DEUTSCHE BUNDESBANK
EUROSYSTEM

14. August 2018

Rundschreiben Nr. 65/2018

An alle
Kreditinstitute

Selbstzertifizierungspflicht für alle Teilnehmer an TARGET2-Bundesbank
hier: Vorabinformation über neue Anforderungen zur Erhöhung der Sicherheit

Sehr geehrte Damen und Herren,

die Cyber-Attacken in der jüngeren Vergangenheit sowie neue Risiken und erhöhte fachliche Anforderungen der Zahlungsverkehrsüberwachung (Oversight) an Finanzmarktinfrastrukturen haben das Eurosystem veranlasst, die bis heute gültigen Sicherheitsmaßnahmen für den Zugang zur TARGET2-Gemeinschaftsplattform zu überprüfen. Im Ergebnis hat das Eurosystem beschlossen, erhöhte Sicherheitsmaßnahmen zu implementieren, um allen TARGET2-Teilnehmern, also allen kritischen wie nicht-kritischen Teilnehmern, eine noch bessere betriebliche Stabilität bzw. operationelle Zuverlässigkeit von TARGET2 sowie einen sicheren Zugang zur Gemeinschaftsplattform zu gewährleisten.

Was bedeutet der Beschluss des Eurosystems im Allgemeinen und für Sie als Teilnehmer an TARGET2-Bundesbank im Besonderen? Erstens: Ab Ende 2018 müssen alle Teilnehmer an TARGET2, also alle kritischen und nicht-kritischen Teilnehmer, die sogenannte „Selbstzertifizierungserklärung“ für TARGET2 abgeben und jedes Jahr erneuern. Dabei handelt es sich um eine Erklärung hinsichtlich des Umsetzungsgrades bestimmter sicherheitsrelevanter Anforderungen. Unabhängig vom Beschluss des Eurosystems gilt diese Selbstzertifizierungspflicht auch für HAM-Kontoinhaber bei der Bundesbank, sofern sie einen eigenen technischen Zugang zur TARGET2-Gemeinschaftsplattform haben. Nicht betroffen sind HAM-Kontoinhaber ohne eigenen technischen Zugang, d. h. deren HAM-Konto ausschließlich “co-managed“ wird. Zweitens:

Deutsche Bundesbank, Zentrale, Z 14-11
Wilhelm-Epstein-Straße 14, 60431 Frankfurt am Main, Telefon: 069 9566-3224
info@bundesbank.de, www.bundesbank.de, SWIFT: MARK DE FF

…

Die sogenannte „Selbstzertifizierungserklärung“ ist grundsätzlich von einer Führungskraft (Vorstands- oder vergleichbare Ebene) mit Verantwortung für den entsprechenden Geschäftsbereich sowie für den Bereich der Informationstechnologie (IT) zu unterschreiben. Ab Ende 2019 müssen kritische Teilnehmer (und nur diese!) die „Selbstzertifizierungserklärung“ zusätzlich von ihrer externen oder internen Revision unterzeichnen lassen. Die überwiegende Mehrheit von Ihnen hat jedoch den Status eines nicht-kritischen Teilnehmers und somit ist die Unterzeichnung durch die externe oder interne Revision dann nicht notwendig. Institute, die von uns als kritische Teilnehmer eingestuft wurden, sind über die betreffende Änderung bereits gesondert informiert worden. Für HAM-Kontoinhaber bei der Bundesbank (mit eigenem technischem Zugang) gelten die gleichen Sicherheitsanforderungen wie für nicht-kritische Teilnehmer.

Einzelheiten über die Klassifizierung „kritische versus nicht-kritische Teilnehmer“ entnehmen Sie bitte der jeweils aktuellen Fassung des Leitfadens für TARGET2-Nutzer (derzeit aktuell ist Version 11.0, Stand: November 2017, Seite 60 ff.):

https://www.bundesbank.de/Redaktion/DE/Standardartikel/Aufgaben/Unbarer_Zahlungsverkehr/target2_veroeffentlichungen_leitfaden.html

Hinweis: Die in diesem Rundschreiben bekannt gemachten Neuerungen werden ab der kommenden Version des Leitfadens (Version 12.0) enthalten sein.

Die genaue Beschreibung der sogenannten „Selbstzertifizierungserklärung“ inklusive der einzelnen Sicherheitsanforderungen sowie das entsprechende „Selbstzertifizierungsformular“, kurz Meldeformular genannt, sind diesem Rundschreiben beigefügt: Sicherheitsanforderungen (siehe Anlage 1), Meldeformular (siehe Anlage 2).

Das Meldeformular ist von allen Teilnehmern an TARGET2-Bundesbank auszufüllen: von kritischen wie nicht-kritischen Teilnehmern sowie von HAM-Kontoinhabern bei der Bundesbank, die einen eigenen technischen Zugang zur TARGET2-Gemeinschaftsplattform haben. Die Erklärung ist dabei, unabhängig davon, ob für den Zugang zu TARGET2 ein (externer) technischer Dienstleister genutzt wird, von jedem Institut selbst abzugeben.

Rechtzeitig vor dem konkreten Meldetermin werden wir alle an TARGET2-Bundesbank teilnehmenden Institute sowie alle betroffenen HAM-Kontoinhaber bei der Bundesbank auf dem Postweg anschreiben und darum bitten, das Meldeformular auszufüllen, zu unterschreiben und uns bis zum Abgabetermin (voraussichtlich Mitte Dezember 2018) zukommen zu lassen. Bis zu dieser gesonderten Aufforderung bitten wir Sie, sich bereits mit der „Selbstzertifizierungserklärung“ vertraut zu machen, jedoch noch keine Meldeformulare bei uns einzureichen.

Deutsche Bundesbank, Zentrale, Z 14-11
Wilhelm-Epstein-Straße 14, 60431 Frankfurt am Main, Telefon: 069 9566-3224
info@bundesbank.de, www.bundesbank.de, SWIFT: MARK DE FF

Selbstverständlich werden wir Sie fortlaufend und umfassend über alle weiteren Entwicklungen zu diesem Thema informieren. Die Mitarbeiterinnen und Mitarbeiter der Kundenbetreuungsservices (KBS) an den jeweiligen Standorten der Hauptverwaltungen der Bundesbank sind gerne bereit, Ihre Fragen zum Thema „Selbstzertifizierungspflicht“ zu beantworten.

Mit freundlichen Grüßen

Deutsche Bundesbank
Schrade Heid

DEUTSCHE BUNDESBANK 58

Beglaubigt:
M. Bayer
Tarifbeschäftigte

Anlagen

Deutsche Bundesbank, Zentrale, Z 14-11
Wilhelm-Epstein-Straße 14, 60431 Frankfurt am Main, Telefon: 069 9566-3224
info@bundesbank.de, www.bundesbank.de, SWIFT: MARK DE FF

Anlage 1 (DE)

Anforderung 1.1: Informationssicherheitspolitik

Die Geschäftsführung sollte einen klaren sicherheitspolitischen Kurs festlegen, der im Einklang mit den Geschäftszielen steht; darüber hinaus sollte sie sich zur Informationssicherheit verpflichten und diese fördern, indem sie eine in der gesamten Organisation geltende Strategie ausarbeitet und aufrechterhält.

Anforderung 1.2: Interne Organisation

Um die Umsetzung einer Informationssicherheitsstrategie innerhalb der Organisation anzustoßen und zu überwachen, sollte ein Steuerungsrahmen geschaffen werden. Die Geschäftsführung sollte der Informationssicherheitsstrategie zustimmen, Sicherheitsrollen zuweisen sowie die Implementierung der entsprechenden Strategie innerhalb der gesamten Organisation koordinieren und überprüfen.

Anforderung 1.3: Externe Parteien

Die Sicherheit der Informationen und informationsverarbeitenden Einrichtungen einer Organisation sollte nicht durch die Einführung von Produkten externer Parteien verringert werden. Der Zugang externer Parteien zu den informationsverarbeitenden Stellen der Organisation sollte in jedem Fall kontrolliert werden. Sofern externe Parteien einen Zugang benötigen oder Produkte und Dienstleistungen externer Parteien erforderlich sind, sollte eine Risikoprüfung erfolgen, um die sicherheitsrelevanten Auswirkungen zu ermitteln und die Kontrollanforderungen zu bestimmen. Die Kontrollen sollten mit der externen Partei vereinbart und vertraglich festgelegt werden.

Anforderung 1.4: Vermögensverwaltung (Asset Management)

Alle organisationseigenen Werte (z. B. Hard- und Software) sollten erfasst und einem Eigentümer namentlich zugeordnet sein. Die Zuständigkeit für die Aufrechterhaltung angemessener Kotrollen ist festzulegen. **ANMERKUNG:** Der Eigentümer kann, soweit angemessen, die Durchführung bestimmter Kontrollen delegieren, er ist jedoch weiterhin für den ordnungsgemäßen Schutz der organisationseigenen Werte verantwortlich.

Anforderung 1.5: Klassifizierung von Informationen

Damit ersichtlich ist, ob, mit welcher Priorität und in welchem Umfang Informationen während ihrer Verwendung zu schützen sind, sollten Informationen klassifiziert werden. Mithilfe eines Klassifizierungsschemas sind angemessene Schutzstufen zu definieren und die Notwendigkeit spezieller Maßnahmen im Umgang mit bestimmten Informationen zu kommunizieren.

Anforderung 1.6: Personelle Sicherheit

Welche Mitarbeiter für Sicherheitsfragen verantwortlich sind, sollte bereits vor Einstellung dieser Mitarbeiter in einer entsprechenden Stellenbeschreibung benannt und in den jeweils geltenden vertraglichen Bedingungen festgehalten werden. Alle Nutzer, bei denen es sich um Bewerber, Vertragspartner oder Dritte handelt, sollten hinreichend überprüft werden, besonders bei sensiblen Stellen bzw. Aufträgen. Bewerber, Vertragspartner und Dritte, die informationsverarbeitende Einrichtungen nutzen, sollten eine Vereinbarung unterzeichnen, in der ihre Sicherheitsrollen und Verantwortlichkeiten festgelegt sind. Es sollte gewährleistet sein, dass alle Mitarbeiter, Vertragspartner und Dritte für den Sicherheitsaspekt hinreichend sensibilisiert sind. Zur Minimierung möglicher Sicherheitsrisiken sollten sie an Fortbildungen und Schulungen zu Sicherheitsverfahren und dem korrekten Umgang mit informationsverarbeitenden Einrichtungen teilnehmen. Es sollte ein formelles Disziplinarverfahren geschaffen werden, das bei Verletzung von Sicherheitsbestimmungen zur Anwendung kommt. Das Ausscheiden eines Mitarbeiters, Vertragspartners oder Dritten bzw. dessen Wechsel innerhalb der Organisation muss durch Zuweisung entsprechender Verantwortlichkeiten gesteuert werden, und es ist zu gewährleisten, dass sämtliche Betriebsmittel zurückgegeben und alle Zugangsberechtigungen entzogen werden.

Anforderung 1.7: Physische und umgebungsbezogene Sicherheit

Kritische oder sensible informationsverarbeitende Einrichtungen sind in Sicherheitsbereichen unterzubringen, die durch eine genau festgelegte Sicherheitszone sowie entsprechende Sicherheitsbarrieren und Zutrittskontrollen geschützt sind. Sie sollten physisch vor unrechtmäßigem Zugang sowie Zerstörung und Manipulation geschützt sein.

Die Betriebsmittel sollten vor physischen und umgebungsbezogenen Bedrohungen geschützt werden. Um das Risiko eines unerlaubten Zugriffs auf Informationen zu mindern sowie Schäden und Verluste zu verhindern, ist es erforderlich, dass sämtliche Betriebsmittel (auch solche, die nicht am Standort verwendet werden) geschützt sind und ein Schutz gegen das Entfernen von Eigentum besteht. Zur

Abwehr physischer Bedrohungen und zum Schutz der zugehörigen Infrastruktur wie der Stromversorgung und der Verkabelung können Sondermaßnahmen erforderlich sein.

Anforderung 1.8: Betriebsmanagement

Für die Steuerung und den Betrieb sämtlicher informationsverarbeitender Einrichtungen sind Verantwortlichkeiten und Verfahren festzulegen.

Was die Betriebsprozesse betrifft, sollten bei Bedarf die Verantwortlichkeiten aufgeteilt werden, um das Risiko eines fahrlässigen oder vorsätzlichen Systemmissbrauchs zu verringern.

Die betrieblichen Anforderungen an neue Systeme sind festzulegen, zu dokumentieren und vor ihrer Abnahme und Verwendung zu testen. Es müssen Maßnahmen getroffen werden, um den Eintritt von Schadsoftware und nicht autorisiertem mobilen Programmcode zu verhindern bzw. aufzudecken. Für Software und informationsverarbeitende Einrichtungen besteht die Gefahr, dass sie durch das Eindringen von Schadsoftware wie Computerviren, Netzwerkwürmern, trojanischen Pferden und logischen Bomben geschädigt werden. Die Nutzer sollten für diese Gefahren sensibilisiert werden. Die verantwortlichen Personen sollten Mechanismen einrichten, wo dies angemessen erscheint, um das Eindringen von Schadsoftware zu verhindern bzw. aufzudecken und diese Software zu entfernen, sowie Maßnahmen treffen, um mobile Programmcodes zu kontrollieren.

Es müssen Routineverfahren eingerichtet werden, um die vereinbarten Backup-Maßnahmen sowie die Strategie zur Sicherung der Daten und zur Erprobung ihrer zeitnahen Wiederherstellung umzusetzen.

Um Netzwerke, die sich über eine gesamte Organisation erstrecken können, sicher zu verwalten, muss dem Datenverkehr, rechtlichen Aspekten sowie der Überwachung und dem Schutz besondere Beachtung geschenkt werden. Des Weiteren sind unter Umständen zusätzliche Kontrollmechanismen zum Schutz sensibler Daten, die über öffentliche Netzwerke geleitet werden, erforderlich. Speichermedien sollten kontrolliert und physisch geschützt werden.

Damit Dokumente, Computermedien, Ein- und Ausgabedaten sowie Systemdokumentationen nicht unerlaubt eingesehen, verändert, entfernt oder zerstört werden können, sind entsprechende betriebliche Verfahren zu etablieren.

Ein Austausch von Informationen und Software zwischen verschiedenen Organisationen sollte auf Basis einer formellen Austauschrichtlinie erfolgen und im Rahmen von Austauschvereinbarungen durchgeführt werden. Zudem sind die einschlägigen Rechtsvorschriften einzuhalten. Verfahren und Standards sollen festgelegt werden, durch die in der Übertragung befindliche Informationen sowie physische Medien mit solchen Informationen geschützt werden.

Die Systeme sind zu überwachen und Informationssicherheitsereignisse zu melden. Es empfiehlt sich der Einsatz von Betreiberprotokollen und Fehlerprotokollen, um sicherzustellen, dass Probleme im Bereich des Informationssystems erkannt werden.

Eine Systemüberwachung sollte gegeben sein, um die Wirksamkeit der eingeführten Kontrollmechanismen zu überprüfen und die Übereinstimmung mit einem entsprechenden Zugangsmodell zu verifizieren.

Anforderung 1.9: Zugangskontrolle

Der Zugang zu Informationen, informationsverarbeitenden Einrichtungen und Geschäftsprozessen sollte auf Basis von Betriebs- und Sicherheitsanforderungen kontrolliert werden. Die Bestimmungen zur Zugangskontrolle sollten den Regelungen zur Informationsweitergabe und Autorisierung Rechnung tragen.

Um die Zuweisung von Rechten zum Zugriff auf Informationssysteme und -dienste zu kontrollieren, müssen formelle Verfahren etabliert werden. Diese Verfahren sollten den gesamten Lebenszyklus des Nutzerzugangs abdecken – angefangen von der Erstregistrierung neuer Nutzer bis hin zur endgültigen Abmeldung von Nutzern, die keinen Zugang mehr benötigen.

Zu beachten ist insbesondere auch die Notwendigkeit, im Bedarfsfall die Zuweisung von Rechten zum bevorrechtigten Zugang zu kontrollieren, mit denen Nutzer Systemkontrollen umgehen können.

Die Nutzer sollten auf ihre Verantwortung zur Aufrechterhaltung wirksamer Zugangskontrollen hingewiesen werden, insbesondere was die Verwendung von Passwörtern und die Sicherheit der Benutzerausstattung betrifft.

Der Grundsatz des aufgeräumten Schreibtischs und leeren Bildschirms sollte umgesetzt werden, um das Risiko eines unberechtigten Zugangs oder der Beschädigung von Unterlagen, Medien und informationsverarbeitenden Einrichtungen zu verringern.

Der Zugang zu internen wie auch externen vernetzten Diensten ist zu kontrollieren. Wenn Nutzer Zugang zu Netzwerken und Netzwerkdiensten erhalten, darf dies nicht die Sicherheit der Netzwerkdienste beeinträchtigen, d. h. es sollte gewährleistet werden, dass geeignete Schnittstellen zwischen dem Netzwerk der Organisation und den Netzwerken anderer Organisationen und öffentlichen Netzwerken eingerichtet sind, geeignete Authentifizierungsverfahren für Nutzer und Betriebsmittel angewandt werden und die Zugangskontrollen zu den Informationsdiensten umgesetzt werden.

Die Sicherheitseinrichtungen sollten so eingesetzt werden, dass der Zugang zu Betriebssystemen nur autorisierten Nutzern gewährt wird. Diese Einrichtungen sollten in der Lage sein, autorisierte Nutzer zu authentifizieren, erfolgreiche und fehlgeschlagene Systemauthentifizierungsversuche aufzuzeichnen, die Verwendung spezieller Systemsonderrechte zu dokumentieren und Alarm auszulösen, wenn Systemsicherheitsbestimmungen verletzt werden; des Weiteren sollten geeignete Möglichkeiten zur Authentifizierung vorhanden sein, und die Verbindungszeit der Nutzer sollte gegebenenfalls begrenzt werden können.

Der logische Zugriff auf die Software und die Informationen einer Anwendung sollte auf autorisierte Nutzer beschränkt werden. Beim Einsatz des Mobile Computing sollte das Risiko, das mit der Arbeit in einer ungeschützten Umgebung einhergeht, besonders berücksichtigt und für geeigneten Schutz gesorgt werden.

Bietet die Organisation Telearbeit an, sollten Schutzmaßnahmen am Telearbeitsplatz getroffen werden, und es sollte gewährleistet sein, dass geeignete Vorkehrungen für diese Arbeitsmethode bestehen.

Anforderung 1.10: Beschaffung, Entwicklung und Wartung von Informationssystemen

Zu Informationssystemen zählen Betriebssysteme, Infrastruktur, Branchenanwendungen, Standardanwendungen, Dienste und von Nutzern entwickelte Programme. Vor der Entwicklung und/oder Implementierung von Informationssystemen sollten die Sicherheitsanforderungen ermittelt und vereinbart werden.

Zur Gewährleistung einer korrekten Verarbeitung sollten geeignete Kontrollen in die Anwendungen, auch in solche, die von Benutzern entwickelt wurden, integriert werden. Die Validierung von Ein- und Ausgabedaten und intern verarbeiteten Daten sollte Bestandteil dieser Kontrollen sein. Zusätzliche Kontrollen sind eventuell für Systeme erforderlich, die sensible, wertvolle oder kritische Informationen verarbeiten oder diese beeinflussen. Solche Kontrollen sind auf Basis der Sicherheitsanforderungen und einer Risikoprüfung festzulegen.

Es sollte eine Leitlinie zur Anwendung von Kryptografie entwickelt werden, um die Vertraulichkeit, Authentizität und Integrität von Informationen zu schützen. Zur Unterstützung derartiger Maßnahmen sollte die Verwaltung kryptografischer Schlüssel geregelt sein.

Der Zugang zu Systemdateien und zum Quellcode sollte kontrolliert werden; IT-Projekte und Supportmaßnahmen sind in sicherer Form durchzuführen. Die Organisation sollte dafür sorgen, dass sensible Daten in Testumgebungen nicht frei zugänglich sind. Projekt- und Supportumgebungen sind einer strengen Kontrolle zu unterstellen.

Für den Umgang mit Schwachstellen sollten wirksame, systematische und reproduzierbare Verfahren entwickelt werden, deren Wirksamkeit durch Messungen bestätigt wird. In diese Überlegungen sollten alle Betriebssysteme und genutzten Anwendungen einbezogen werden.

Anforderung 1.11: Informationssicherheit bei Beziehungen zu Anbietern

Um den Schutz des internen Komponentensystems des Teilnehmers zu gewährleisten, das zum Versand/Empfang von TARGET2-Zahlungen genutzt wird und den Anbietern zugänglich ist, sollten mit dem Anbieter die Anforderungen an die Informationssicherheit vereinbart und dokumentiert werden, um

die Risiken zu begrenzen, die mit dem Zugang des Anbieters zum internen Komponentensystem des Teilnehmers verbunden sind.

Anforderung 1.12: Umgang mit Vorfällen der Informationssicherheit und diesbezügliche Verbesserungen

Um einen konsistenten und wirksamen Ansatz für den Umgang mit Vorfällen der Informationssicherheit (wozu auch die Meldung von Sicherheitsereignissen und -schwachstellen zählt) sicherzustellen, sollten entsprechende Verantwortlichkeiten und Verfahren festgelegt werden, damit rasch, wirksam und ordnungsgemäß auf Vorfälle der Informationssicherheit reagiert werden kann.

Anforderung 1.13: Überprüfung der Erfüllung technischer Anforderungen

Das interne Komponentensystem eines Teilnehmers, das zum Versand/Empfang von TARGET2-Zahlungen verwendet wird (d. h. Back-Office-Systeme, interne Netzwerke und die Infrastruktur für die Verbindung zu externen Netzwerken), sollte regelmäßig darauf überprüft werden, ob die Informationssicherheitsstrategie und -standards der Organisation eingehalten werden.

Die folgenden Anforderungen (2.1 bis 2.6) beziehen sich auf das Business-Continuity-Management (**ANMERKUNG:** Diese Anforderungen betreffen ausschließlich kritische Teilnehmer).

Jeder TARGET2-Teilnehmer, der vom Eurosystem im Hinblick auf das reibungslose Funktionieren von TARGET2 als kritisch eingestuft wurde, muss über eine Strategie zur Aufrechterhaltung des Geschäftsbetriebs verfügen, die folgende Elemente aufweist:

Anforderung 2.1:

Business-Continuity-Pläne wurden erstellt, und Verfahren zu deren Aufrechterhaltung sind vorhanden.

Anforderung 2.2:

Es muss ein Ausweichstandort vorhanden sein.

Anforderung 2.3:

Das Risikoprofil des Ausweichstandorts muss sich von dem des Primärstandorts unterscheiden. Dies bedeutet, dass sich der Ausweichstandort a) in deutlicher Entfernung vom Primärstandort befinden muss und b) nicht von denselben Komponenten der physischen Infrastruktur abhängen darf. Dadurch wird das

Risiko minimiert, dass beide Standorte von derselben Störung betroffen sind. Der Ausweichstandort sollte beispielsweise an ein anderes Energieversorgungsnetz und eine andere Hauptfernmeldeleitung als der Primärstandort angeschlossen sein.

Anforderung 2.4:

Im Falle einer größeren Betriebsstörung, die dazu führt, dass auf den Primärstandort nicht zugegriffen werden kann und/oder für den Betrieb notwendige Mitarbeiter nicht verfügbar sind, muss der kritische Teilnehmer in der Lage sein, den normalen Betrieb vom Ausweichstandort aus wiederaufzunehmen und dort den Geschäftstag ordnungsgemäß abzuschließen und den/die folgenden Geschäftstag(e) zu beginnen.

Anforderung 2.5:

Es müssen Verfahren etabliert sein, die gewährleisten, dass die kritischsten Transaktionen während der Verlagerung vom Primärstandort auf den Ausweichstandort ausgeführt werden können.

Anforderung 2.6:

Die Fähigkeit, Betriebsstörungen zu bewältigen, wird mindestens einmal jährlich geprüft, und alle diesbezüglich wichtigen Mitarbeiter werden angemessen geschult. Der Abstand zwischen den Tests sollte nicht länger als ein Jahr sein.

Annex 1 (EN)

Requirement 1.1: Information security policy

Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy applicable across the organisation.

Requirement 1.2: Internal organisation

A management framework should be established to initiate and monitor the implementation of an information security policy within the organisation. Management should approve the information security policy, assign security roles and coordinate and review the implementation of the policy across the organisation.

Requirement 1.3: External parties

The security of the organisation's information and information processing facilities should not be reduced by the introduction of external party products. Any access to the organisation's information processing facilities by external parties should be controlled. When access by external parties or products/services from external parties is/are required, a risk assessment should be carried out to determine the security implications and control requirements. Controls should be agreed and defined in an agreement with the external party.

Requirement 1.4: Asset management

All organisational assets (e.g. hardware, software) should be accounted for and have a nominated owner. The responsibility for the maintenance of appropriate controls should be assigned. **NOTE:** The implementation of specific controls can be delegated by the owner as appropriate, but the owner remains responsible for the proper protection of the assets.

Requirement 1.5: Information classification

Information should be classified to indicate the need, priorities and degree of protection required when handling it. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.

Requirement 1.6: Human resources security

Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs. Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities. An adequate level of awareness should be ensured among all employees, contractors and third party users, and education and training in security procedures and the correct use of information processing facilities should be provided to them, to minimise possible security risks. A formal disciplinary process for handling security breaches should be established. Responsibilities should be in place to ensure an employee's, contractor's or third party user's exit from or transfer within the organisation is managed, and that the return of all equipment and the removal of all access rights are completed.

Requirement 1.7: Physical and environmental security

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage and interference.

Equipment should be protected from physical and environmental threats. Protection of equipment (including that used off-site) and the removal of property is necessary to reduce the risk of unauthorised access to information and to guard against loss or damage. Special measures may be required to protect against physical threats and to safeguard supporting facilities such as the electrical supply and cabling infrastructure.

Requirement 1.8: Operations management

Responsibilities and procedures should be established for the management and operation of all information processing facilities.

As regards operating procedures, segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

The operational requirements of new systems should be established, documented and tested prior to their acceptance and use. Precautions must be taken to prevent and detect the introduction of malicious code and unauthorised mobile code. Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses and logic bombs, and users should be made aware of its dangers. Managers should, where appropriate, introduce controls to prevent, detect and remove malicious code and control mobile code.

Routine procedures should be established to implement the agreed backup policy and strategy for taking backup copies of data and rehearsing their timely restoration.

The secure management of networks, which may span organisation boundaries, requires careful consideration to be given to dataflow, legal implications, monitoring and protection. Additional controls may also be required to protect sensitive information passing over public networks. Data storage media should be controlled and physically protected.

Appropriate operating procedures should be established to protect documents, computer media, input/output data and system documentation from unauthorised disclosure, modification, removal and destruction.

Exchanges of information and software between organisations should be based on a formal exchange policy and carried out in line with exchange agreements, and should be compliant with any relevant legislation. Procedures and standards should be established to protect information and physical media containing information in transit.

Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure that information system problems are identified.

System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

Requirement 1.9: Access control

Access to information, information processing facilities and business processes should be controlled on the basis of business and security requirements. Access control rules should take account of policies for information dissemination and authorisation.

Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final deregistration of users that no longer require access.

Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights which allow users to override system controls.

Users should be made aware of their responsibility for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

A clear desk and clear screen policy should be implemented to reduce the risk of unauthorised access or damage to papers, media and information processing facilities.

Access to both internal and external networked services should be controlled. User access to networks and network services should not compromise the security of the network services, i.e. it should be ensured that appropriate interfaces are in place between the organisation's network and networks owned by other organisations and public networks, appropriate authentication mechanisms are applied for users and equipment, and controls of user access to information services are enforced.

Security facilities should be used to restrict access to operating systems to authorised users. The facilities should be capable of authenticating authorised users, recording successful and failed system authentication attempts, recording the use of special system privileges, issuing alarms when system security policies are breached, providing appropriate means for authentication and, where appropriate, restricting users' connection times.

Logical access to application software and information should be restricted to authorised users. When mobile computing is used, the risks of working in an unprotected environment should be considered and appropriate protection applied.

In the case of teleworking the organisation should apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

Requirement 1.10: Information systems acquisition, development and maintenance

Information systems include operating systems, infrastructures, business applications, off-the-shelf products, services and user-developed applications. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.

Appropriate controls should be built into applications, including user-developed applications, to ensure correct processing. These controls should include the validation of input data, internal processing and output data. Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls should be determined on the basis of security requirements and risk assessment.

A policy should be developed on the use of cryptographic controls to protect the confidentiality, authenticity and integrity of information. Key management should be in place to support the use of cryptographic controls.

Access to system files and program source code should be controlled and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments. Project and support environments should be strictly controlled.

Technical vulnerability management should be implemented in an effective, systematic and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems and any other applications in use.

Requirement 1.11: Information security in supplier relationships

To ensure protection of the participant's internal component system used for sending/receiving TARGET2 payments that is accessible by suppliers, information security requirements for mitigating the risks associated with supplier's access to the participant's internal component system should be agreed with the supplier and documented.

Requirement 1.12: Management of information security incidents and improvements

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses, management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

Requirement 1.13: Technical compliance review

A participant's internal component system used for sending/receiving TARGET2 payments (i.e. back office systems, internal networks and external network connectivity infrastructure) should be regularly reviewed for compliance with the organization's information security policies and standards.

The following requirements (2.1 to 2.6) relate to business continuity management (**NOTE:** these requirements are applicable to critical participants only).

Each TARGET2 participant classified by the Eurosystem as being critical for the smooth functioning of the TARGET2 system must have a business continuity strategy in place comprising the following elements.

Requirement 2.1:

Business continuity plans have been developed and procedures for maintaining them are in place.

Requirement 2.2:

An alternate operational site must be available.

Requirement 2.3:

The risk profile of the alternate site must be different from that of the primary site, meaning that the alternate site must (i) be a significant distance away from and (ii) not depend on the same physical infrastructure components as the primary business location. This minimises the risk of both sites being affected by the same event. For example, the alternate site should be on a different power grid and central telecommunication circuit from those of the primary business location.

Requirement 2.4:

In the event of a major operational disruption rendering the primary site inaccessible and/or critical staff unavailable, the critical participant must be able to resume normal operations from the alternate site, where it must be possible to properly close the business day and open the following business day(s).

Requirement 2.5:

Procedures must be in place to ensure that the most critical business transactions can be performed while business is being moved from the primary to the alternate site.

Requirement 2.6:

The ability to cope with operational disruptions must be tested at least once a year and critical staff must be aptly trained. The maximum period between tests should not exceed one year.

Anlage 2 (DE)

Selbstzertifizierungserklärung

1. Kontaktdaten

In der nachstehenden Tabelle sind der Name des TARGET2-Teilnehmers und die Kontaktdaten der Person anzugeben, die als Ansprechpartner zur Verfügung steht, wenn weitere Informationen benötigt werden.

Name des TARGET2-Teilnehmers	
Anschrift	
BIC/Kontonummer	
Kontaktperson (Name in Druckbuchstaben)	
Kontaktperson (Telefon)	
Kontaktperson (E-Mail)	

2 Selbstzertifizierende Organisation

TARGET2-Teilnehmer können sich entweder direkt oder über eine gemeinsame technische Infrastruktur mit der TARGET2-Gemeinschaftsplattform verbinden. In diesem Zusammenhang ist zu klären, ob alle TARGET2-Teilnehmer, die eine gemeinsame technische Infrastruktur nutzen, eine Selbstzertifizierungs-erklärung bei ihrer Zentralbank einreichen müssen, oder ob nur der TARGET2-Teilnehmer, der diese gemeinsame technische Infrastruktur betreibt, eine solche Erklärung vorlegen muss. Eine multinational tätige Bank verfügt beispielsweise über eine Reihe von Zweigstellen; dabei nutzen alle Zweigstellen die von der Zentrale betriebene technische Infrastruktur. Hier stellt sich die Frage, ob alle Zweigstellen eine Selbstzertifizierungserklärung bei der Zentralbank, mit der sie eine Geschäftsbeziehung unterhalten, einreichen müssen oder nur die Zentrale als Betreiberin der technischen Infrastruktur.

Die Sicherheitsanforderungen gelten nicht nur für eine zentrale technische Plattform, sondern grundsätzlich auch für die Zweigstellen einer Bank, selbst wenn diese eine zentrale Infrastruktur nutzen. Die physischen Sicherheitskontrollen beispielsweise sind sowohl von dem TARGET2-Teilnehmer, der die gemeinsame technische Infrastruktur betreibt, als auch von der Zweigstelle zu gewährleisten. Der Anwendungsbereich ist jedoch unterschiedlich. Der als Betreiber der gemeinsamen technischen Infrastruktur fungierende TARGET2-Teilnehmer muss Kontrollen zum Schutz des Rechenzentrums durchführen, während eine Zweigstelle dafür Sorge zu tragen hat, dass die für die Anbindung an die gemeinsame technische Infrastruktur verwendeten Komponenten angemessen geschützt sind.

Bei den obigen Ausführungen handelt es sich lediglich um ein Beispiel, das veranschaulichen soll, warum jeder einzelne TARGET2-Teilnehmer eine Selbstzertifizierungserklärung bei der Zentralbank, mit der er eine Geschäftsbeziehung unterhält, vorlegen muss.

Darüber hinaus ist es wichtig zu beachten, dass es letztendlich in der Hauptverantwortung des jeweiligen TARGET2-Teilnehmers liegt, genau zu prüfen, welche Sicherheitsanforderungen für die spezifischen technischen und organisatorischen Strukturen seiner Institution gelten. Wenn ein TARGET2-Teilnehmer seinen Geschäftsbetrieb ganz oder teilweise an einen Dritten (z. B. ein Servicebüro) ausgelagert hat, muss er sicherstellen, dass dieser Dritte die vom Eurosystem für TARGET2-Teilnehmer festgelegten Sicherheitsanforderungen erfüllt.

Zusammenfassend ist festzuhalten, dass alle TARGET2-Teilnehmer (d. h. sowohl direkte Teilnehmer als auch Nebensysteme) eine Selbstzertifizierungserklärung bei der Zentralbank, mit der sie eine Geschäftsbeziehung unterhalten, einreichen sollten. Wenn Teile des Geschäftsbetriebs und/oder der für den Zugang zu TARGET2 verwendeten technischen Infrastruktur von verschiedenen TARGET2-Teilnehmern gemeinsam genutzt werden, hat jeder TARGET2-Teilnehmer seine eigene Selbstzertifizierungserklärung bei der jeweiligen Zentralbank vorzulegen. Wenn eine oder mehrere Sicherheitsanforderungen nicht anwendbar sind, muss der TARGET2-Teilnehmer dies in der unten stehenden Tabelle zur Prüfung der Umsetzung angeben. Ferner sollte in der entsprechenden, in der Selbstzertifizierungserklärung enthaltenen Rubrik (mit der Bezeichnung „Umsetzungsfortschritt“) erläutert werden, warum eine bestimmte Sicherheitsanforderung nicht anwendbar ist.

In Zweifelsfällen werden die TARGET2-Teilnehmer gebeten, sich mit der Zentralbank, mit der sie eine vertragliche Beziehung unterhalten, in Verbindung zu setzen, um den Umfang ihrer Selbstzertifizierung zu klären.

3. Servicebüro

Neben einer direkten Anbindung an die TARGET2-Gemeinschaftsplattform kann die Anbindung auch über ein Servicebüro erfolgen.

Ist Ihre Organisation über ein Servicebüro an die TARGET2-Gemeinschaftsplattform angeschlossen?	Ja	Nein
Wenn ja, geben Sie bitte den Namen des Servicebüros an.		

4. Prüfung der Umsetzung (Compliance Check)

Für jede der vom Eurosystem festgelegten Anforderungen muss der TARGET-Nutzer in der Selbstzertifizierungserklärung angeben, inwieweit diese umgesetzt wurden.

Im Falle der Nichtumsetzung (Stufe 2 oder 3) dieser Anforderungen sind in der entsprechenden, in der Selbstzertifizierung enthaltenen Rubrik (mit der Bezeichnung „Umsetzungsfortschritt“) die größten Risiken[1] zu beschreiben. Darüber hinaus sollte ein Aktionsplan zur Behebung des Problems beigefügt sowie der vorgesehene Termin für die Umsetzung jeder einzelnen Maßnahme benannt werden. Die zuständige Zentralbank muss diese Angaben auswerten und die Durchführung der Maßnahmen zur Risikominderung überwachen.

[1] Ein großes Risiko könnten beispielsweise sein: unzureichende Vorkehrungen gegen Denial-of-Service-Angriffe, eine nicht vorhandene unterbrechungsfreie Stromversorgung u. Ä.

Umsetzungsgrad

TARGET2-Teilnehmer sind verpflichtet anzugeben, inwieweit die vom Eurosystem in seiner Funktion als TARGET2-Systembetreiber festgelegten Anforderungen zum Informationssicherheitsmanagement umgesetzt wurden.

Durch Ankreuzen der entsprechenden Kästchen gibt der TARGET2-Teilnehmer bekannt, inwieweit die Vorgaben umgesetzt wurden.

- **Vollständige Umsetzung:** Der Teilnehmer hat die in der Selbstzertifizierungserklärung aufgeführte Anforderung vollständig umgesetzt.
- **Stufen der Nichtumsetzung:**
    - **Stufe 1:** keine wesentlichen Bereiche der Nichtumsetzung; es kann mit hinreichender Sicherheit davon ausgegangen werden, dass dies nicht zu einer Beeinträchtigung der reibungslosen Funktion von TARGET2 und/oder negativen Auswirkungen auf andere Systemteilnehmer führen wird.
    - **Stufe 2:** wesentliche Bereiche der Nichtumsetzung; eine Zusicherung wie in Stufe 1 kann nicht gegeben werden; eine Ausnutzung der ermittelten Schwachstellen könnte zu einer Beeinträchtigung der reibungslosen Funktion von TARGET2 und/oder negativen Auswirkungen auf andere Systemteilnehmer führen.
    - **Stufe 3:** Nichtumsetzung; eine Zusicherung wie in Stufe 1 kann nicht gegeben werden; eine Ausnutzung der ermittelten Schwachstellen würde zu einer erheblichen Beeinträchtigung der reibungslosen Funktion von TARGET2 und/oder negativen Auswirkungen auf andere Systemteilnehmer führen.

	Vollständige Umsetzung	Nichtumsetzung			Nicht anwendbar
		Stufe 1	Stufe 2	Stufe 3	
1 Anforderungen an das Informations-sicherheits-management					
Anforderung 1.1	☐	☐	☐	☐	☐
Anforderung 1.2	☐	☐	☐	☐	☐
Anforderung 1.3	☐	☐	☐	☐	☐
Anforderung 1.4	☐	☐	☐	☐	☐
Anforderung 1.5	☐	☐	☐	☐	☐
Anforderung 1.6	☐	☐	☐	☐	☐
Anforderung 1.7	☐	☐	☐	☐	☐
Anforderung 1.8	☐	☐	☐	☐	☐
Anforderung 1.9	☐	☐	☐	☐	☐
Anforderung 1.10	☐	☐	☐	☐	☐
Anforderung 1.11	☐	☐	☐	☐	☐
Anforderung 1.12	☐	☐	☐	☐	☐
Anforderung 1.13	☐	☐	☐	☐	☐

2. Anforderungen an das Business-Continuity-Management (HINWEIS: gilt nur für kritische Teilnehmer)					
Anforderung 2.1	☐	☐	☐	☐	☐
Anforderung 2.2	☐	☐	☐	☐	☐
Anforderung 2.3	☐	☐	☐	☐	☐
Anforderung 2.4	☐	☐	☐	☐	☐
Anforderung 2.5	☐	☐	☐	☐	☐
Anforderung 2.6	☐	☐	☐	☐	☐
Welcher Informations-sicherheitsstandard wird für Sicherheits-kontrollen hauptsächlich verwendet?					

Umsetzungsfortschritt

Sofern Bereiche der Nichtumsetzung gemäß Stufe 2 oder 3 ermittelt wurden, ist auch der folgende Abschnitt auszufüllen.

Geben Sie bitte für jede in der obigen Tabelle als „nicht anwendbar“ gekennzeichnete Anforderung eine kurze Begründung an. Anmerkungen:
Wurden Risiken infolge einer Nichtumsetzung (gemäß Stufe 2 oder 3) der Anforderungen 1.1 bis 1.13 und 2.1 bis 2.6 ermittelt? Anmerkungen:
Welche Schritte werden eingeleitet, damit eine vollständige Umsetzung der Anforderungen erreicht wird bzw. der Grad der Nichterfüllung nur noch der Stufe 1 entspricht? Anmerkungen:
Bis zu welchem Datum soll die vollständige Umsetzung erreicht werden bzw. der Grad der Nichterfüllung nur noch der Stufe 1 entsprechen? Anmerkungen:

5. Unterzeichner

Die Selbstzertifizierungserklärung ist von einer Führungskraft (auf Vorstandsebene oder einer vergleichbaren Ebene) zu unterzeichnen, die für den entsprechenden Geschäftsbereich verantwortlich ist. Angesichts der wichtigen Rolle, die der Informationstechnologie (IT) zukommt, sollte die Selbstzertifizierung zusätzlich von einer Führungskraft (ebenfalls auf Vorstands- oder vergleichbarer Ebene) aus dem IT-Bereich des Teilnehmers unterzeichnet werden. Wenn eine Führungskraft sowohl für den Geschäfts- als auch den IT-Bereich zuständig ist, reicht eine Unterschrift aus.

Bei kritischen TARGET2-Teilnehmern ist die Selbstzertifizierung mit Wirkung ab dem Jahr 2019 zusätzlich vom (externen oder internen) Revisor des jeweiligen kritischen Teilnehmers zu unterzeichnen.

Zertifizierung

Die Unterzeichner bestätigen, dass sie die in dieser Selbstzertifizierungserklärung aufgeführten Anforderungen gelesen und verstanden haben. Die Erklärung gilt für ein Jahr und muss spätestens ein Jahr nach dem Datum der ersten Unterschrift erneuert werden.

Die Unterzeichner bestätigen, dass die in der Erklärung enthaltenen Informationen ein zutreffendes und genaues Bild der aktuellen Situation vermitteln. Sie bestätigen ferner, dass die Erklärung unter ihrer Leitung und Kontrolle erstellt wurde und die ausgewiesenen Angaben von qualifiziertem Personal ordnungsgemäß erhoben und ausgewertet wurden. Alle Angaben sind nach bestem Wissen und Gewissen der Unterzeichner zutreffend, korrekt und vollständig. Den Unterzeichnern ist bekannt, dass die Einreichung dieser Daten eine wesentliche Verpflichtung ist und die Einreichung falscher, ungenauer oder irreführender Angaben einen Verstoß gegen Artikel 34 Absatz 2 Buchstabe c der TARGET2-Leitlinie darstellt, was ein Grund für den Ausschluss des betreffenden Instituts von TARGET2 ist.

Die Unterzeichner bestätigen ferner, dass es in ihrer Organisation einen Mechanismus gibt, der sicherstellt, dass die Einhaltung der Anforderungen im folgenden Jahr gewährleistet bleibt, oder – sofern die Maßnahmen noch nicht vollständig umgesetzt wurden – dass angemessene Vorkehrungen getroffen werden, die zufriedenstellende Fortschritte bei der Durchführung der im Aktionsplan aufgeführten Punkte ermöglichen.

Erste Unterschrift

Name der Führungskraft aus dem Geschäftsbereich (in Druckbuchstaben):	
Titel:	
Datum:	
Unterschrift:	

Zweite Unterschrift

Name der Führungskraft aus dem IT-Bereich (in Druckbuchstaben):	
Titel:	
Datum:	
Unterschrift:	

Unterschrift des Revisors – auszufüllen von kritischen TARGET2-Teilnehmern (ab 2019)

Name des Prüfers (in Druckbuchstaben):	
Titel (Angabe, ob interner oder externer Revisor):	
Datum:	
Unterschrift:	

Diese Selbstzertifizierungserklärung bitte zurücksenden an

Name der Zentralbank:	
Anschrift:	
Kontaktperson:	

Annex 2 (EN)

Self-certification statement

1. **Contact details**

In the following the name of the TARGET2 participant and contact details of a person to be contacted in case further information is required should be provided.

Name of the TARGET2 participant	
Address	
BIC/account number	
Contact person (name) (print)	
Contact person (telephone)	
Contact person (e-mail)	

2. **Self-certifying organisation**

TARGET2 participants can connect to the TARGET2 SSP either directly or via a shared technical infrastructure. In this context it needs to be clarified whether those TARGET2 participants using a shared technical infrastructure have to submit a self-certification statement to their central bank or only the TARGET2 participant which is operating the technical infrastructure which is shared with others. For example, a multi-country bank participating in TARGET2 has a number of branches. These branches are all using the technical infrastructure operated by the head office. The question here is whether all branches have to submit the self-certification statement to the central bank with which they are having a business relationship or only the head office which is operating the technical infrastructure.

The security requirements are not exclusively applicable to a centralised technical platform. Rather they are generally applicable also to the branches of a bank even if they are using a

centralised infrastructure. For example, the controls related to physical security have to be met by both the TARGET2 participant hosting the shared technical infrastructure and the branch. However, the scope will be different. The TARGET2 participant hosting the shared technical infrastructure will have to implement controls protecting the data centre while a branch will have to make sure that the components used for connecting to the shared technical infrastructure are properly protected.

It should be noted that the above is just an example used to illustrate the need for each individual TARGET2 participant to submit a self-certification statement to the central bank with which it is having business relationship.

Furthermore it is important to understand that it is ultimately the key responsibility of the respective TARGET2 participant to thoroughly assess which security requirements are applicable to the specific and unique technical as well as organisational set-up of its institution. In the event a TARGET2 participant has outsourced (parts of) its operations to a third party (for example a service bureau), the TARGET2 participant must seek assurance that the third party is compliant with the security requirements set-up by the Eurosystem for TARGET2 participants.

In conclusion, each TARGET2 participant (i.e. direct participants and ancillary systems) should submit a self-certification statement to the central bank with which it is having business relationship. If parts of the operations and/or technical infrastructure used for the TARGET2 access are shared by different TARGET2 participants, each TARGET2 participant should submit its own self-certification statement to its respective central bank. In case one or more security requirements are not applicable, the TARGET2 participant should indicate this in the compliance check table below. Moreover, it should be explained in the relevant box included in the self-certification statement (labelled “towards compliance”) why a specific security requirement is not applicable.

In case of doubt, TARGET2 participants are kindly invited to contact the central bank with which they are having a contractual relationship in order to clarify the scope of their self-certification statement.

3. Service Bureau

Apart from establishing a direct connection to the TARGET2 single shared platform (SSP) participants can connect through a Service Bureau.

Is your organisation connected to the TARGET2 SSP via a Service Bureau?	Yes	No
If yes, please indicate the name of the Service Bureau		

4. Compliance check

For each of the requirements specified by the Eurosystem the TARGET2 user must report its level of compliance in the self-certification statement.

In the event of non-compliance at level 2 or level 3 with these requirements, a description of the major risks[1] should be included in the relevant box included in the self-certification statement (labelled “towards compliance”). Furthermore, an action plan for rectifying the situation and the planned dates for implementing each particular measure should be included. This information must be evaluated and the implementation of risk-mitigating measures monitored by the central bank responsible.

[1] A major risk could be, for instance, insufficient measures against denial of service attacks, uninterruptible power supply not in place, etc.

Level of compliance

TARGET2 participants are required to indicate their level of compliance with the requirements regarding information security management specified by the Eurosystem in its capacity as TARGET2 system operator.

The TARGET2 participant should indicate its level of compliance by ticking the appropriate box.

- **Full compliance:** the participant fully complies with the requirement as described in the self-certification statement.
- **Levels of non-compliance**
    - **Level 1:** no significant areas of non-compliance; reasonable assurance can be given that this does not have the potential to harm the smooth functioning of TARGET2 and/or adversely affect other system participants.
    - **Level 2:** significant areas of non-compliance; reasonable assurance cannot be given, and an exploitation of the vulnerabilities identified could harm the smooth functioning of TARGET2 and/or adversely affect other system participants.
    - **Level 3:** non-compliance; reasonable assurance cannot be given, and an exploitation of the vulnerabilities identified would significantly harm the smooth functioning of TARGET2 and/or adversely affect other system participants.

	Full compliance	Non-compliance			Not applicable
		Level 1	Level 2	Level 3	
1 Information security management requirements					
Requirement 1.1	☐	☐	☐	☐	☐
Requirement 1.2	☐	☐	☐	☐	☐
Requirement 1.3	☐	☐	☐	☐	☐
Requirement 1.4	☐	☐	☐	☐	☐
Requirement 1.5	☐	☐	☐	☐	☐
Requirement 1.6	☐	☐	☐	☐	☐
Requirement 1.7	☐	☐	☐	☐	☐
Requirement 1.8	☐	☐	☐	☐	☐
Requirement 1.9	☐	☐	☐	☐	☐
Requirement 1.10	☐	☐	☐	☐	☐
Requirement 1.11	☐	☐	☐	☐	☐
Requirement 1.12	☐	☐	☐	☐	☐
Requirement 1.13	☐	☐	☐	☐	☐

2. Business continuity management requirements (NOTE: applicable to critical participants only)					
Requirement 2.1	☐	☐	☐	☐	☐
Requirement 2.2	☐	☐	☐	☐	☐
Requirement 2.3	☐	☐	☐	☐	☐
Requirement 2.4	☐	☐	☐	☐	☐
Requirement 2.5	☐	☐	☐	☐	☐
Requirement 2.6	☐	☐	☐	☐	☐
Which information security standard is mainly used for security controls?					

Towards compliance

If any areas of non-compliance at level 2 or level 3 have been identified, the following section must be completed.

For each requirement indicated as "not applicable" in the table above, please provide a short explanation why it is not applicable. Comments:
Have any risks resulting from non-compliance at level 2 or level 3 with requirements 1.1 to 1.13 and 2.1 to 2.6 been identified? Comments:
What steps will be taken to achieve full compliance or reduce non-compliance to level 1? Comments:
By when will full compliance or non-compliance at level 1 be achieved? Comments:

5. Signatory

The self-certification statement should be signed by a senior official (i.e. at board level or equivalent) responsible for the relevant business area. Given the heavy reliance on information technology (IT), the self-certification statement should, in addition, be signed by a senior official (also at board level or equivalent) responsible for the IT department within the organisation of the participant. If a senior official is responsible for both, the business area and the IT department, one signature is sufficient.

With effect from 2019 for critical participants the self-certification statement should also be signed by the (external or internal) auditor of the critical TARGET2 participant.

Certification

The signatories confirm that they have read and understood the requirements outlined in this self-certification statement. The statement is valid for one year and is due for renewal one year after the date of the first signature.

The signatories certify that the information contained in the statement represents a true and accurate picture of the current situation. They further certify that the statement has been prepared under their direction and supervision and that qualified personnel properly gathered and evaluated the information provided. The submitted information is, to the best of the signatories' knowledge and belief, true, accurate and complete. The signatories are aware that the submission of this information is a material obligation and that submitting false, inaccurate or misleading information constitutes a breach of Article 34 (2) (c) of the TARGET2 Guideline, which is one of the grounds for termination of an institution's participation in TARGET2.

Finally, the signatories confirm that their organisation has a mechanism in place to ensure that it will remain in compliance over the coming year or, if compliance has not yet been achieved, that appropriate measures will be taken to make satisfactory progress on the work items listed in the action plan.

First signature

Name of official from the business area (print)	
Title	
Date	
Signature	

Second signature

Name of official from IT department (print)	
Title	
Date	
Signature	

Auditor signature – for completion by critical TARGET2 participants (note as of 2019)

Name of Auditor (print)	
Title (indicate whether internal or external auditor)	
Date	
Signature	

This self-certification statement should be returned to

Name of central bank	
Address	
Contact person	