-conception. Il est donc important que les projets s'organisent au plus vite pour respecter non seulement les critères prescriptifs, mais également les critères recommandés lorsque cela est possible.

3 Processus de contrôle

3.1 Traitement des faux-positifs

Certaines vulnérabilités remontées par Sonar peuvent ne pas présenter de véritable risque de sécurité, et ne nécessitent pas de correction dans le code : il s'agit de faux-positifs.

Il est possible à tout moment de retrouver les vulnérabilités classées comme faux-positifs dans SonarQube.

Pour toute demande de classification d'anomalie comme faux positif, se référer au mode opératoire décrit dans la note d'application.

3.2 Publication du rapport d'analyse Sonar

Les chefs de projet sont responsables de la fourniture des éléments d'analyse de qualité permettant de prouver le respect des critères prescriptifs à chaque demande de mise en production par le CORSN.

Le format attendu du rapport ainsi que les modalités de communication de celui-ci au CORSN est défini dans la note d'application.

3.3 Dérogations

3.3.1 Dérogations temporaires

Si les critères prescriptifs ne sont pas validés, il est possible de demander une dérogation auprès du manager du département autorisant la mise en production à titre exceptionnel.

Les dérogations temporaires doivent être assorties d'un plan de mise en conformité avec les prescriptions.

La demande doit enfin être validée par le manager du département.

Le format attendu de la dérogation ainsi que les modalités de communication de celle-ci au CORSN est défini dans la note d'application.

3.3.2 Dérogations permanentes

Si une application ne peut pas être mise en conformité avec ces prescriptions (que ce soit techniquement, contractuellement ou budgétairement) à long terme, il est possible de demander une dérogation permanente.

Sont notamment concernées :

- Les progiciels ou SaaS
- Les applications en MCO hors DevOps

Les dérogations permanentes sont soumises à un avis technique consultatif donné par le DDL.

La demande doit enfin être validée par le manager du département, et sera remontée pour information au CODIR DSIT.

L'existence d'une dérogation permanente n'exempte pas le projet de mettre en œuvre ce qui est en son pouvoir pour suivre et améliorer la qualité du code source de l'application lorsque cela est possible.

Le format attendu de la dérogation ainsi que les modalités de communication de celle-ci au CORSN est défini dans la note d'application.

3.4 Validation par le CORS-N de la conformité

Le CORS-N est responsable de la vérification des critères prescriptifs, sur base des éléments fournis lors de la demande de mise en production.

En cas de non-respect des critères prescriptifs et en l'absence de dérogation, la mise en production sera refusée.

Les modalités de communication des éléments relatifs à cette prescription au CORSN sont définies dans la note d'application.