COMMENT REMPLIR LA MAQUETTE D'INCIDENT DORA

Aide au remplissage champ par champ de la maquette

26 AOÛT 2025
AUTORITÉ DE CONTRÔLE PRUDENTIEL ET DE RÉSOLUTION
4 Place de Budapest, 75009, Paris

INTRODUCTION

Dans les pages ci-dessous, vous pourrez trouver la maquette .JSON de la notification d'un incident majeur conformément à l'article 19 DORA. **Il s'agit d'un exemple** qui doit être pour pris pour tel, mais qui doit servir de base pour vos remises.

Cette maquette-exemple contient tous les champs possibles. Ils ne sont toutefois pas tous obligatoires, notamment lors de la remise initiale. Nous avons donc employé un code couleur : les champs d'une remise initiale sont **verts**, et ceux d'une remise intermédiaire sont **bleus**. Les champs non-colorés sont donc ceux d'une remise finale. Le cas particulier d'une remise de reclassification doit au moins contenir tous les champs d'une remise initiale, et peut avoir des précisions de remises intermédiaires, suivant quand la déclassification a eu lieu.

Les **obligations réglementaires ainsi que des conseils de remplissage** (précédés d'un # et de couleur **violette**) sont ajoutés à côté de certains champs. Ce document fournit des informations sur les difficultés les plus communément rencontrées jusqu'à ce jour, en plus d'indiquer le format de base d'une remise.

Quelques rappels :

- Utilisation des clés et des valeurs correspondants : pour l'ensemble des remises, les clés (indiquées entre "" **avant** les ' :') doivent toujours être identiques à ce qui est indiquée dans la maquette. Les valeurs (indiquées entre "" **après** les ' :') ne sont que des exemples mais : 1/ dans certains cas des menus déroulants sont fournis ; 2/ le format doit être respecté.
- Vous pouvez conserver tous les champs pour toutes les remises (en ne remplissant que les champs de la remise en question), ou avoir des modèles différents pour chaque type de remise, qui n'incluent que les champs à remplir.
- Si le développement d'outils visant au remplissage (semi) automatique des .JSON est une bonne chose, il est essentiel de s'assurer de son bon paramétrage et de mettre en place des vérifications afin, notamment, de s'assurer que de mauvaises informations ne sont pas transmises.
- **Tout rapport doit contenir les informations des rapports précédents**, lesquelles peuvent toutefois être modifiées si l'entité a évolué dans sa perception de l'incident. Notamment, il est nécessaire de conserver les informations du rapport initial dans les rapports intermédiaires et le rapport final (et, si un tel rapport a lieu, dans le rapport de reclassification de l'incident en incident non-majeur). De même, les informations des rapports intermédiaires doivent être laissées – ou mieux, précisées – dans le rapport final.

MAQUETTE ANNOTÉE


```
{
  "incidentSubmission": "initial_notification", # Des erreurs sur le type de notification figurent dans les notifications. Il est primordial de mettre à jour ce champ à chaque nouvelle remise (même si vous reprenez la notification initiale dans les rapports subséquents, ce qui est demandé). Il n'y a que 4 réponses possibles dans ce champ : "initial_notification", "intermediate_report", "final_report", "major_incident_reclassified_as_non-major".
  "reportCurrency": "EUR",   # Ce champ est contraint. Vous devez mettre une valeur parmi : "EUR", "BGN", "CZK", "DKK", "HUF", "PLN", "RON", "ISK", "CHF", "NOK", "SEK".
  "submittingEntity": {
    "name": "String",
    "code": "String",
    "affectedEntityType": [                # Ce champ est contraint. Vous devez mettre (au moins) une valeur parmi : "credit_institution", "payment_institution", "exempted_payment_institution", "account_information_service_provider", "electronic_money_institution", "exempted_electronic_money_institution", "investment_firm", "crypto-asset_service_provider", "issuer_of_asset-referenced_tokens", "central_securities_depository", "central_counterparty", "trading_venue", "trade_repository", "manager_of_alternative_investment_fund", "management_company", "data_reporting_service_provider", "insurance_and_reinsurance_undertaking", "insurance_intermediary_reinsurance_intermediary_and_ancillary_insurance_intermediary", "institution_for_occupational_retirement_provision", "credit_rating_agency", "administrator_of_critical_benchmarks", "crowdfunding_service_provider", "securitisation_repository"
      "credit_institution"
    ]
  },
  "affectedEntity": [
    {
      "name": "String",
      "code": "String",
```

"affectedEntityType": [# Ce champ est contraint. Vous devez mettre (au moins) une valeur parmi : "credit_institution", "payment_institution", "exempted_payment_institution", "account_information_service_provider", "electronic_money_institution", "exempted_electronic_money_institution", "investment_firm", "crypto-asset_service_provider", "issuer_of_asset-referenced_tokens", "central_securities_depository", "central_counterparty", "trading_venue", "trade_repository", "manager_of_alternative_investment_fund", "management_company", "data_reporting_service_provider", "insurance_and_reinsurance_undertaking", "insurance_intermediary_reinsurance_intermediary_and_ancillary_insurance_intermediary", "institution_for_occupational_retirement_provision", "credit_rating_agency", "administrator_of_critical_benchmarks", "crowdfunding_service_provider", "securitisation_repository"

"credit_institution"

],

"LEI": "00000000000000000000" # Certains ne mettent pas que le LEI dans la case (mettant par exemple « LEI : », ou mettant un autre code). Il ne faut mettre que le LEI brut dans la case, et seul un LEI est accepté.

}

],

"ultimateParentUndertaking": {

"name": "String", # L'orthographe varie parfois d'une notification à l'autre ce qui empêche de faire des recoupements. Il est nécessaire de toujours employer le même orthographe, qui doit être le nom légal de l'entité (pas une abréviation).

"code": "String",

"affectedEntityType": [# Ce champ est contraint. Vous devez mettre (au moins) une valeur parmi : "credit_institution", "payment_institution", "exempted_payment_institution", "account_information_service_provider", "electronic_money_institution", "exempted_electronic_money_institution", "investment_firm", "crypto-asset_service_provider", "issuer_of_asset-referenced_tokens", "central_securities_depository", "central_counterparty", "trading_venue", "trade_repository", "manager_of_alternative_investment_fund", "management_company", "data_reporting_service_provider", "insurance_and_reinsurance_undertaking", "insurance_intermediary_reinsurance_intermediary_and_ancillary_insurance_intermediary", "institution_for_occupational_retirement_provision", "credit_rating_agency",

"administrator_of_critical_benchmarks", "crowdfunding_service_provider", "securitisation_repository"

"credit_institution"

],

"LEI": "00000000000000000000" # Certains ne mettent pas que le LEI dans la case (mettant par exemple « LEI : », ou mettant un autre code). Il ne faut mettre que le LEI brut dans la case, et seul un LEI est acceptée.

},

"primaryContact": {

"name": "String",

"email": "jdoe@example.com", # Certaines adresses renseignées n'acceptent parfois pas de recevoir des mails (des BAL communes notamment). Il faut toujours s’assurer que l’adresse donnée est utilisable et utilisée, afin de faciliter les retours sur l’incident.

"phone": "+40744442029"

},

"secondaryContact": {

"name": "String",

"email": "jdoe@example.com", # Certaines adresses renseignées n'acceptent parfois pas de recevoir des mails (des BAL communes notamment). Il faut toujours s’assurer que l’adresse donnée est utilisable et utilisée, afin de faciliter les retours sur l’incident.

"phone": "+33 1234567890989898898999876767676767"

},

"incident": {

"financialEntityCode": "String", # Pour des raisons de transmission du reporting, il est **nécessaire** d’utiliser un code ne contenant que des caractères alphanumériques OU des « - », rien d’autre n’est autorisé. Vous êtes sinon libre d’utiliser le code interne qui vous sied. Toutefois, dans le cas d'un incident impactant plusieurs entités d'un même groupe, il serait souhaitable d'avoir un numéro d'incident unique (pour permettre les recoupements) complété d'un chiffre ou d'une lettre (pour distinguer les entités impactées).

Exemple : l'incident est identifié par le n°312245 ; pour chaque entité le numéro d'incident serait n°312245-a, n°312245-b, etc. Il faut toutefois bien que les codes soient **distincts** pour chaque entité qui soumet un reporting.

"detectionDateTime": "2001-12-17T09:30:47.0",

"classificationDateTime": "2001-12-17T09:30:47.0Z",

"incidentDescription": "String", # Les descriptions sont parfois trop succinctes. De nombreuses abréviations internes sont insérées et il est souvent difficile de comprendre l'incident. Il faudrait donc utiliser des termes qui peuvent être compris par un lecteur externe à l'entité, et pouvoir expliquer précisément le problème (et en quoi il est majeur).

"classificationTypes": [# Certains ne déclarent qu'un seul critère d'incident, ou deux dont « critical_services_affected » (et ne déclarent pas être victimes d'« acte de malveillance »). Nous rappelons donc que conformément au Règlement d'exécution (UE) 2025/302, un incident majeur est majeur si et seulement si le critère "acte de malveillance" (ie si l'un des types d'incidents déclarés est « cybersecurity-related »), **OU** si 1) **des fonctions critiques** (« critical_services_affected ») ou alors des fonctions **qui nécessitent une autorisation, sont enregistrées ou sont supervisées** sont impactées par l'incident **ET** 2) au moins **DEUX** critères sont remplis parmi : "clients_financial_counterparts_and_transactions_affected", "geographical_spread", "data_losses", "economic_impact", "reputational_impact", "duration_and_service_downtime".

Il faut donc vérifier si les critères sont remplis avant de notifier un incident qui n'est, en réalité, pas majeur. Il faut ensuite dans cette liste "classificationTypes": (entre [ ]) mettre les dictionnaires (les valeurs entre { }) des critères **qui se rapportent à l'incident qui est notifié, en les séparant d'une virgule**.

Par exemple, si l'incident est majeur à cause des critères "geographical_spread", "reputational_impact" et "duration_and_service_downtime", **il ne faut conserver que ces trois "classificationCriterion", et retirer les trois autres.**

{

"classificationCriterion": "clients_financial_counterparts_and_transactions_affected",

},

{

"classificationCriterion": "geographical_spread",

"countryCodeMaterialityThresholds": [# Ce champ est contraint. Vous devez mettre (au moins) une valeur parmi : "AT", "BE", "BG", "HR", "CY", "CZ", "DK", "EE", "ES", "FI", "FR", "DE", "GR", "HU", "IS", "IE", "IT", "LI", "LT", "LU", "LV", "MT", "NL", "NO", "PL", "PT", "RO", "SE", "SI", "SK"

"RO"

],

"memberStatesImpactType": [# Il y a parfois des réponses libres qui ne prennent pas en compte les choix disponibles dans ce champ. Conformément au Règlement d'exécution (UE) 2025/302, la réponse à ce champ doit faire partie d'un menu déroulant (avec un détail explicatif au champ ci-dessous). Les réponses possibles sont : "clients", "financial_counterparts", "branch_of_the_financial_entity", "financial_entities_within_the_group_carrying_out_activities_in_the_respective_member_state", "financial_market_infrastructure", "third-party_providers_that_may_be_common_to_other_financial_entities"

"clients"

],

"memberStatesImpactTypeDescription": "String" # Descriptions parfois trop brèves. Conformément au Règlement d'exécution (UE) 2025/302, ce champ doit contenir la description de l'incidence et de la gravité de l'incident majeur lié aux TIC dans chaque État membre touché, y compris l'évaluation de l'incidence et de la gravité sur: a) les clients; b) les contreparties financières; c) les succursales de l'entité financière; d) les autres entités financières du groupe qui exercent des activités dans l'État membre concerné; e) les infrastructures des marchés financiers; f) les prestataires tiers qui peuvent être communs à d'autres entités financières, le cas échéant, dans un ou plusieurs autres États membres. Ce champ est **obligatoire** si le critère "geographical_spread" est rempli.

},

{

"classificationCriterion": "data_losses",

"dataLosseMaterialityThresholds": [# Il y a parfois des réponses libres qui ne prennent pas en compte les choix disponibles dans ce champ. Conformément au Règlement d'exécution (UE) 2025/302, la réponse à ce champ doit faire partie d'un menu déroulant (avec un détail explicatif au champ ci-dessous). Les réponses possibles sont : "availability", "authenticity", "integrity", "confidentiality"

"authenticity",

"availability"

],

"dataLossesDescription": "String"

},

{

"classificationCriterion": "reputational_impact",

"reputationalImpactType": [# Il y a parfois des réponses libres qui ne prennent pas en compte les choix disponibles dans ce champ. Conformément au Règlement d'exécution (UE) 2025/302, la réponse à ce champ doit faire partie d'un menu déroulant (avec un détail explicatif au champ ci-dessous). Les réponses possibles sont : "the_major_ict-related_incident_has_been_reflected_in_the_media",

"the_major_ict-related_incident_has_resulted_in_repetitive_complaints_from_different_clients_or_financial_counterparts_on_client-facing_services_or_critical_business_relationships",

"the_financial_entity_will_not_be_able_to_or_is_likely_not_to_be_able_to_meet_regulatory_requirements_as_a_result_of_the_major_ict-related_incident",

"the_financial_entity_will_or_is_likely_to_lose_clients_or_financial_counterparts_with_a_material_impact_on_its_business_as_a_result_of_the_major_ict-related_incident"

"the_major_ict-related_incident_has_been_reflected_in_the_media"

],

"reputationalImpactDescription": "String" # Descriptions parfois trop brèves. Conformément au Règlement d'exécution (UE) 2025/302, ce champ doit contenir des informations comprenant : « le type de médias (par exemple, médias traditionnels et numériques, blogs, plateformes de diffusion en continu) et la couverture médiatique, y compris la portée des médias (locale, nationale, internationale). Ne relèvent pas d'une couverture médiatique dans ce contexte les quelques commentaires négatifs d'abonnés ou d'utilisateurs de réseaux sociaux. L'entité financière indique également si la couverture médiatique a mis en évidence des risques importants pour ses clients liés à l'incident majeur lié aux TIC, y compris le risque d'insolvabilité de l'entité financière ou le risque de perte de fonds. Les entités financières indiquent également si elles ont communiqué aux médias des éléments permettant d'informer de manière fiable le public de l'incident majeur lié aux TIC et de ses conséquences. Les entités financières peuvent également indiquer si de fausses informations ont circulé dans les médias en ce qui concerne l'incident lié aux TIC, y compris des informations fondées sur la propagation délibérée de fausses informations par des acteurs de la menace, ou des

informations relatives à la dégradation du site web de l'entité financière ou illustrant cette dégradation. »

},

{

"classificationCriterion": "economic_impact",

"economicImpactMaterialityThreshold": "String"

},

{

"classificationCriterion": "critical_services_affected ",

}

],

"isBusinessContinuityActivated": true,

"incidentOccurrenceDateTime": "2001-12-17T09:30:47.0", # Ce format est obligatoire, et est lu : Année-Mois-JourTHeure:Minute:Seconde.Dixièmedeseconde . Par ailleurs, il faut faire attention à la cohérence entre ce champ, et ceux de «incidentDuration », « serviceDowntime » et « servicerestorationDateTime ».

"incidentDuration": "100:23:54", # Ce format est obligatoire, et est lu : Jour:Heure:Minutes. Ici, l'incident a donc duré 100 jours, 23 heures et 54 minutes. Même si la durée de l'incident ne se compte qu'en heures (ex. : un incident qui dure 04h12 minutes), il faudra indiquer : "00:04:12". Par ailleurs, il faut faire attention à la cohérence entre ce champ, et ceux de « serviceDowntime », « servicerestorationDateTime » et « incidentOccurenceDateTime ».

"originatesFromThirdPartyProvider": "String", # Il n'y a parfois pas de précision sur qui est à l'origine de l'incident. Conformément au Règlement d'exécution (UE) 2025/302, ce champ est obligatoire si un prestataire est à l'origine de l'incident. En ce cas, il faut écrire le nom et un code d'identification (LEI, EUID, ...) unique du prestataire qui est la cause de l'incident (**pas simplement « oui »**), en précisant quel code est utilisé. **Il ne faut rien indiquer** dans ce champ si l'incident n'est pas causé par un prestataire tiers (c'est à dire laisser « "" »).

"otherInformation": "String", # Ce champ n'est parfois pas rempli. Conformément au Règlement d'exécution (UE) 2025/302 , ce champ sert à indiquer des informations non reprises dans le modèle. Surtout, il **est obligatoire dans le cas d'un incident reclassé en incident non-majeur**. Dans ce cas, ce champ doit **expliquer les raisons qui poussent l'entité à reclassifier l'incident**.

"incidentDiscovery": "it_security", # Ce champ est contraint. Vous devez mettre (au moins) une valeur parmi : "it_security", "staff", "internal_audit", "external_audit", "clients", "financial_counterparts", "third-party_provider", "attacker", "monitoring_systems", "authority_agency_law_enforcement_body", "other"

"competentAuthorityCode": "String", # Il y a parfois des réponses libres. Nous rappelons donc qu'il est obligatoire de mettre dans ce champ le code de l'incident que l'autorité compétente, ici l'ACPR, vous fournit. Ce code vous est envoyé par mail lors de l'accusé de réception du dépôt de la remise initiale. Ce code est composé de l'année (en 4 chiffres), d'un I ou d'un M (suivant qu'il s'agisse d'un Incident ou d'une Menace), et enfin d'un numéro d'identification à 7 chiffres.

"incidentType": {

"incidentClassification": [# Il y a parfois des réponses libres qui ne prennent pas en compte les choix disponibles dans ce champ. Conformément au Règlement d'exécution (UE) 2025/302, la réponse à ce champ doit faire partie d'un menu déroulant (avec un détail explicatif au champ ci-dessous). Les réponses possibles sont : "cybersecurity-related", "process_failure", "system_failure", "external_event", "payment-related", "other". En cas de "other", vous devez décrire précisément la classification (dans "otherIncidentClassification").

"cybersecurity-related",

"other"

],

"threatTechniques": [# Il y a parfois des réponses libres qui ne prennent pas en compte les choix disponibles dans ce champ. Conformément au Règlement d'exécution (UE) 2025/302, la réponse à ce champ doit faire partie d'un menu déroulant (avec un détail explicatif au champ ci-dessous). Les réponses possibles sont : "social_engineering_including_phishing", "ddos", "identity_theft", "data_encryption_for_impact_including_ransomware", "resource_hijacking", "data_exfiltration_and_manipulation_including_identity_theft", "data_destruction", "defacement", "supply-chain_attack", "other". En cas de "other", vous devez décrire précisément la technique employée (dans " otherThreatTechniques ").

"social_engineering_including_phishing",

"other"

],

"otherIncidentClassification": "String",

"otherThreatTechniques": "String",

"indicatorsOfCompromise": "String"

},

"rootCauseHLClassification": [# Ce champ est contraint. Vous devez mettre (au moins) une valeur parmi : "malicious_actions", "process_failure", "system_failure_malfunction", "human_error", "external_event"

"malicious_actions",

"system_failure_malfunction"

],

"rootCausesDetailedClassification": { # Il y a parfois des causes détaillées contradictoire avec les causes plus larges choisies dans la classification "rootCauseHLClassification", ou des réponses libres qui ne prennent pas en compte les choix disponibles dans ce champ. Une cohérence est attendue avec le champ "rootCauseHLClassification".

Par exemple, si la cause choisie est "system_failure", il faut choisir des causes détaillées avec "system_failure_".

Conformément au Règlement d'exécution (UE) 2025/302 , les choix possibles pour ce champ sont : "malicious_actions_deliberate_internal_actions", "malicious_actions_deliberate_physical_damage_manipulation_theft", "malicious_actions_fraudulent_actions", "process_failure_insufficient_monitoring_or_failure_of_monitoring_and_control", "process_failure_insufficient_unclear_roles_and_responsibilities", "process_failure_ICT_risk_management_process_failure", "process_failure_insufficient_or_failure_of_ict_operations_and_ict_security_operations" , "process_failure_insufficient_or_failure_of_ict_project_management", "process_failure_inadequacy_of_internal_policies_procedures_and_documentation", "process_failure_inadequate_ict_systems_acquisition_development_and_maintenance ", "process_failure_other", "system_failure_hardware_capacity_and_performance", "system_failure_hardware_maintenance", "system_failure_hardware_obsolescence_ageing", "system_failure_software_compatibility_configuration", "system_failure_software_performance", "system_failure_network_configuration", "system_failure_physical_damage", "system_failure_other", "human_error_omission", "human_error_mistake", "human_error_skills_knowledge", "human_error_inadequate_human_resources", "human_error_miscommunication", "human_error_other", "external_event_natural_disasters_force_majeure", "external_event_third-party_failures", "external_event_other" .

Ce champ est par ailleurs **obligatoire dans un rapport final.**

},

"rootCausesAdditionalClassification": [# Il y a parfois des causes additionnelles contradictoires avec les causes plus larges choisies dans la classification "rootCausesDetailedClassification", ou des réponses libres qui ne prennent pas en compte les choix disponibles dans ce champ. Une cohérence est attendue avec le champ "rootCausesDetailedClassification". Conformément au Règlement d'exécution (UE) 2025/302 , ce champ est obligatoire pour les choix 2.a , 2.c, 2.d et 2.g du champ "rootCausesDetailedClassification", soit ceux qui nécessitent des détails additionnels. La précision doit être cohérente (si on déclare un problème de surveillance au champ "rootCausesDetailedClassification", il faut que la précision soit dans les problèmes de surveillances et pas ailleurs). Les choix possibles pour ce champ sont : "monitoring_of_policy_adherence", "monitoring_of_third-party_service_providers", "monitoring_and_verification_of_remediation_of_vulnerabilities", "identity_and_access_management", "encryption_and_cryptography", "logging", "failure_in_specifying_accurate_risk_tolerance_levels", "insufficient_vulnerability_and_threat_assessments", "inadequate_risk_treatment_measures", "poor_management_of_residual_ict_risks", "vulnerability_and_patch_management", "change_management", "capacity_and_performance_management", "ict_asset_management_and_information_classification", "backup_and_restore", "error_handling", "inadequate_ict_systems_acquisition_development_and_maintenance", "insufficient_or_failure_of_software_testing"

"backup_and_restore"

],

"rootCausesOther": "String",

"rootCausesInformation": "String", # Ce champ n'est parfois pas rempli. Nous rappelons donc que conformément au Règlement d'exécution (UE) 2025/302, en cas d'actions malveillantes, il faut fournir une "description du mode opératoire de l'action malveillante, y compris les tactiques, techniques et procédures utilisées, ainsi que du vecteur d'entrée de l'incident majeur lié aux TIC, y compris une description des enquêtes et des analyses qui ont permis d'identifier les causes originelles, le cas échéant" . **Même s'il n'y a pas eu d'actes de malveillance**, il faut décrire "la séquence des évènements qui ont conduit à l'incident majeur". **Ce champ est donc toujours obligatoire**.

"rootCauseAddressingDateTime": "2001-12-17T09:30:47.0", # Ce format est obligatoire, et est lu : Année-Mois-JourTHeure:Minute :Seconde.Dixièmedeseconde.

"incidentResolutionSummary": "String", # Ce champ n'est parfois pas rempli. Conformément au Règlement d'exécution (UE) 2025/302 , il est essentiel que ce champ soit rempli et explique la façon dont l'incident a été résolu. Cette description doit contenir une description des mesures de résolution, avec a) Actions prises pour résoudre de façon définitive l'incident majeur lié aux TIC (à l'exclusion de toute action temporaire); b) pour chaque action prise, indiquer la participation potentielle d'un prestataire tiers et de l'entité financière; c) indiquer si les procédures ont été adaptées à la suite de l'incident majeur lié aux TIC; d) indiquer tout contrôle supplémentaire qui a été mis en place ou qu'il est prévu d'instaurer, avec le calendrier de mise en œuvre correspondant. Enfin, il faut une deuxième partie de réponse qui porte sur les enseignements tirés de cet incident

"incidentResolutionDateTime": "2001-12-17T09:30:47.0", # Ce format est obligatoire, et est lu : Année-Mois-Jour T Heure:Minute:Seconde.Dixièmedeseconde.

"incidentResolutionVsPlannedImplementation": "String",

"assessmentOfRiskToCriticalFunctions": "String",

"informationRelevantToResolutionAuthorities": "String",

"financialRecoveriesAmount": 0.1, # Ce chiffre est à fournir en valeur absolue. Il ne faut pas utiliser de séparateur de millier, million, etc. De plus, conformément au Règlement d'exécution (UE) 2025/302, les données doivent toujours être en k-euros (ou autre monnaie), et pas en euros, millions d'euros, etc. Le « 0.1 » ici est donc compris comme 100 euros.

"grossAmountIndirectDirectCosts": 0.1, # Ce chiffre est à fournir en valeur absolue. Il ne faut pas utiliser de séparateur de millier, million, etc. De plus, conformément au Règlement d'exécution (UE) 2025/302, les données doivent toujours être en k-euros (ou autre monnaie), et pas en euros, millions d'euros, etc. Le « 0.1 » ici est donc compris comme 100 euros.

"recurringNonMajorIncidentsDescription": "String",

"recurringIncidentDate": "2001-12-17T09:30:47.0" # Ce format est obligatoire, et est lu : Année-Mois-JourTHeure:Minute:Seconde.Dixièmedeseconde.

},

"impactAssessment": {

"hasImpactOnRelevantClients": true,

"serviceImpact": {

"serviceDowntime": "00:00:00", # Ce format est obligatoire, et est lu : Jour:Heure:Minutes. Ici, le service a donc été interrompu 0 jour, 0 heure et 0 minute. Même si

la durée de l'incident ne se compte qu'en heures (ex. : un incident qui dure 04h12 minutes), il faudra indiquer : "00:04:12". Par ailleurs, il faut faire attention à la cohérence entre ce champ, et ceux de «incidentDuration », « servicerestorationDateTime » et « incidentOccurenceDateTime ».

"serviceRestorationDateTime": "2001-12-17T09:30:47.0", # Ce format est obligatoire, et est lu : Année-Mois-JourTHeure:Minute:Seconde.Dixièmedeseconde . Par ailleurs, il faut faire attention à la cohérence entre ce champ, et ceux de «incidentDuration », « incidentOccurenceDateTime » , et « serviceDowntime ».

"isTemporaryActionsMeasuresForRecovery": true,

"descriptionOfTemporaryActionsMeasuresForRecovery": "String" # Ce champ n'est parfois pas rempli. Conformément au Règlement d'exécution (UE) 2025/302 , la réponse à ce champ est obligatoire en cas d'action temporaire prise. La réponse doit en particulier contenir des informations sur : « les actions immédiates prises, y compris l'isolement de l'incident au niveau du réseau, les procédures de contournement activées, les ports USB bloqués, le site de reprise après sinistre activé, tout autre contrôle de sécurité supplémentaire temporairement mis en place. Les entités financières indiquent la date et l'heure de la mise en œuvre des actions temporaires ainsi que la date prévue de retour sur le site primaire. Pour les éventuelles actions temporaires qui n'auraient pas été mises en œuvre mais qui sont encore prévues, indiquer la date à laquelle leur mise en œuvre est attendue. Si aucune action/mesure temporaire n'a été prise, veuillez en indiquer la raison. » Il est donc également nécessaire de remplir ce champ même si aucune action n'a été prise.

},

"criticalServicesAffected": "String",

"affectedAssets": {

"affectedClients": {

"number": 1, # Nous rappelons que ce chiffre est à fournir en valeur absolue, et il ne faut pas utiliser de séparateur de millier, million, etc. Il convient par ailleurs d'assurer la cohérence de ce nombre avec le champ pourcentage ci-dessous.

"percentage": 3.5 # Nous rappelons qu'il faut mettre jusqu'à 5 chiffres maximum (dont 1 maximum après la virgule, arrondi au supérieur), et pas de symbole pourcentage. Si par exemple on tombe sur 150.45%, l'on écrira 150.5 . **Le pourcentage doit être calculé par rapport au nombre total de clients de l'entité.** Il convient par ailleurs d'assurer la cohérence de ce pourcentage avec le champ number ci-dessus.

},

"affectedFinancialCounterparts": {

"number": 2, # Nous rappelons que ce chiffre est à fournir en valeur absolue, et qu'il ne faut pas utiliser de séparateur de millier, million, etc. Il convient par ailleurs d'assurer la cohérence de ce nombre avec le champ pourcentage ci-dessous.

"percentage": 4.6 # Nous rappelons qu'il faut mettre jusqu'à 5 chiffres maximum (dont 1 maximum après la virgule, arrondi au supérieur), et pas de symbole pourcentage. Si par exemple on tombe sur 150.45%, l'on écrira 150.5 . **Le pourcentage doit être calculé par rapport au nombre total de contreparties de l'entité.** Il convient par ailleurs d'assurer la cohérence de ce pourcentage avec le champ number ci-dessus.

},

"affectedTransactions": {

"number": 3, # Nous rappelons que ce chiffre est à fournir en valeur absolue, et qu'il ne faut pas utiliser de séparateur de millier, million, etc. Il convient par ailleurs d'assurer la cohérence de ce nombre avec le champ pourcentage ci-dessous.

"percentage": 5.7 # Il faut mettre jusqu'à 5 chiffres maximum (dont 1 maximum après la virgule, arrondi au supérieur), et pas de symbole pourcentage. Si par exemple on tombe sur 150.45%, l'on écrira 150.5 . **Le pourcentage doit être calculé par rapport au nombre moyen de transactions quotidiennes de l'entité (et pas par rapport aux transactions pendant l'incident). Il est donc hautement improbable de tomber sur un pourcentage exact.** Il convient par ailleurs d'assurer la cohérence de ce pourcentage avec le champ « number » ci-dessus.

},

"valueOfAffectedTransactions": 1, # Ce chiffre est à fournir en valeur absolue, et qu'il ne faut pas utiliser de séparateur de millier, million, etc. De plus, conformément au Règlement d'exécution (UE) 2025/302, les données doivent toujours être en k-euros (ou autre monnaie), et pas en euros, millions d'euros, etc. Le « 1 » ici est donc compris comme 1 000 euros.

"numbersActualEstimate": [# Ce champ n'est parfois pas entièrement rempli. Conformément au Règlement d'exécution (UE) 2025/302 , ce champ doit indiquer si les chiffres sur les clients, les transactions et les contreparties financières affectées sont réels ou estimés, ou s'il n'y a eu aucun impact. Il est donc **obligatoire** d'avoir **trois** réponses dans cette liste**. Il faut donc une première valeur parmi :** "actual_figures_for_clients_affected", "estimates_for_clients_affected", "no_impact_on_clients" .

Il en faut une seconde parmi :

"actual_figures_for_transactions_affected", "estimates_for_transactions_affected", "no_impact_on_transactions"

Et enfin il faut une troisième réponse parmi :

"actual_figures_for_financial_counterparts_affected",
"estimates_for_financial_counterparts_affected",
"no_impact_on_financial_counterparts"

"actual_figures_for_clients_affected",

“actual_figures_for_transactions_affected”,

“actual_figures_for_financial_counterparts_affected”

]

},

"affectedFunctionalAreas": "String", # Bien que ce champ ne soit pas contraint, il est **nécessaire** de se limiter aux choix identifiés dans le Règlement d’exécution (UE) 2025/302 pour le remplir.

"isAffectedInfrastructureComponents": "yes", # Il y a parfois des réponses libres qui ne prennent pas en compte les choix disponibles dans ce champ. Conformément au Règlement d’exécution (UE) 2025/302, la réponse à ce champ doit faire partie d'un menu déroulant (avec un détail explicatif au champ ci-dessous). Les réponses possibles sont : « yes », « no », « information_not_available ».

"affectedInfrastructureComponents": "String",

"isImpactOnFinancialInterest": "yes" # Il y a parfois des réponses libres qui ne prennent pas en compte les choix disponibles dans ce champ. Conformément au Règlement d’exécution (UE) 2025/302, la réponse à ce champ doit faire partie d'un menu déroulant. Les réponses possibles sont : « yes », « no », « information_not_available ».

},

"reportingToOtherAuthorities": [# Il y a parfois des réponses libres qui ne prennent pas en compte les choix disponibles dans ce champ. Conformément au Règlement d’exécution (UE) 2025/302, la réponse à ce champ doit faire partie d'un menu déroulant (avec un détail explicatif au champ ci-dessous). Les réponses possibles sont : "police_law_enforcement", "csirt", "data_protection_authority", "national_cybersecurity_agency", "none", "other". Ce champ étant obligatoire, il **faut** répondre « none » si jamais seule l’autorité compétente DORA a été notifiée.

"police_law_enforcement",

"other"

],

"reportingToOtherAuthoritiesOther": "String", # Ce champ n'est parfois pas rempli. Conformément au Règlement d’exécution (UE) 2025/302, la réponse à ce champ est obligatoire si le choix "other" est sélectionné au champ 3.31 . Il convient alors d'écrire le **nom** de toutes les autres autorités qui ont eu un reporting de l'incident.

"informationDurationServiceDowntimeActualOrEstimate": "estimates"

}