Nbr	Chapter/ Annex nbr	Page	Line	Topic	Comments
1				General Observation	It would be desirable to have a definition of what are the 'core' services
2	2.3	10	table	Indicative list of standardised securities	Recommend that Repo should be included in the list
3	2.60	15	24	Interaction with external CSD	
4	2.60	16	1	Scenario 1	Requires better definition of a cross CSD settlement process and particularly the link process when a CSD is not in T2S. As part of ecomonic business case T2S should advise practical examples and actual business impact in terms of cost, time and complexity
5	3.1.2.7	11	7	End-of-day-procedures	DVP deadline – recommendation is a single deadline of 16:00 with CSDs free to set their own deadlines
6	5.46	20	13	High priority	The section on triggering cancellations at the end of the recycling period needs to be clarified (should be harmonised)
7	7.2.2.3	15	9		There would be a requirement for a threshold above which participants may apply Top priority status. Recommend a procedure to monitor the use of the priority setting functionality to ensure that it is not abused
8	7	12	24	Cut-off time for DVP Settlements	Propose that partial settlements is a continuous process given that other events may be contingent upon settlement such as securities lending, onward deliveries, etc. If partial settlement is required to be limited to a certain operating window, then it is suggested that it should be triggered more than 15 minutes before the EOD
9	Annex 14.3.1	12	11	Requirements on T2S	'It has to be decided for each CSD which data may be administered directly, without being routed via a CSD'. Suggest that CSDs agree upon a consistent practice
10	13.2	6	3	Night-time settlement communication	Recommend that Users receive settlement confirmations in the overnight batches as and when they occur, but have the option to receive the last trade status updates from the last of the night time batches thereby avoiding redundant messaging
11	15			Billing	Propose that the billing function should be a web-based application
12	18			Information Security Requirements	To provide User confidence recommend that there is a regular external audit of information risk controls
13	18.2.1.2	6	2	Information Security Framework	The Information Security Policy, and associated documentation, should be reviewed at least annually in-line with best practice. Policies should be clear on accountability. SOX controls could be used as a reference source
14	18.9.5.1	29	4	Change Control Procedures	Definition should include Information Owner / Asset Owner review and approval process, segregated code promotion, provision for emergency change, audit trail etc.
15	18.8.4.4	24	4	Remote diagnostic & config	Logical Access - Should be based on roles / least privilege principles, and subject to re certification. Connectivity standards should be defined for external / 3rd party access (may need to consider multi-factor authentication). Access should be adequately audit trailed (unique userid, date / time stamp, action performed etc.). Privileged access should be subject to breakglass controls. Passwords should be communicated securely
16	18.4.1.1	8	7	Inventory of assets	Need to define the information / asset classes, and labelling standards in order to determine appropriate risk treatment
17	18.7.6.2	17	19	Network controls	Stringent industry standard encryption controls should be applied to sensitive data so that it is adequately protected and purged from systems where possible
18	18.9.23	27	11	Message integrity	Data Integrity - Application should incorporate input validation rules. Requirements for confidentiality, integrity, non-repudiation of electronic messaging should be defined
19	18.7.9.2	20	6	Monitoring system use	Application should be subject to regular vulnerability / penetration testing to prevent the possibility of unauthorised access
20	18.7.8	18	13	Migration - introduction	Standards for connectivity should be defined. Requests for external connectivity should be subject to expert/senior management review and approval
21	18.7.5.1	17	8	Information back-up	Controls for offsite storage should be defined (encryption, secure storage etc.)
22	18.7.8.4	19	11	Electronic messaging	Recommend that 'appropriately protected' is further defined
23	18.11	31	11	Info security aspects of BC mgt	Scope should be defined to include people, process, and technology, and follow best practice guidelines (e.g. BS25999)
24	18.7.7.2	18	6	Disposal of media	Require further clarification of the process / standards applied to the secure removal / disposal of data
25	18.9.5.5.	29	15	Outsourced software development	Propose that documents clearly state that outsourced software development is to be consistent with T2S policies or ISO standards
26	18.10	30	5	Information security management	Recommend that details of the Information Security Management organisation be published as soon as it is practical to do so
27	19.040	4	2	T2S will have high level of resilience	T2S will have "rapid recovery and timely resumption of operation" capability. T2S.20.410 states this services will be resumed within 2 hours from the point of the *decision* to execute the DR. It is recommended that DR is implemented to ensure the resumption of operations within 2 hours from the time of *failure*
28	19.060	4	14	Syst & Appl S/W will be updated in parallel	Preference for synchronous updates as all databases will have the same real time information whereas with asynchronous updates, one region will always be slightly behind the other, usually only by a matter of minutes but during which time there's a risk that instructions might have been missed
29	19.190	6	7	Static & transactional data	Require further details about parallel processing re: horizontal and vertical scalability
30	20.030	4	5	Night downtime	Require clarification that instructions sent to T2S in the overnight down-time are queued for the next available batch
31	Annex 3	7	8	Proposal 32	Require confirmation that T2S will queue messages during maintenance windows
32	Annex 3	4	9	Proposal 18	Recommend one set of harmonised deadlines and schedules
33	Annex 3	4	21	Proposal 23	Require stronger commitment that CSDs will adopt procedures that would maximise the overnight settlement opportunities
34	Annex 3	7	8	Proposal 31	Recommend at least 3 overnight netting processes
35	Annex 3	9	12	Proposal 64	Require service standards, e.g. helpdesk available 24 hours, respond to queries within 1 hour, etc
36	Annex 3	9	19	Proposal 67	Harmonization and standardization decisions should be guided by the best practices across the markets. Furthermore, they should be visionary and be able to accommodate market evolution

37	Annex 11	3	5	Basic Issues	Direct participation criteria should be standard across all T2S CSDs
38	Annex 12	3	16	Introduction	
39	Annex 12	6	33	General Settlement	
40	Chapter 1	5	4	Principle 5	Stronger commitment required to encourage harmonisation. The use of phrases such as 'at least the same level of settlement functionality' reduces local pressure to simplify processes (Spain, Finland, Slovenia, Greece). Statement should say that harmonisation and consistency are the principle drivers not the retaining of local settlement practices
41	Chapter 1	5	21	Principle 7	Legal rules around the definition of settlement finality in Europe are arcane. Recommend that these national differences are clearly stated and request that regulators commit to converge to a common definition.