ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

Il processo della sicurezza delle informazioni nelle piccole e microimprese.

Come abbiamo adattato la Cybersecurity Framework del NIST per l'utilizzo nelle strutture di minori dimensioni

Stefano Toria
Toria Secure Systems GmbH – Zug, Switzerland

Roma 16/10/2017

Agenda

- Presentazione relatore
- Diciotto anni di esperienza con l'ISO 27001 (e BS7799 prima): successi e insuccessi in Italia e all’estero
- Obiettivi di sicurezza delle strutture di dimensioni minori
- Sviluppo di una metodologia semplificata e sua applicazione
- Conclusioni e prospettive
- Q&A
- Bibliografia

Agenda

- Presentazione relatore
- Diciotto anni di esperienza con l'ISO 27001 (e BS7799 prima): successi e insuccessi in Italia e all’estero
- Obiettivi di sicurezza delle strutture di dimensioni minori
- Sviluppo di una metodologia semplificata e sua applicazione
- Conclusioni e prospettive
- Q&A
- Bibliografia

Presentazione relatore

TÒRIA
SECURE SYSTEMS

Stefano Toria

1974-1989, analista programmatore freelance

1980, laurea in Economia e Commercio, Luiss Roma

1983-1992, docente a contratto, Informatica, Luiss Roma

1990-1992, «Virus», MCmicrocomputer

1991-1993, responsabile marketing ISP, MC-link Roma

1994-1997, Club sul Computer Crime, Ipacri, Roma

1999-2001, SecurTeam, Roma

2001-2005, direttore laboratorio software, InfoGuard, Orvieto

2006-2011, consulente e docente ISO 27001, InfoGuard, Zug (CH)

2012-2017, consulente e docente, Crypto AG, Steinhausen (CH)

2017- Toria Secure Systems GmbH, Zug (CH)

Agenda

- Presentazione relatore
- Diciotto anni di esperienza con l'ISO 27001 (e BS7799 prima): successi e insuccessi in Italia e all’estero
- Obiettivi di sicurezza delle strutture di dimensioni minori
- Sviluppo di una metodologia semplificata e sua applicazione
- Conclusioni e prospettive
- Q&A
- Bibliografia

Diciotto anni di esperienza con l'ISO 27001

- Primo contatto: SecurTeam, 1999
- Progetto sviluppo software tool per ISMS, su base BS7799
- Il contesto e i «grandi progetti»
- Sviluppo del tool e successo di mercato

Diciotto anni di esperienza con l'ISO 27001

- InfoGuard, Crypto AG e il mercato gov/mil
- Certificazioni e formazione: BS7799 e ISO 27001
- Lo standard come strumento di lavoro
- Risposta dei mercati: Italia, Svizzera, Medio Oriente

Diciotto anni di esperienza con l'ISO 27001

- Sviluppo del mercato
- «Troppo complicato, troppe risorse»
- Norma utilizzata come linea-guida per progetti non necessariamente di compliance

Diciotto anni di esperienza con l'ISO 27001

- Progetto particolare – *«Pet Project»*
  - Azienda molto piccola, 15 addetti
  - Servizi telematici alle imprese di assicurazioni
  - Trattamento dati personali *anche sensibili*
  - Gara d’appalto, il capitolato prevede la sicurezza delle inform.
  - L’azienda sceglie di certificarsi ISO 27001
  - Lavoro svolto in modalità «turbo», certificazione OK
  - Vinta gara

Agenda

- Presentazione relatore
- Diciotto anni di esperienza con l'ISO 27001 (e BS7799 prima): successi e insuccessi in Italia e all’estero
- ➡ Obiettivi di sicurezza delle strutture di dimensioni minori
- Sviluppo di una metodologia semplificata e sua applicazione
- Conclusioni e prospettive
- Q&A
- Bibliografia

Obiettivi di sicurezza

- Nel corso degli anni, divergenza tra aziende maggiori e PMI

- «Le piccole, medie e microimprese rappresentano il 99% di tutte le imprese dell'UE. Si contano circa 21 milioni di PMI, che danno lavoro a circa 133 milioni di persone» *(fonte: www.europarl.europa.eu)*

- «Le PMI, ossia le società con meno di 250 dipendenti, rappresentano oltre il 99% delle imprese commerciali in Svizzera e generano due terzi dei posti di lavoro nel paese» *(fonte: www.kmu.admin.ch)*

Obiettivi di sicurezza

- Aziende maggiori:
  - Hanno più facilmente strumenti di stima del patrimonio informativo
  - Hanno strutture IT articolate, policy e piani di sicurezza
  - Negli ultimi anni hanno messo in campo team di specialisti
  - Oppure ricorrono ai servizi di aziende specializzate
  - Diversi livelli di delega

Obiettivi di sicurezza

- Aziende minori:
  - Concentrazione di più funzioni in poche risorse
  - Strutture IT miste, su base volontaristica, BYOD
  - Risorse specialistiche scarse, esterne, o del tutto assenti
  - Rincorsa dell'emergenza, delega pressoché impossibile
  - Scarsa appetibilità per il mercato dei grandi player

Obiettivi di sicurezza

- Il mercato delle PMI in Svizzera
  - Agricoltura e allevamento
    - Utilizzo minimo o nullo di strumenti IT
  - Servizi finanziari e patrimoniali
  - Alberghiero e ristorazione
  - Studi professionali
  - Piccola industria (meccanica, elettronica)

Obiettivi di sicurezza

- Esigenze specifiche del mercato locale
  - Circolare FINMA 2008/21, «Rischi operativi – banche», All. 3
  - LPD
  - GDPR 2016/679
  - Varie disposizioni CO e leggi specifiche

Obiettivi di sicurezza

- Ampia disponibilità di informazioni dettagliate
  - MELANI
  - ETH Zurigo
  - Blog aziende specializzate

Agenda

- Presentazione relatore
- Diciotto anni di esperienza con l'ISO 27001 (e BS7799 prima): successi e insuccessi in Italia e all’estero
- Obiettivi di sicurezza delle strutture di dimensioni minori
- ➡ Sviluppo di una metodologia semplificata e sua applicazione
- Conclusioni e prospettive
- Q&A
- Bibliografia

Sviluppo di una metodologia semplificata

- L’attività ha preso l’avvio da due progetti specifici, entrambi in Svizzera Interna
- In entrambi i casi, attacco informatico da *ransomware*
  - distruzione totale di tutto il patrimonio informativo
  - fortunosa ricostruzione attraverso backup «abbastanza» recenti
- Lesson learned: «Bisogna fare qualcosa per non caderci più».

Sviluppo di una metodologia semplificata

- Assunto di partenza:

«Le PMI, in particolare le microimprese, non sono in grado di gestire da sé stesse il proprio processo della sicurezza, indipendentemente da quali e quante fonti di informazioni qualificate, dettagliate e semplificate siano disponibili gratis sul Web»

Sviluppo di una metodologia semplificata

- Proposta operativa
  - Migliorare la comprensione del concetto di «sicurezza»: tutela del patrimonio informativo dai rischi
  - Migliorare la comprensione del concetto di «patrimonio informativo» e di «rischi»
  - Migliorare la consapevolezza dei processi aziendali
  - Attrezzare un «processo trasversale» per garantire che in ogni attività sia presa in considerazione l’esigenza di sicurezza

Sviluppo di una metodologia semplificata

- Proposta metodologica
  - Utilizzare una versione semplificata della ISO 27001
  - Creare una versione semplificata della ISO 27001 *ad hoc*
  - Utilizzare una diversa metodologia
    - eventualmente semplificata

Sviluppo di una metodologia semplificata

- Adozione della Cybersecurity Framework del NIST

- Pro:
  - Framework di partenza semplificato
  - Interazioni tra diversi approcci già risolte
  - Approccio per passi discreti
  - Concreto e non accademico

- Contro:
  - Relativamente nuovo (2014)
  - Scarsa esperienza specifica locale
  - Necessità di (auto-)formazione

Sviluppo di una metodologia semplificata

- Creazione della base metodologica
  - Analisi del documento origine (NIST CSF)
  - Identificazione del livello di implementazione («Implementation Tier»)
    - Scelta del Tier 1: Parziale
  - Identificazione delle sottocategorie da considerare indispensabili nel contesto delle organizzazioni-campione
  - Attribuzione dei livelli di maturità obiettivi e riscontrati

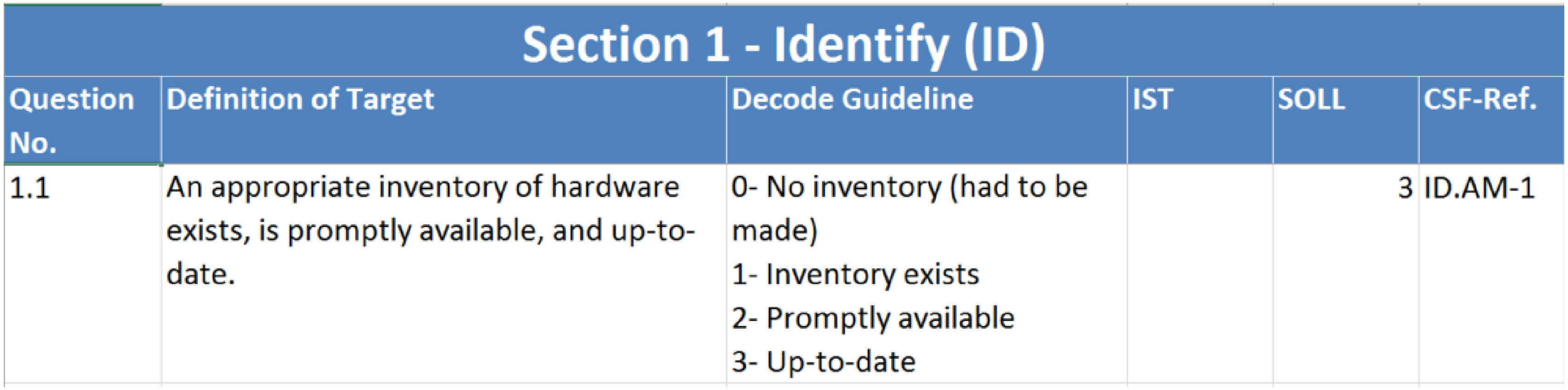
Sviluppo di una metodologia semplificata

- Metodo di acquisizione dei dati
  - Tiene conto delle specificità degli ambienti-campione
    - Uno studio legale e un’impresa di servizi tecnologici
  - Metodo adottato: intervista, escluse domande chiuse
  - In fase di acquisizione privilegiato l’aspetto umano
    - La valutazione dei dati acquisiti dipende dal consulente
    - Aspetto negativo, previsto lavoro specifico

Sviluppo di una metodologia semplificata

- Segue analisi delle singole sottocategorie selezionate, ristrutturate per le esigenze dei nostri progetti
  - La sequenza delle funzioni e categorie è la stessa del CSF
  - I livelli di maturità sono stati attribuiti in base a:
    - Esperienza del team
    - Requisiti di mercato dei clienti
  - Saranno soggetti a revisione

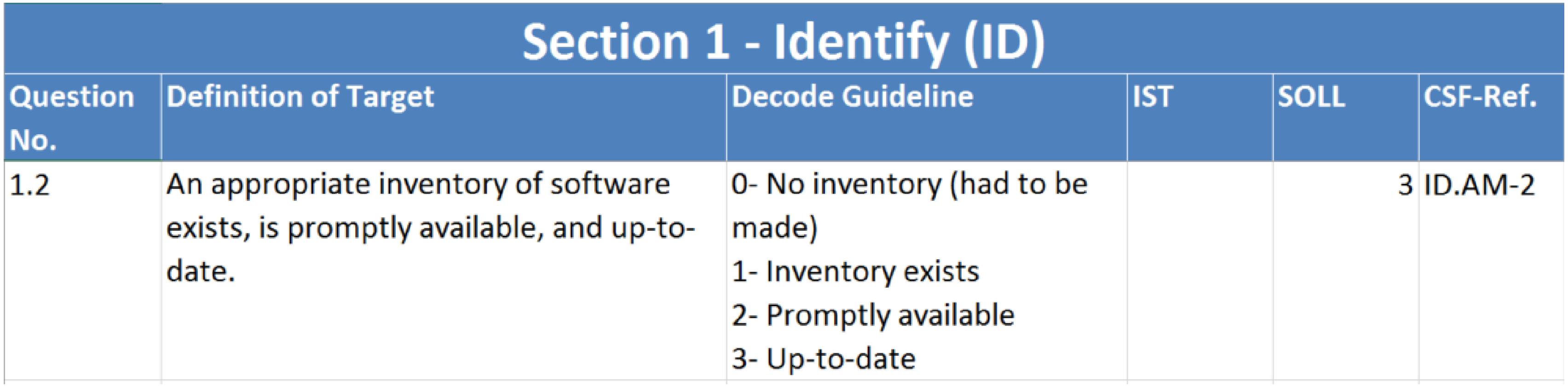
Sviluppo di una metodologia semplificata



Section 1 - Identify (ID)

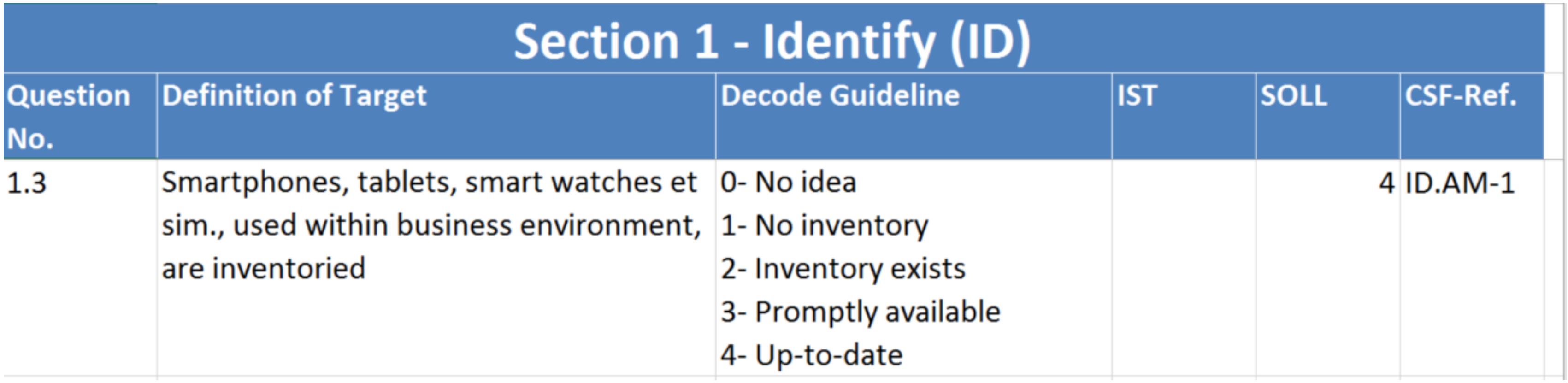
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.1	An appropriate inventory of hardware exists, is promptly available, and up-to-date.	0- No inventory (had to be made) 1- Inventory exists 2- Promptly available 3- Up-to-date		3	ID.AM-1

Sviluppo di una metodologia semplificata



Section 1 - Identify (ID)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.2	An appropriate inventory of software exists, is promptly available, and up-to-date.	0- No inventory (had to be made) 1- Inventory exists 2- Promptly available 3- Up-to-date		3	ID.AM-2

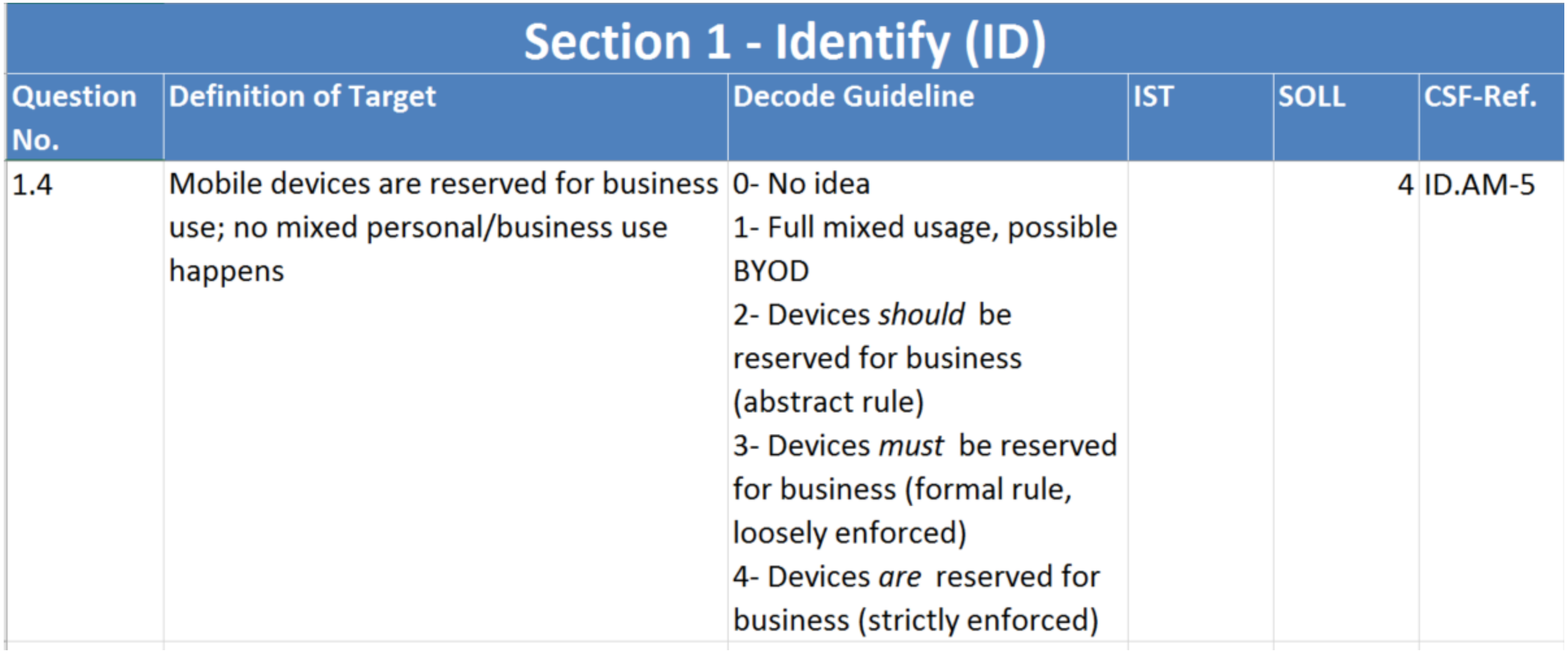
Sviluppo di una metodologia semplificata



Section 1 - Identify (ID)

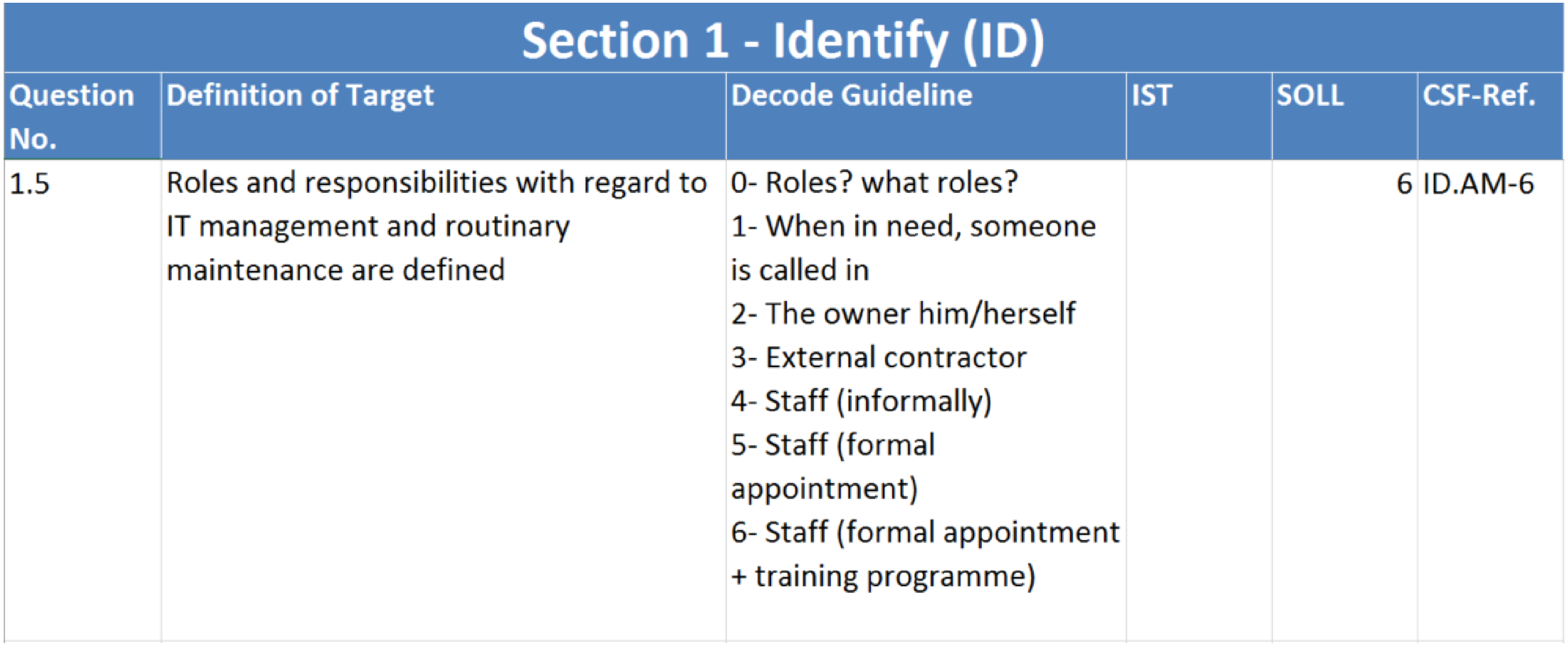
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.3	Smartphones, tablets, smart watches et sim., used within business environment, are inventoried	0- No idea 1- No inventory 2- Inventory exists 3- Promptly available 4- Up-to-date		4	ID.AM-1

Sviluppo di una metodologia semplificata



Section 1 - Identify (ID)					
Question No.	**Definition of Target**	**Decode Guideline**	**IST**	**SOLL**	**CSF-Ref.**
1.4	Mobile devices are reserved for business use; no mixed personal/business use happens	0- No idea 1- Full mixed usage, possible BYOD 2- Devices *should* be reserved for business (abstract rule) 3- Devices *must* be reserved for business (formal rule, loosely enforced) 4- Devices *are* reserved for business (strictly enforced)		4	ID.AM-5

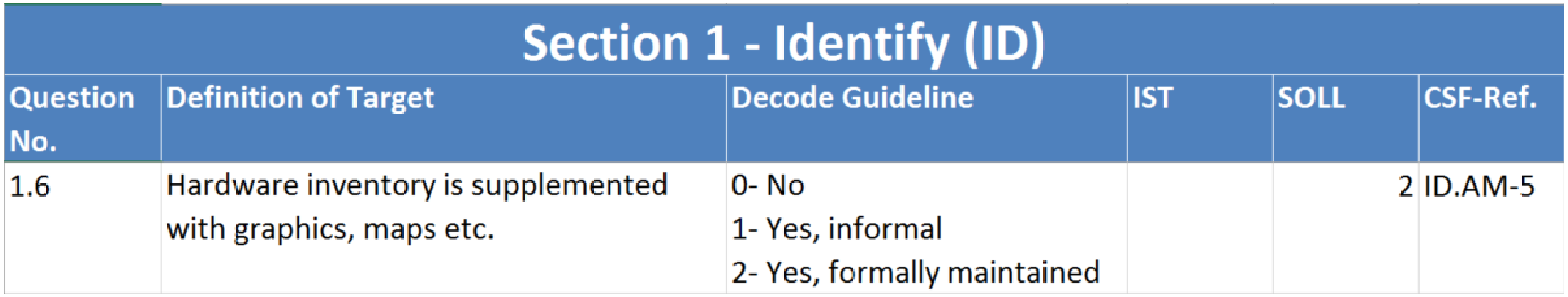
Sviluppo di una metodologia semplificata



Section 1 - Identify (ID)

Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.5	Roles and responsibilities with regard to IT management and routinary maintenance are defined	0- Roles? what roles? 1- When in need, someone is called in 2- The owner him/herself 3- External contractor 4- Staff (informally) 5- Staff (formal appointment) 6- Staff (formal appointment + training programme)		6	ID.AM-6

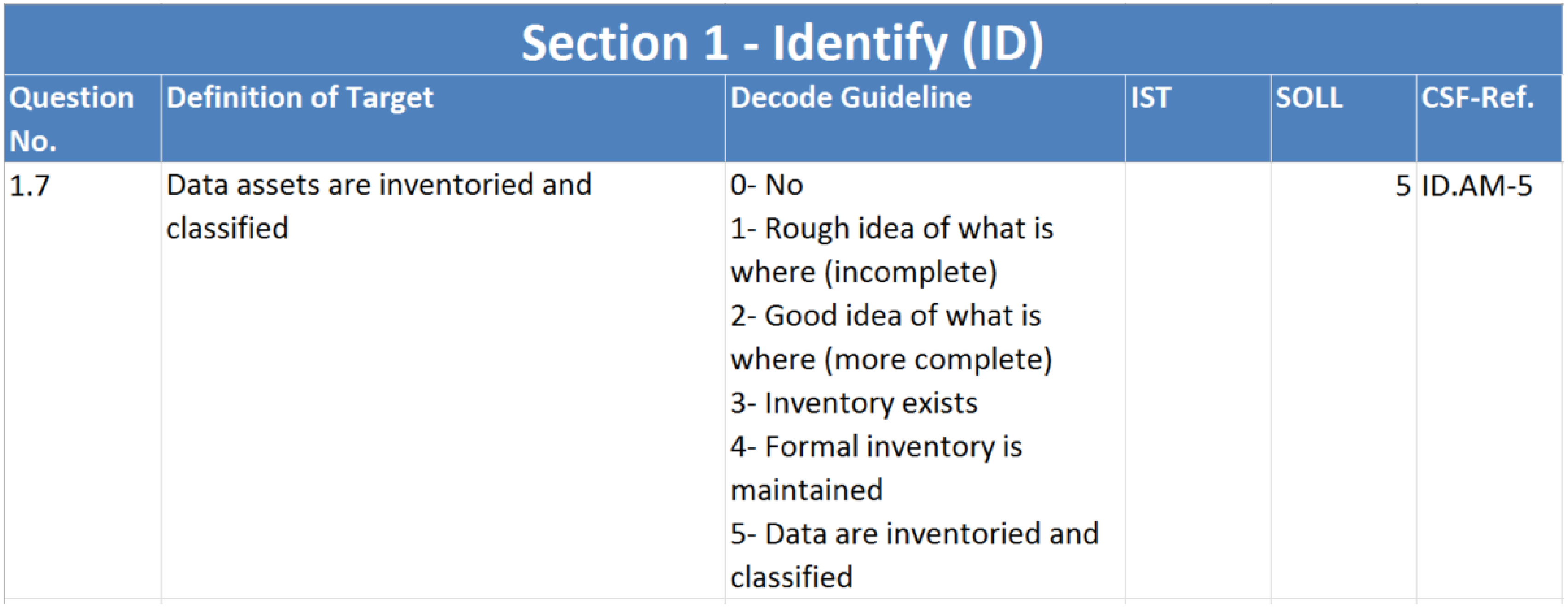
Sviluppo di una metodologia semplificata



Section 1 - Identify (ID)

Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.6	Hardware inventory is supplemented with graphics, maps etc.	0- No 1- Yes, informal 2- Yes, formally maintained		2	ID.AM-5

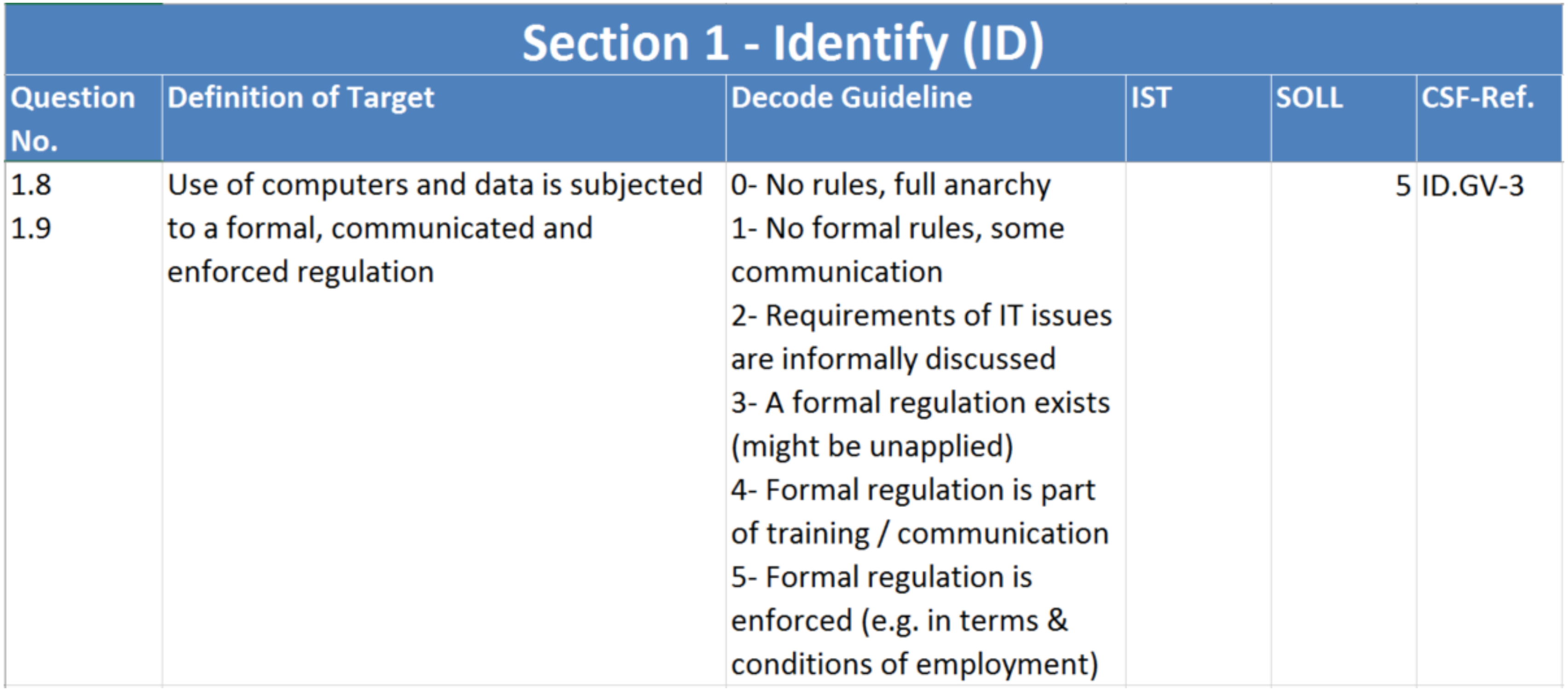
Sviluppo di una metodologia semplificata



Section 1 - Identify (ID)

Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.7	Data assets are inventoried and classified	0- No 1- Rough idea of what is where (incomplete) 2- Good idea of what is where (more complete) 3- Inventory exists 4- Formal inventory is maintained 5- Data are inventoried and classified		5	ID.AM-5

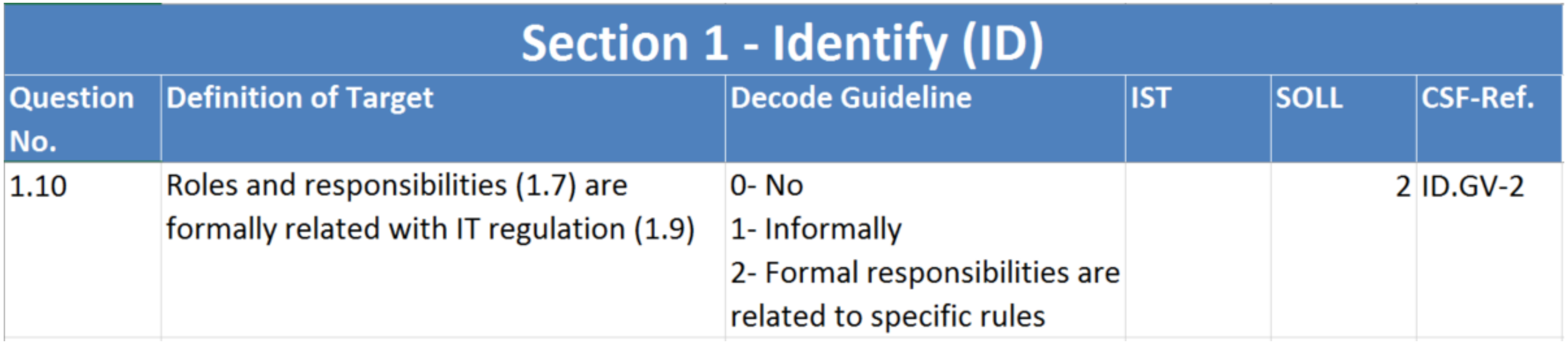
Sviluppo di una metodologia semplificata



Section 1 - Identify (ID)

Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.8 1.9	Use of computers and data is subjected to a formal, communicated and enforced regulation	0- No rules, full anarchy 1- No formal rules, some communication 2- Requirements of IT issues are informally discussed 3- A formal regulation exists (might be unapplied) 4- Formal regulation is part of training / communication 5- Formal regulation is enforced (e.g. in terms & conditions of employment)		5	ID.GV-3

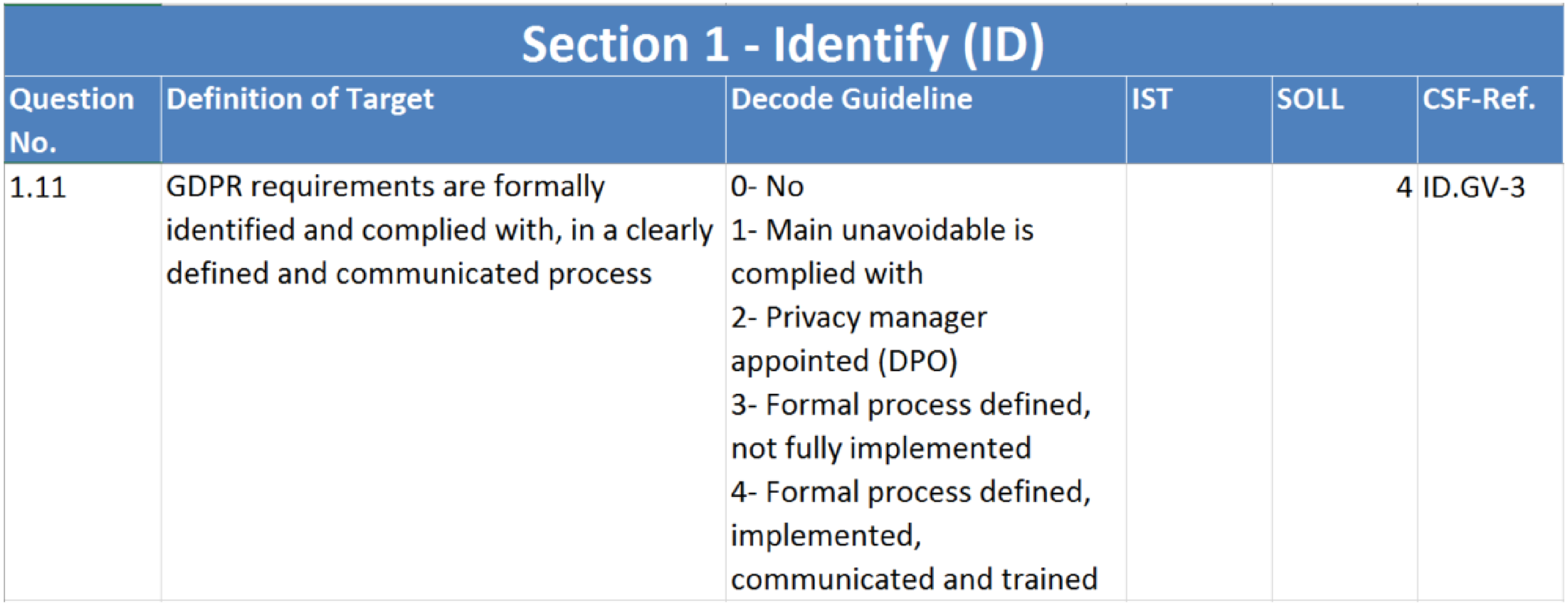
Sviluppo di una metodologia semplificata



Section 1 - Identify (ID)

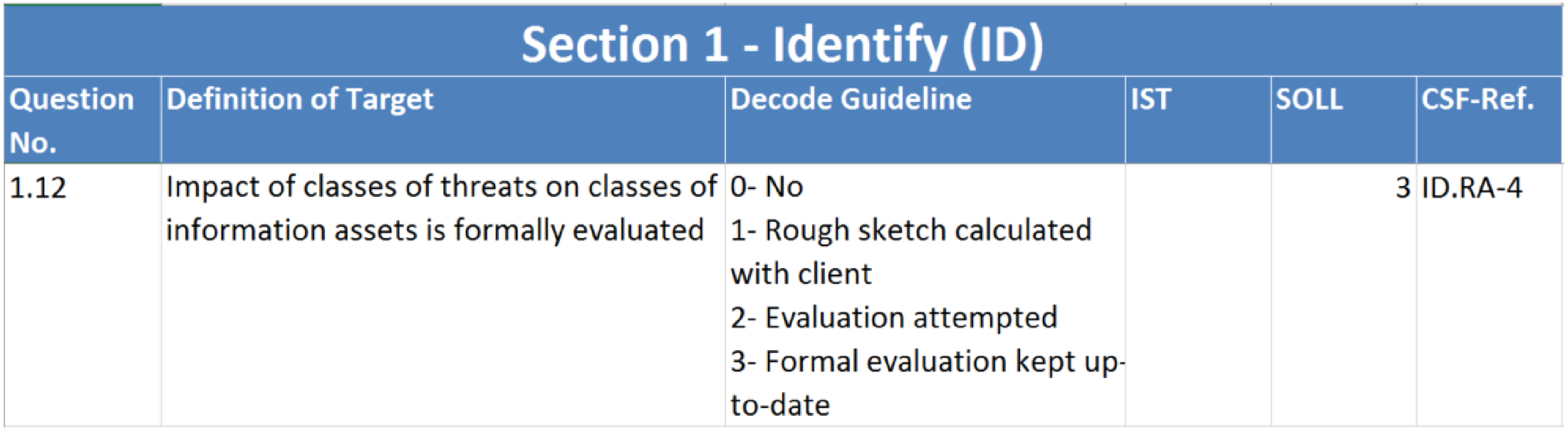
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.10	Roles and responsibilities (1.7) are formally related with IT regulation (1.9)	0- No 1- Informally 2- Formal responsibilities are related to specific rules		2	ID.GV-2

Sviluppo di una metodologia semplificata



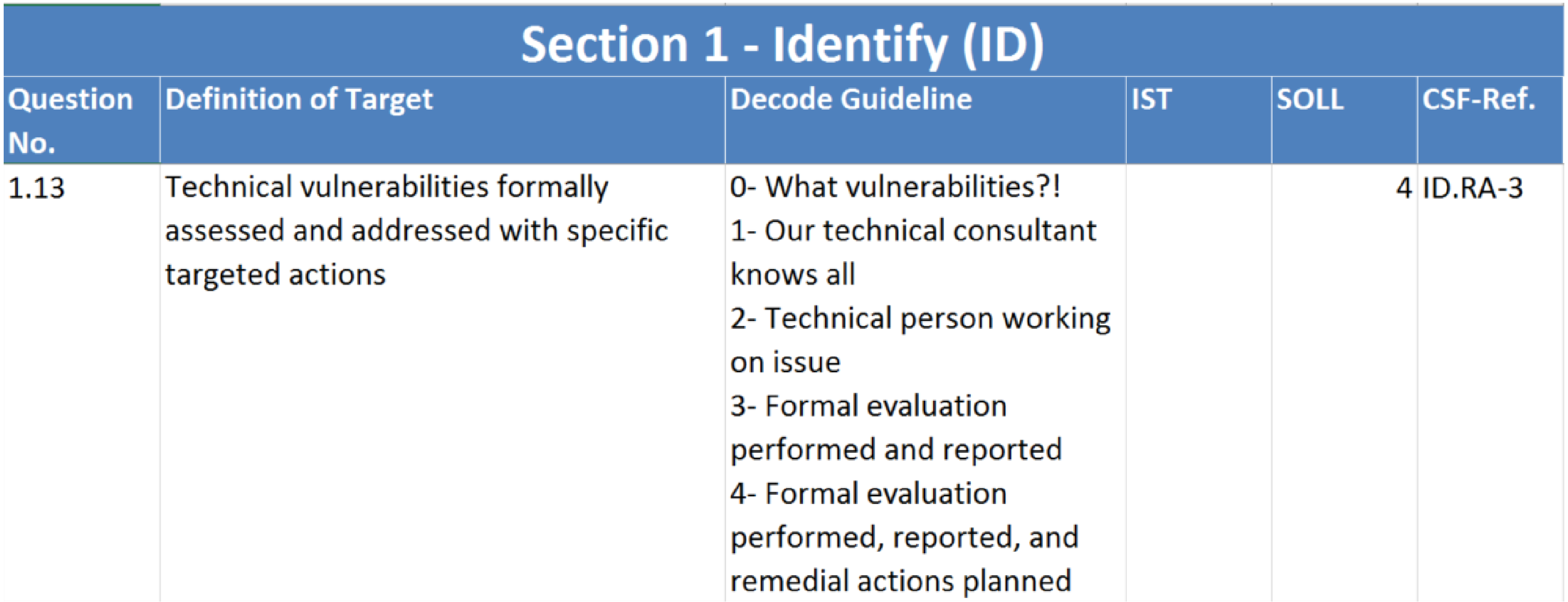
Section 1 - Identify (ID)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.11	GDPR requirements are formally identified and complied with, in a clearly defined and communicated process	0- No 1- Main unavoidable is complied with 2- Privacy manager appointed (DPO) 3- Formal process defined, not fully implemented 4- Formal process defined, implemented, communicated and trained		4	ID.GV-3

Sviluppo di una metodologia semplificata



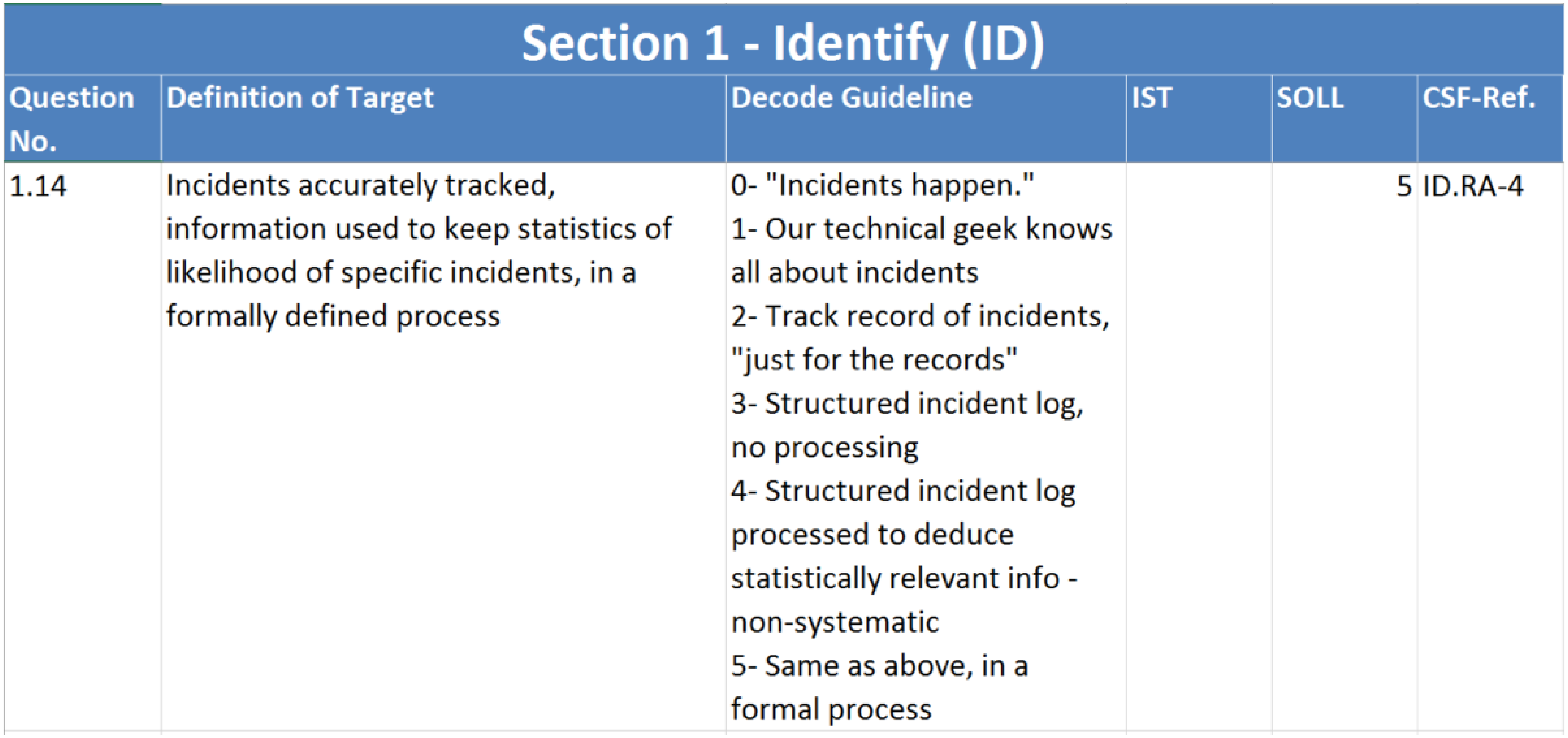
Section 1 - Identify (ID)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.12	Impact of classes of threats on classes of information assets is formally evaluated	0- No 1- Rough sketch calculated with client 2- Evaluation attempted 3- Formal evaluation kept up-to-date		3	ID.RA-4

Sviluppo di una metodologia semplificata



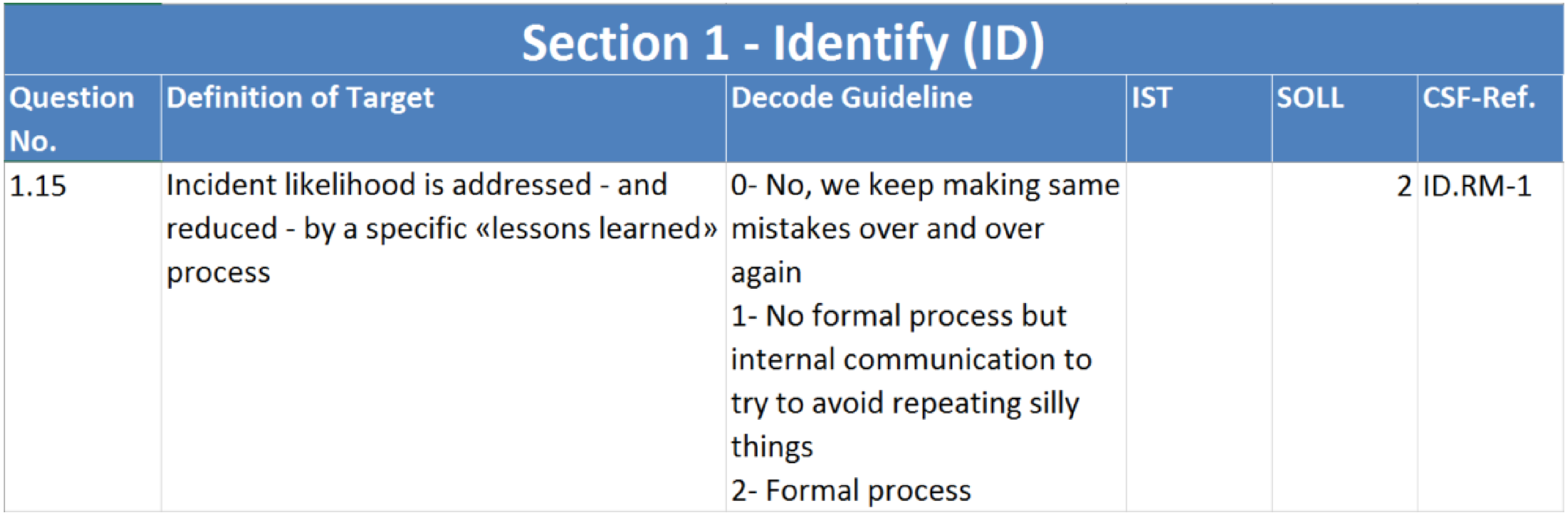
Section 1 - Identify (ID)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.13	Technical vulnerabilities formally assessed and addressed with specific targeted actions	0- What vulnerabilities?! 1- Our technical consultant knows all 2- Technical person working on issue 3- Formal evaluation performed and reported 4- Formal evaluation performed, reported, and remedial actions planned		4	ID.RA-3

Sviluppo di una metodologia semplificata



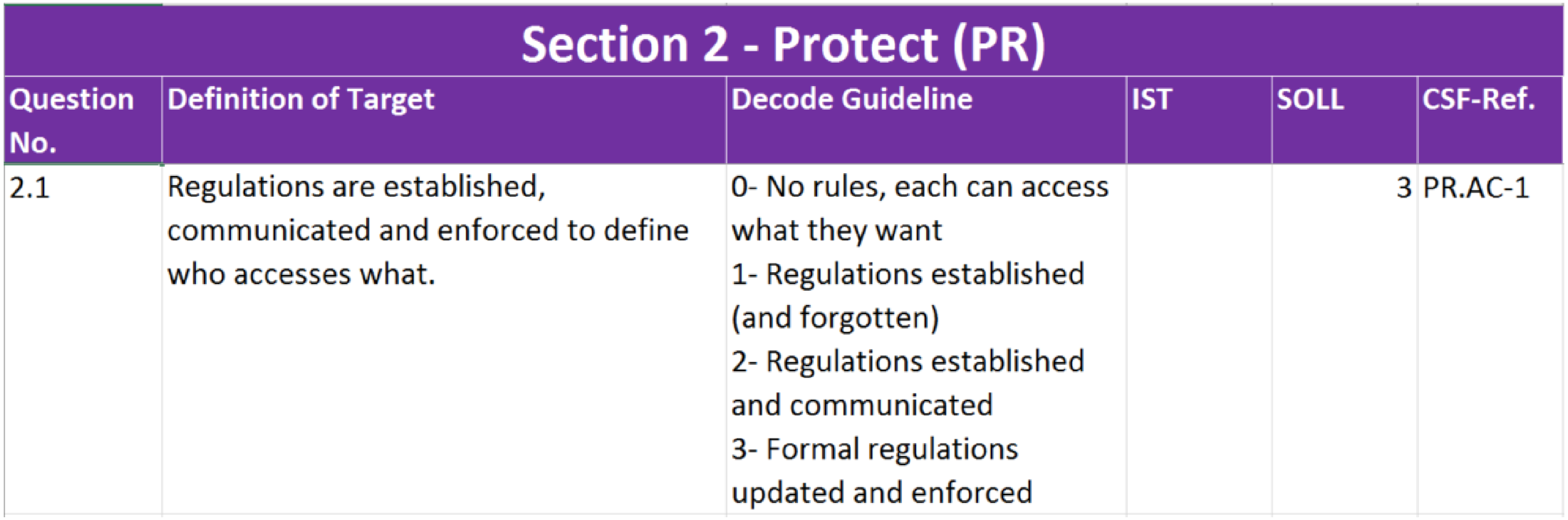
Section 1 - Identify (ID)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.14	Incidents accurately tracked, information used to keep statistics of likelihood of specific incidents, in a formally defined process	0- "Incidents happen." 1- Our technical geek knows all about incidents 2- Track record of incidents, "just for the records" 3- Structured incident log, no processing 4- Structured incident log processed to deduce statistically relevant info - non-systematic 5- Same as above, in a formal process		5	ID.RA-4

Sviluppo di una metodologia semplificata



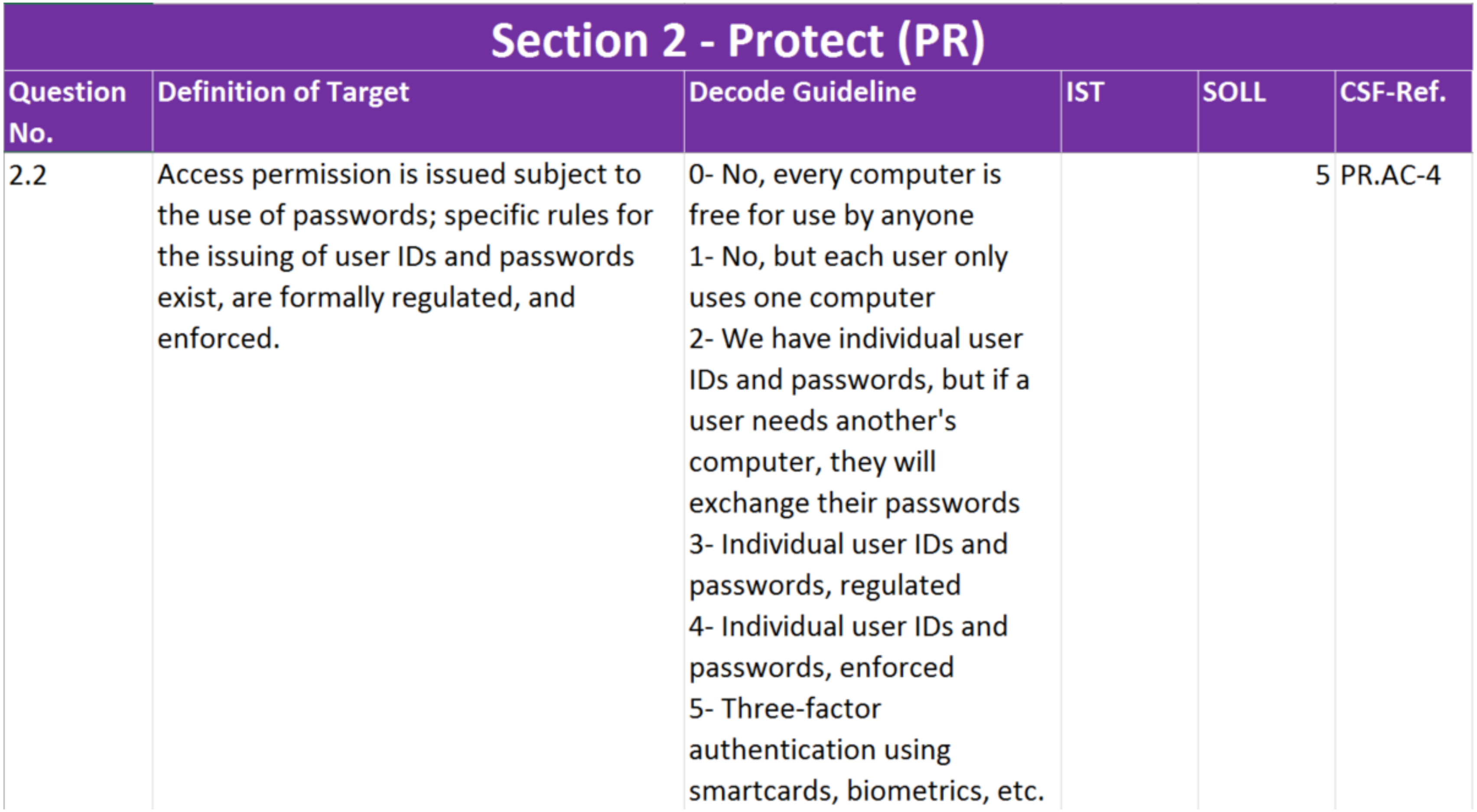
Section 1 - Identify (ID)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
1.15	Incident likelihood is addressed - and reduced - by a specific «lessons learned» process	0- No, we keep making same mistakes over and over again 1- No formal process but internal communication to try to avoid repeating silly things 2- Formal process		2	ID.RM-1

Sviluppo di una metodologia semplificata



Section 2 - Protect (PR)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.1	Regulations are established, communicated and enforced to define who accesses what.	0- No rules, each can access what they want 1- Regulations established (and forgotten) 2- Regulations established and communicated 3- Formal regulations updated and enforced		3	PR.AC-1

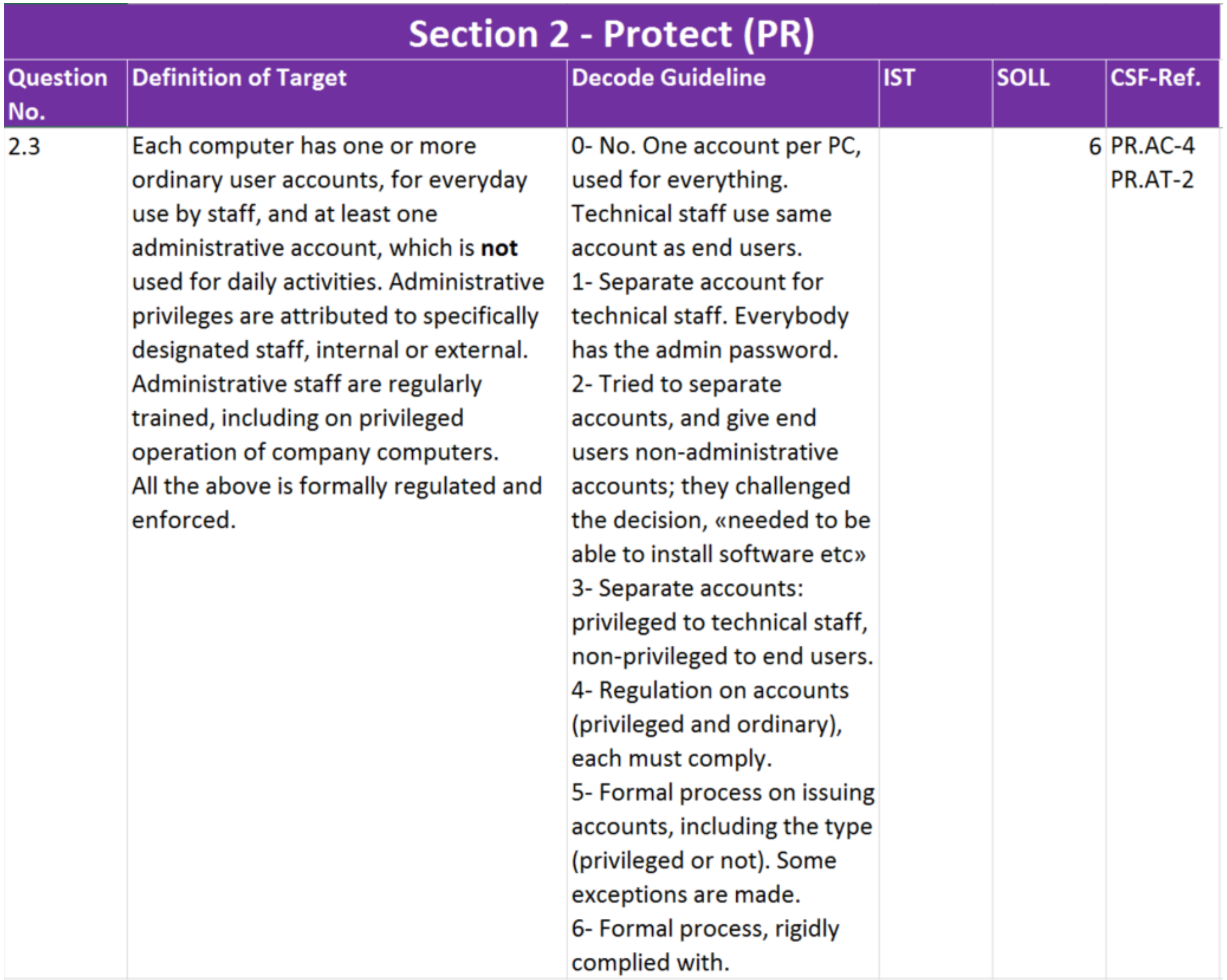
Sviluppo di una metodologia semplificata



Section 2 - Protect (PR)

Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.2	Access permission is issued subject to the use of passwords; specific rules for the issuing of user IDs and passwords exist, are formally regulated, and enforced.	0- No, every computer is free for use by anyone 1- No, but each user only uses one computer 2- We have individual user IDs and passwords, but if a user needs another's computer, they will exchange their passwords 3- Individual user IDs and passwords, regulated 4- Individual user IDs and passwords, enforced 5- Three-factor authentication using smartcards, biometrics, etc.		5	PR.AC-4

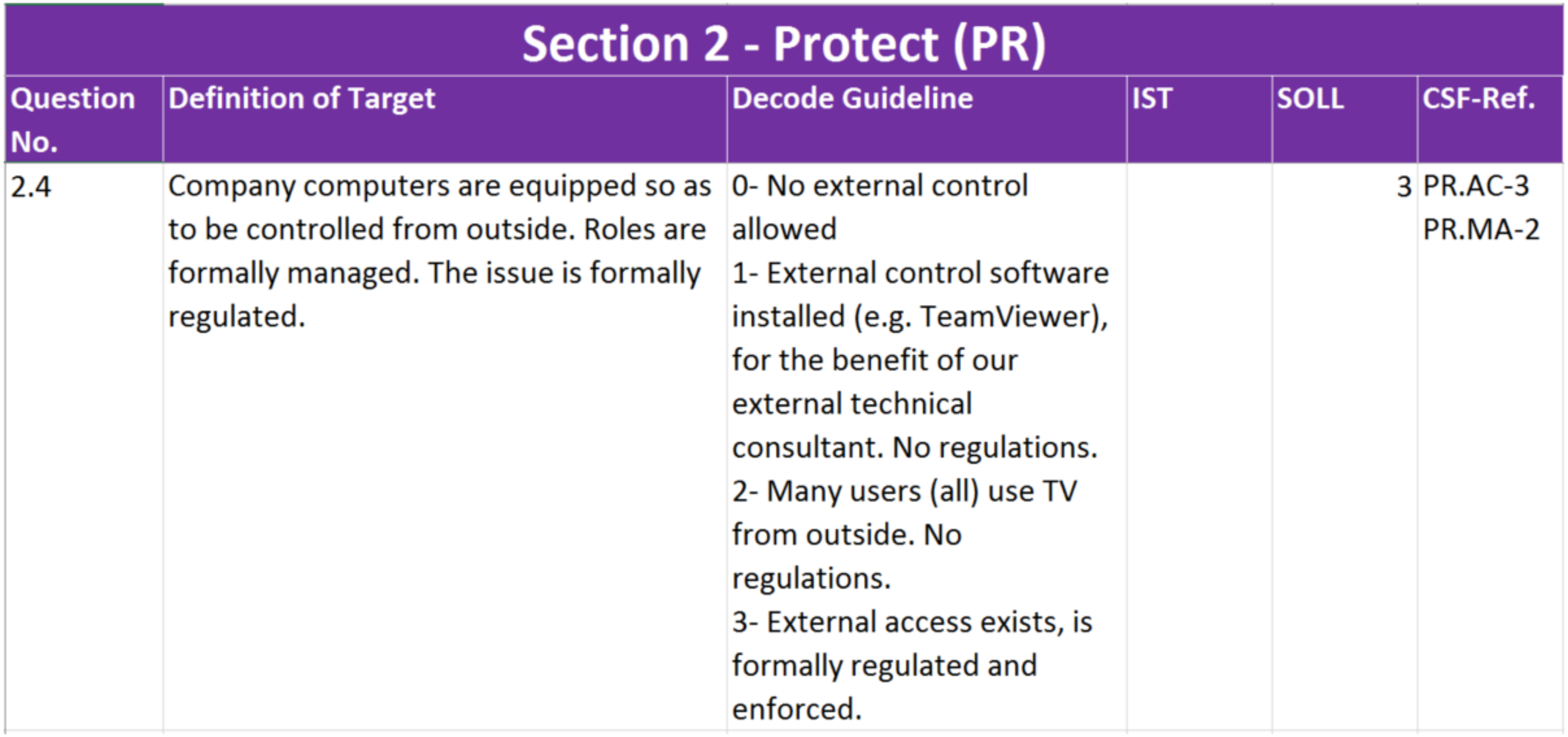
Sviluppo di una metodologia semplificata



Section 2 - Protect (PR)

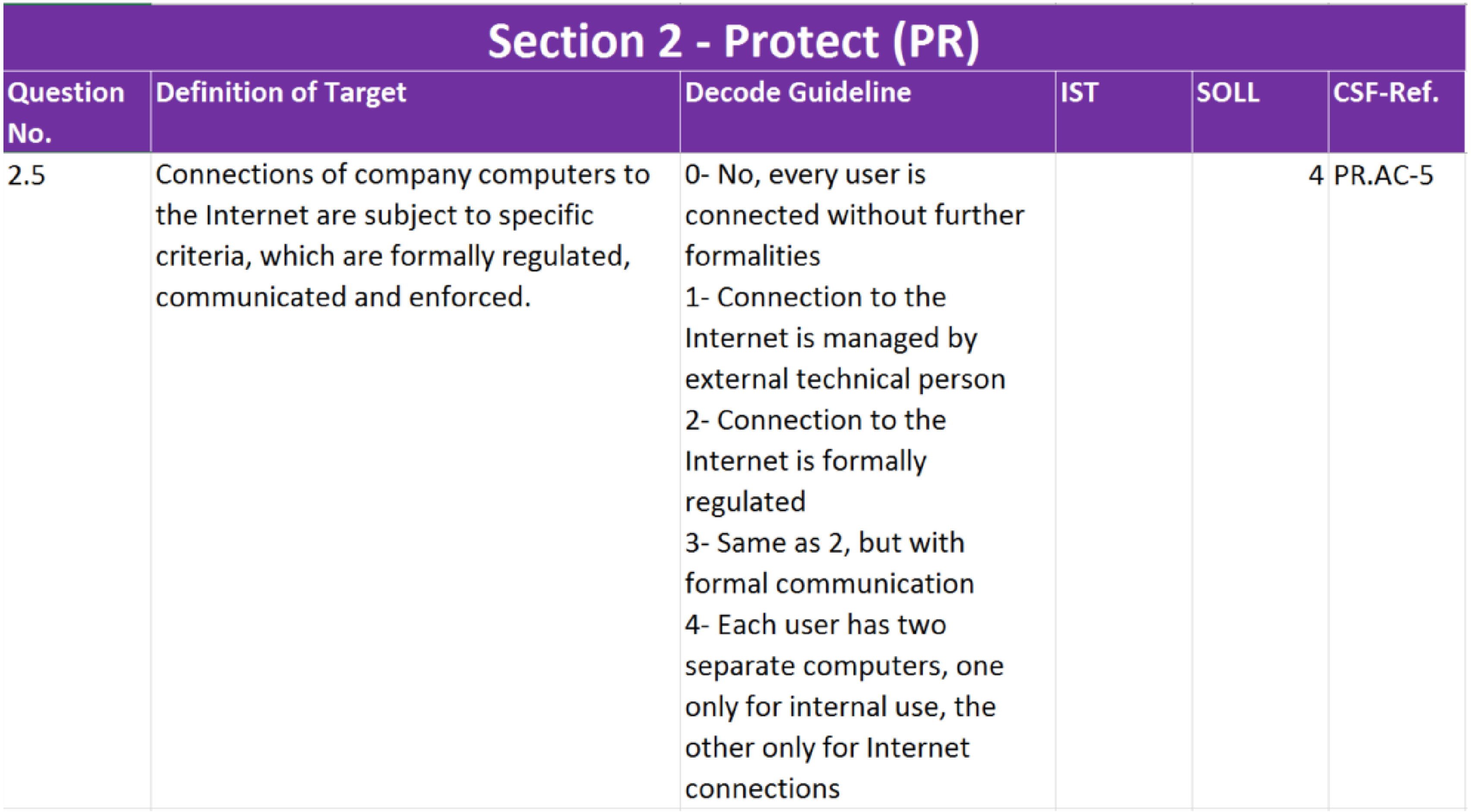
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.3	Each computer has one or more ordinary user accounts, for everyday use by staff, and at least one administrative account, which is **not** used for daily activities. Administrative privileges are attributed to specifically designated staff, internal or external. Administrative staff are regularly trained, including on privileged operation of company computers. All the above is formally regulated and enforced.	0- No. One account per PC, used for everything. Technical staff use same account as end users. 1- Separate account for technical staff. Everybody has the admin password. 2- Tried to separate accounts, and give end users non-administrative accounts; they challenged the decision, «needed to be able to install software etc» 3- Separate accounts: privileged to technical staff, non-privileged to end users. 4- Regulation on accounts (privileged and ordinary), each must comply. 5- Formal process on issuing accounts, including the type (privileged or not). Some exceptions are made. 6- Formal process, rigidly complied with.		6	PR.AC-4 PR.AT-2

Sviluppo di una metodologia semplificata



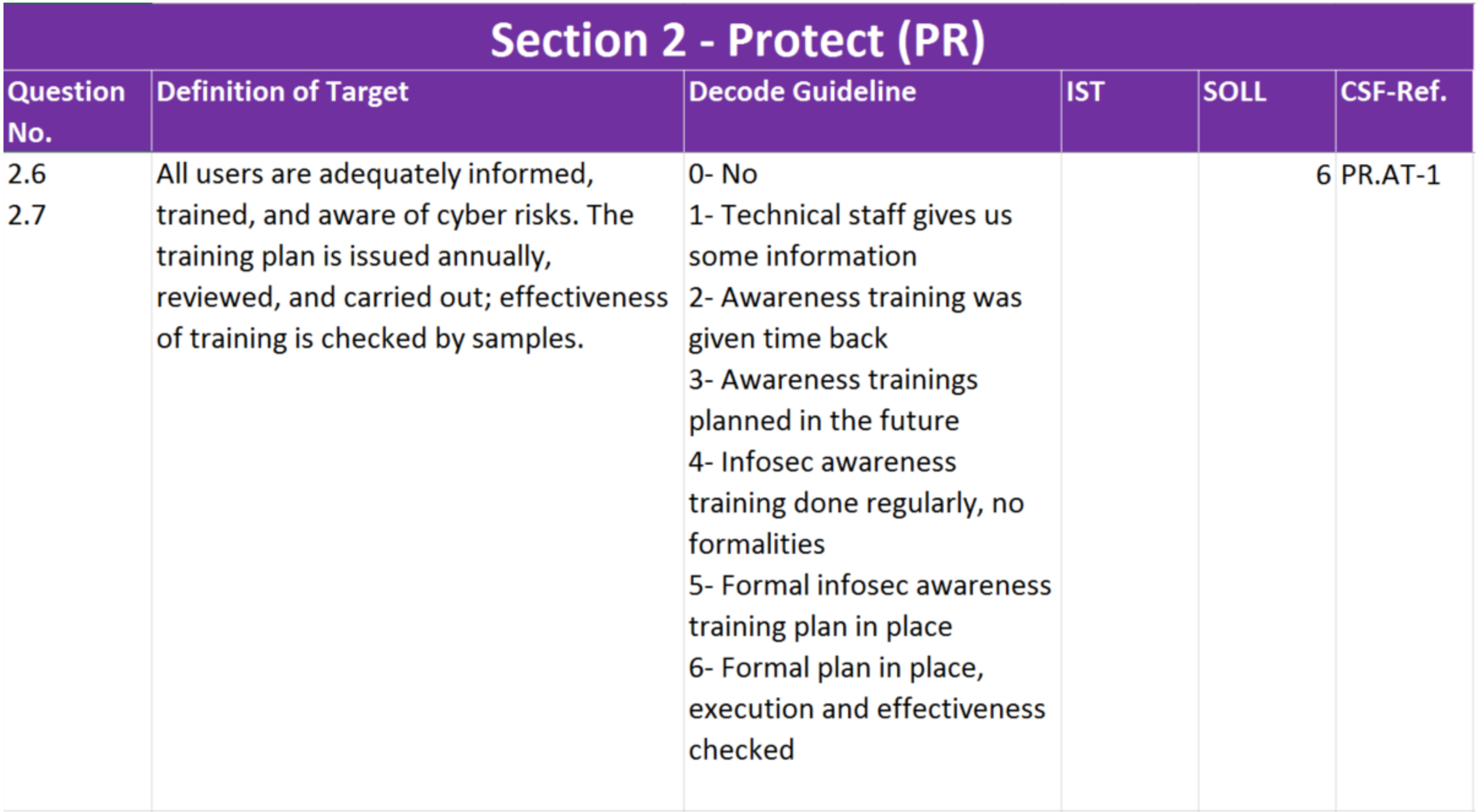
Section 2 - Protect (PR)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.4	Company computers are equipped so as to be controlled from outside. Roles are formally managed. The issue is formally regulated.	0- No external control allowed 1- External control software installed (e.g. TeamViewer), for the benefit of our external technical consultant. No regulations. 2- Many users (all) use TV from outside. No regulations. 3- External access exists, is formally regulated and enforced.		3	PR.AC-3 PR.MA-2

Sviluppo di una metodologia semplificata



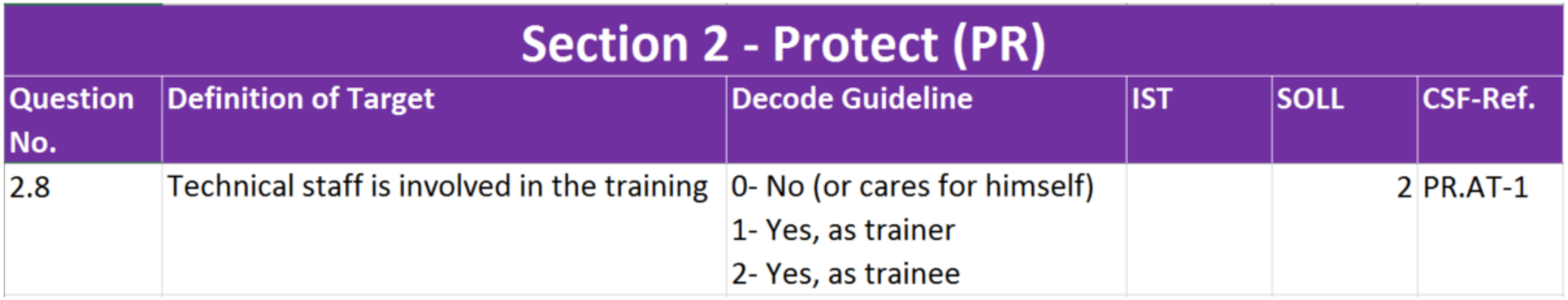
Section 2 - Protect (PR)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.5	Connections of company computers to the Internet are subject to specific criteria, which are formally regulated, communicated and enforced.	0- No, every user is connected without further formalities 1- Connection to the Internet is managed by external technical person 2- Connection to the Internet is formally regulated 3- Same as 2, but with formal communication 4- Each user has two separate computers, one only for internal use, the other only for Internet connections		4	PR.AC-5

Sviluppo di una metodologia semplificata



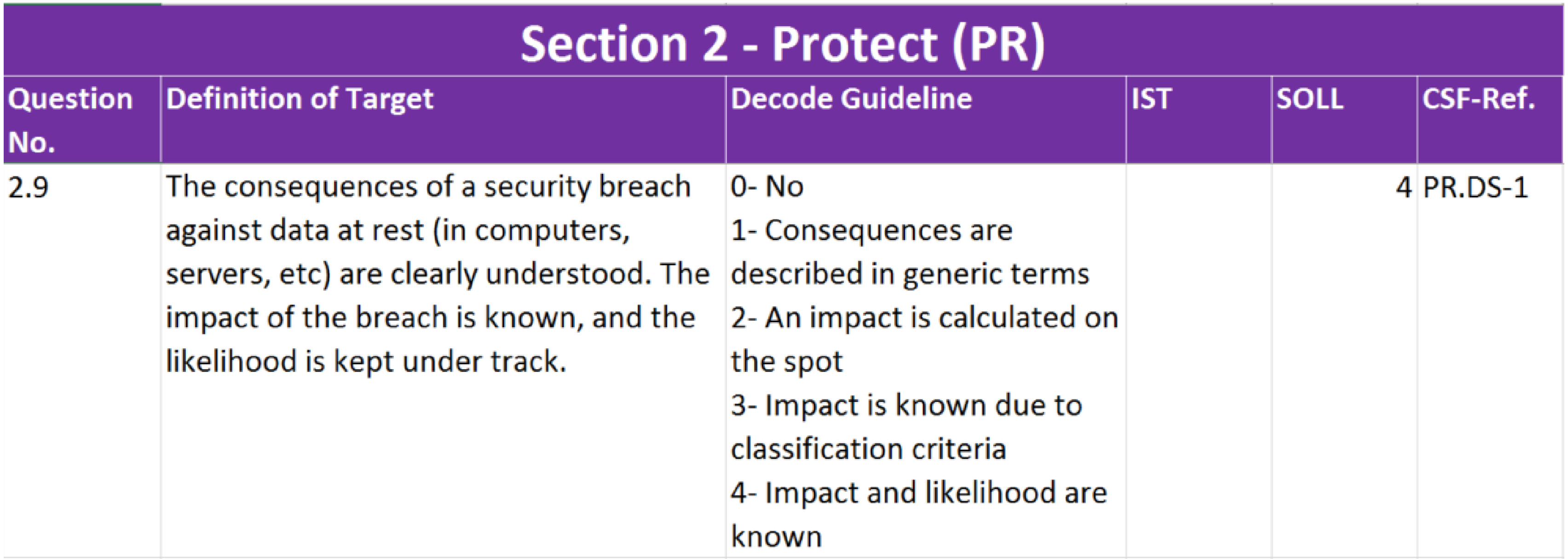
Section 2 - Protect (PR)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.6 2.7	All users are adequately informed, trained, and aware of cyber risks. The training plan is issued annually, reviewed, and carried out; effectiveness of training is checked by samples.	0- No 1- Technical staff gives us some information 2- Awareness training was given time back 3- Awareness trainings planned in the future 4- Infosec awareness training done regularly, no formalities 5- Formal infosec awareness training plan in place 6- Formal plan in place, execution and effectiveness checked		6	PR.AT-1

Sviluppo di una metodologia semplificata



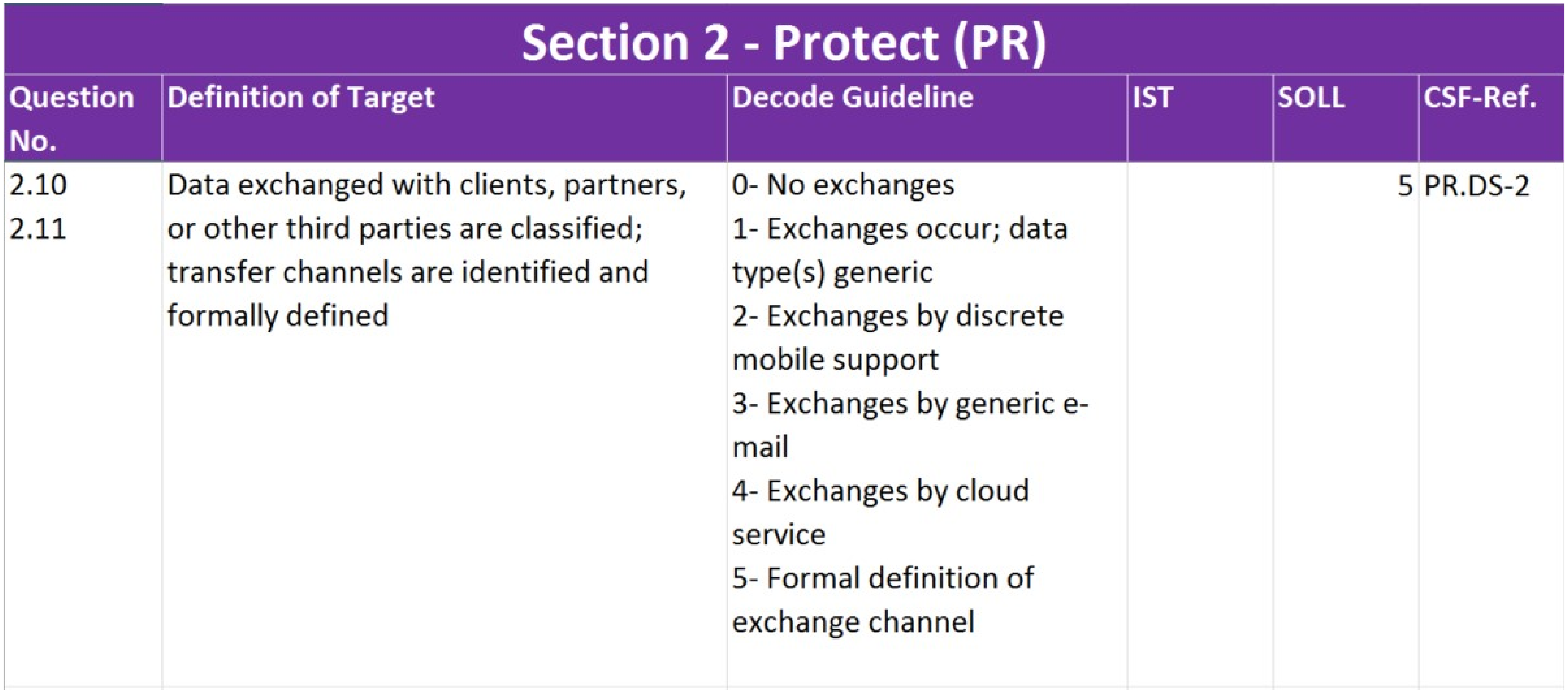
Section 2 - Protect (PR)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.8	Technical staff is involved in the training	0- No (or cares for himself) 1- Yes, as trainer 2- Yes, as trainee		2	PR.AT-1

Sviluppo di una metodologia semplificata



Section 2 - Protect (PR)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.9	The consequences of a security breach against data at rest (in computers, servers, etc) are clearly understood. The impact of the breach is known, and the likelihood is kept under track.	0- No 1- Consequences are described in generic terms 2- An impact is calculated on the spot 3- Impact is known due to classification criteria 4- Impact and likelihood are known		4	PR.DS-1

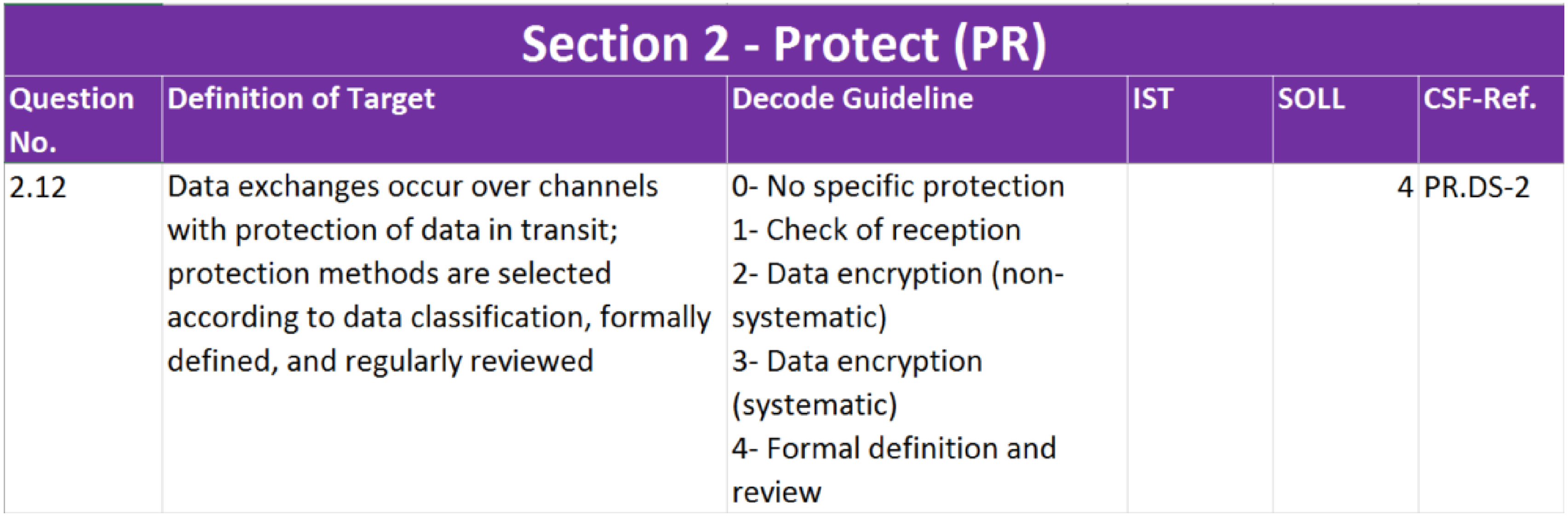
Sviluppo di una metodologia semplificata



Section 2 - Protect (PR)

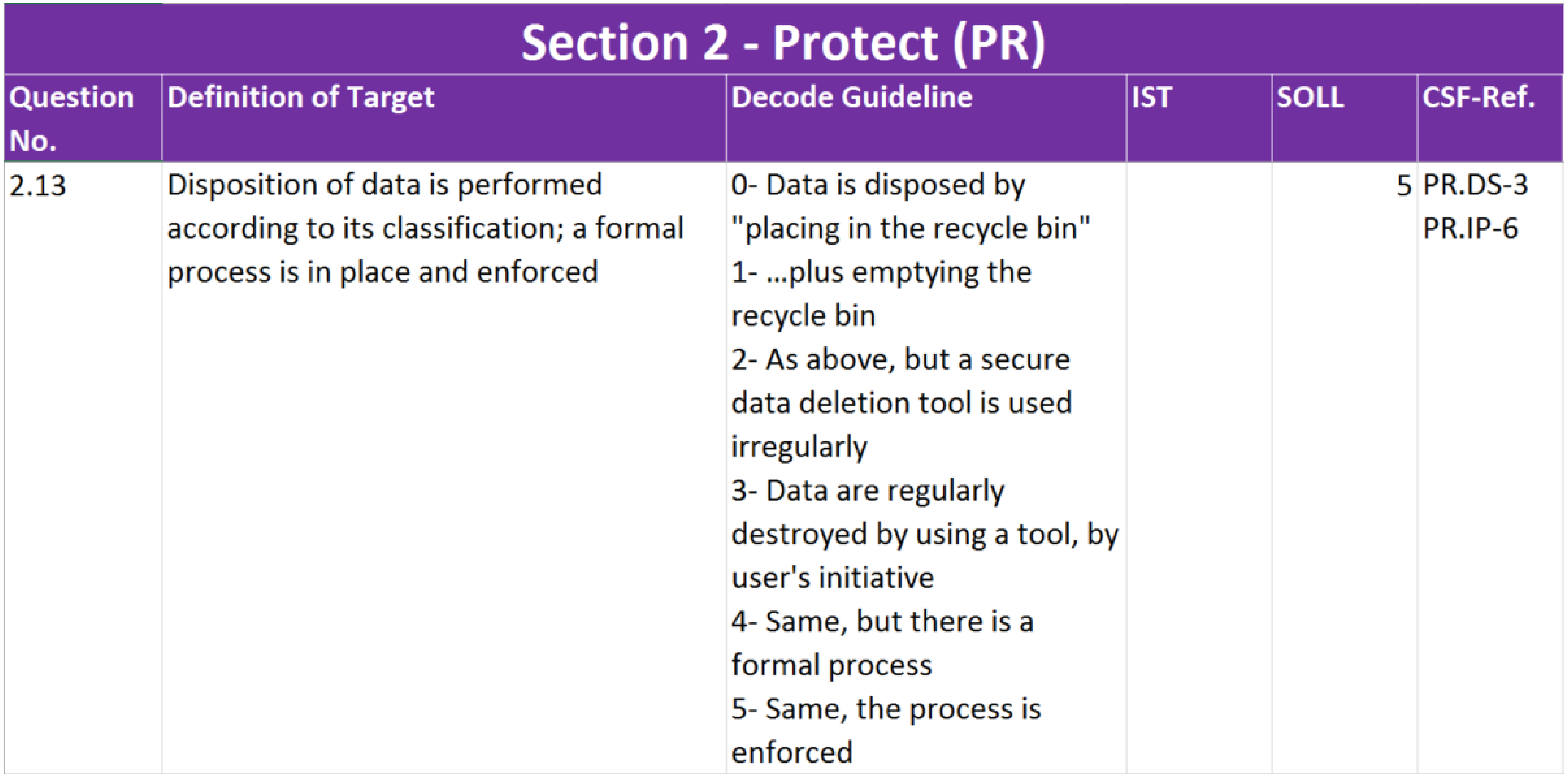
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.10 2.11	Data exchanged with clients, partners, or other third parties are classified; transfer channels are identified and formally defined	0- No exchanges 1- Exchanges occur; data type(s) generic 2- Exchanges by discrete mobile support 3- Exchanges by generic e-mail 4- Exchanges by cloud service 5- Formal definition of exchange channel		5	PR.DS-2

Sviluppo di una metodologia semplificata



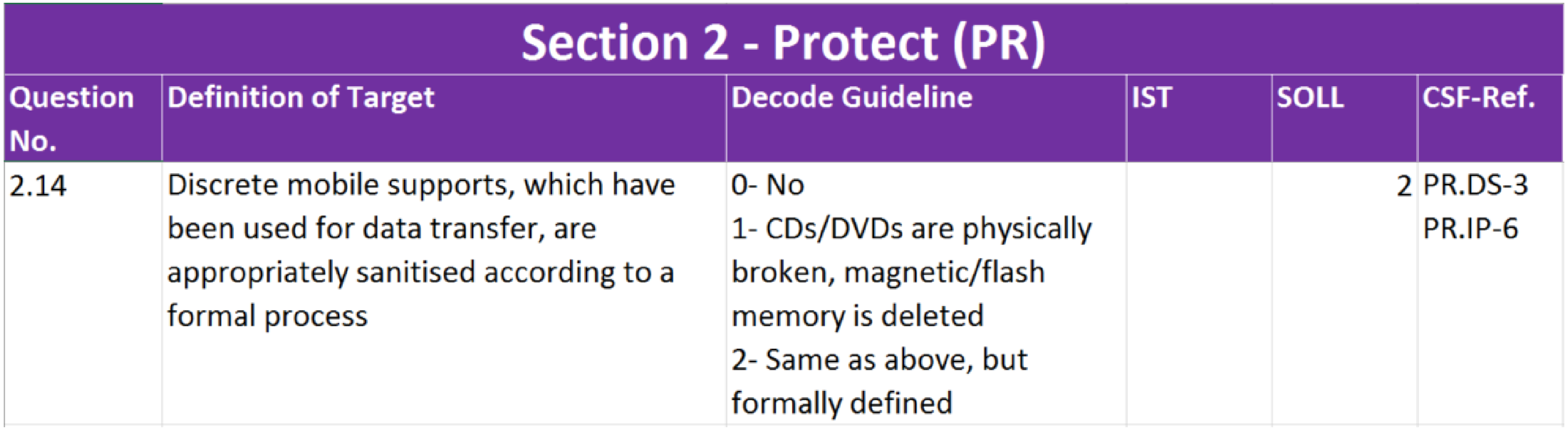
Section 2 - Protect (PR)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.12	Data exchanges occur over channels with protection of data in transit; protection methods are selected according to data classification, formally defined, and regularly reviewed	0- No specific protection 1- Check of reception 2- Data encryption (non-systematic) 3- Data encryption (systematic) 4- Formal definition and review		4	PR.DS-2

Sviluppo di una metodologia semplificata



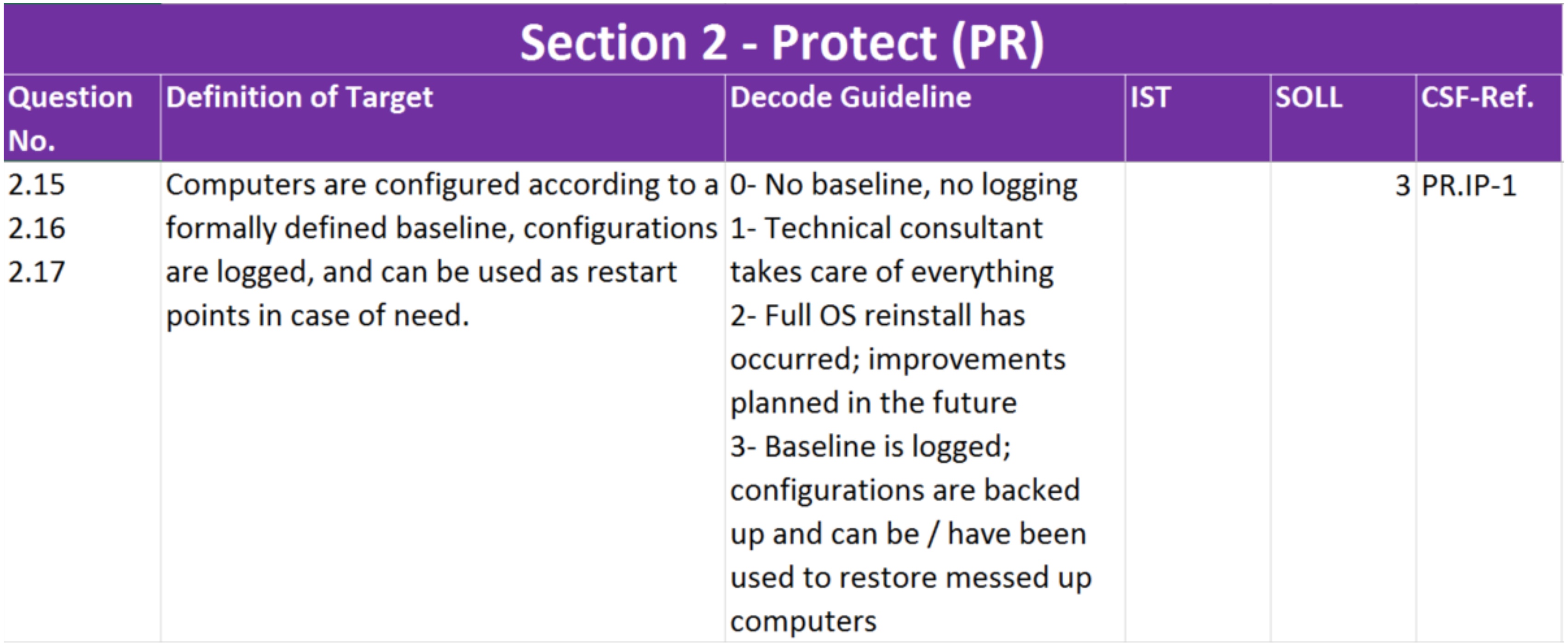
Section 2 - Protect (PR)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.13	Disposition of data is performed according to its classification; a formal process is in place and enforced	0- Data is disposed by "placing in the recycle bin" 1- ...plus emptying the recycle bin 2- As above, but a secure data deletion tool is used irregularly 3- Data are regularly destroyed by using a tool, by user's initiative 4- Same, but there is a formal process 5- Same, the process is enforced		5	PR.DS-3 PR.IP-6

Sviluppo di una metodologia semplificata



Section 2 - Protect (PR)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.14	Discrete mobile supports, which have been used for data transfer, are appropriately sanitised according to a formal process	0- No 1- CDs/DVDs are physically broken, magnetic/flash memory is deleted 2- Same as above, but formally defined		2	PR.DS-3 PR.IP-6

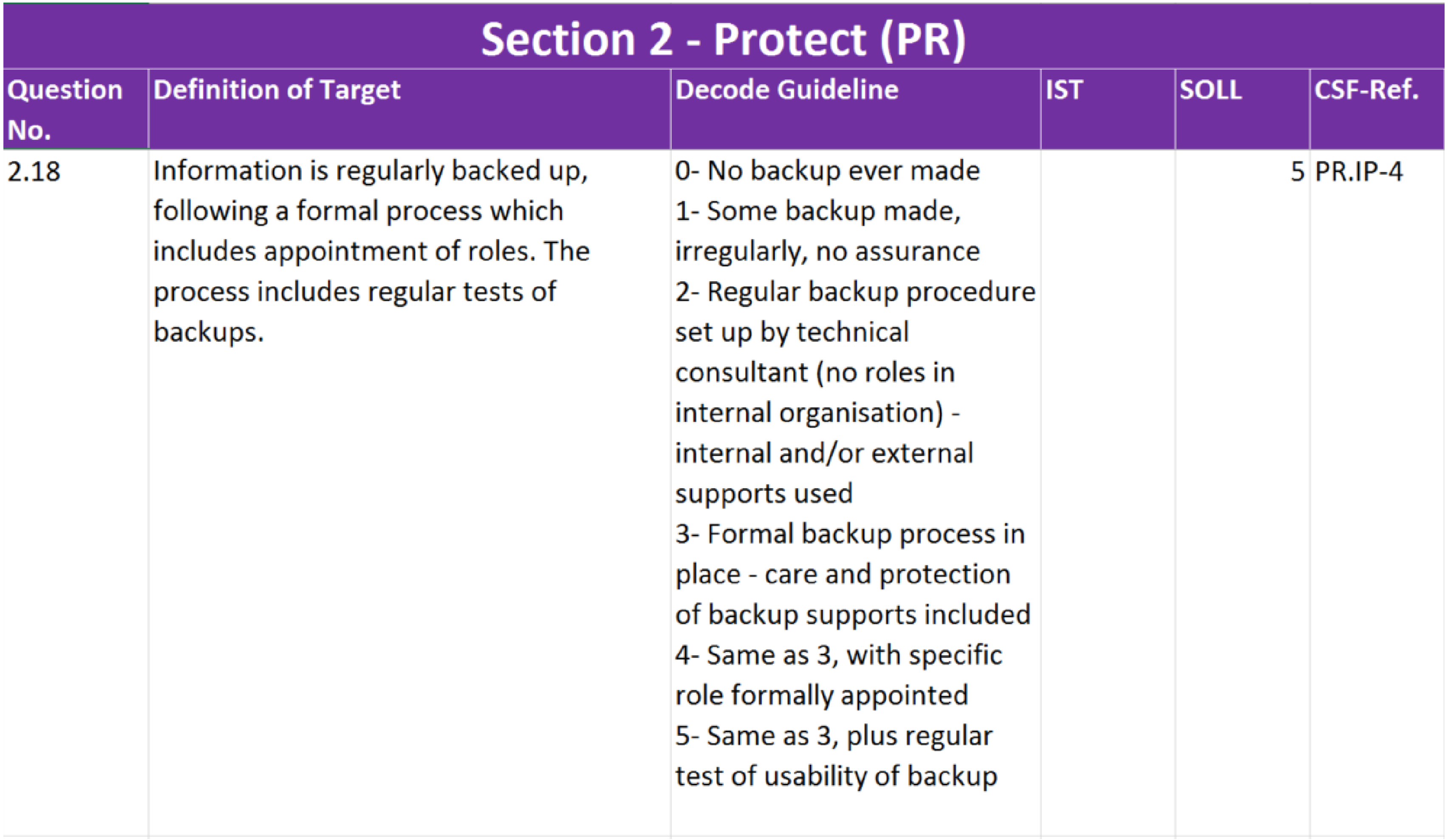
Sviluppo di una metodologia semplificata



Section 2 - Protect (PR)

Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.15 2.16 2.17	Computers are configured according to a formally defined baseline, configurations are logged, and can be used as restart points in case of need.	0- No baseline, no logging 1- Technical consultant takes care of everything 2- Full OS reinstall has occurred; improvements planned in the future 3- Baseline is logged; configurations are backed up and can be / have been used to restore messed up computers		3	PR.IP-1

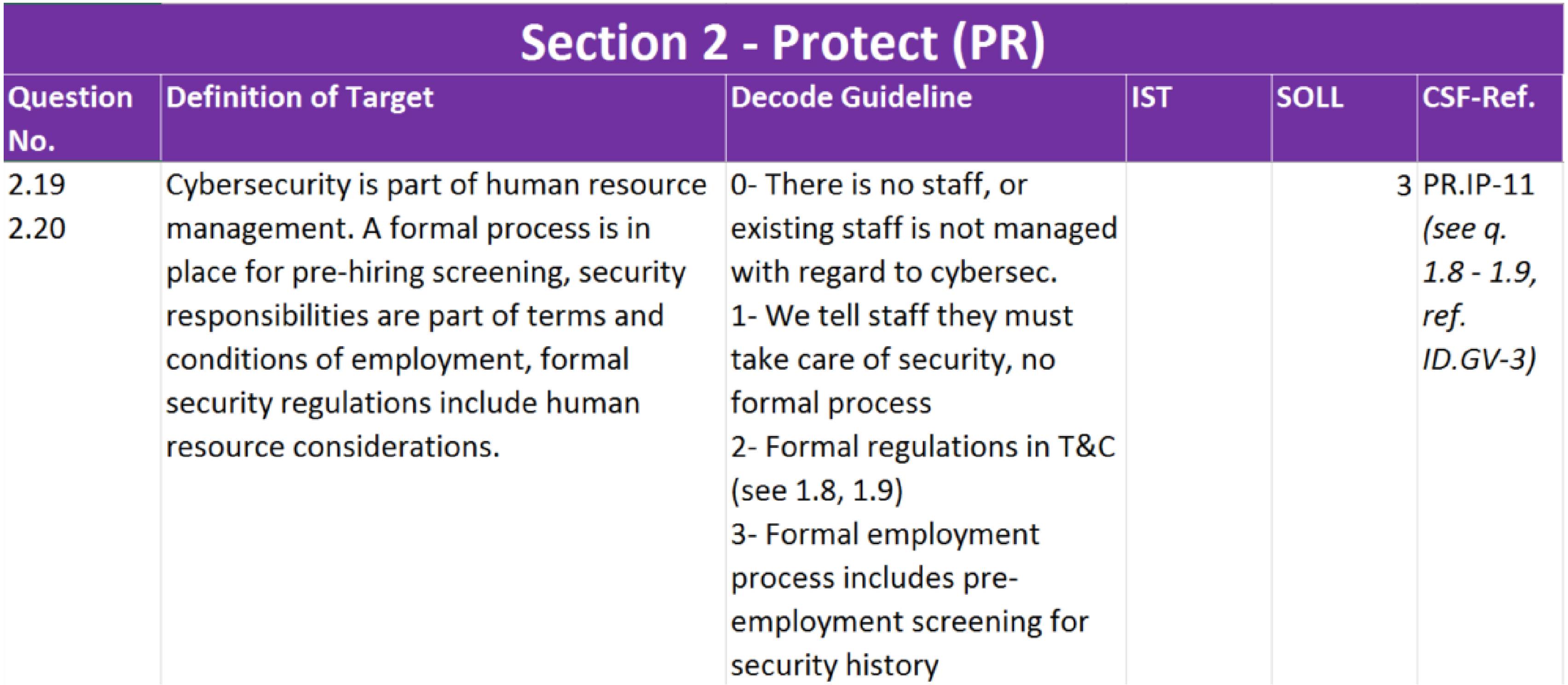
Sviluppo di una metodologia semplificata



Section 2 - Protect (PR)

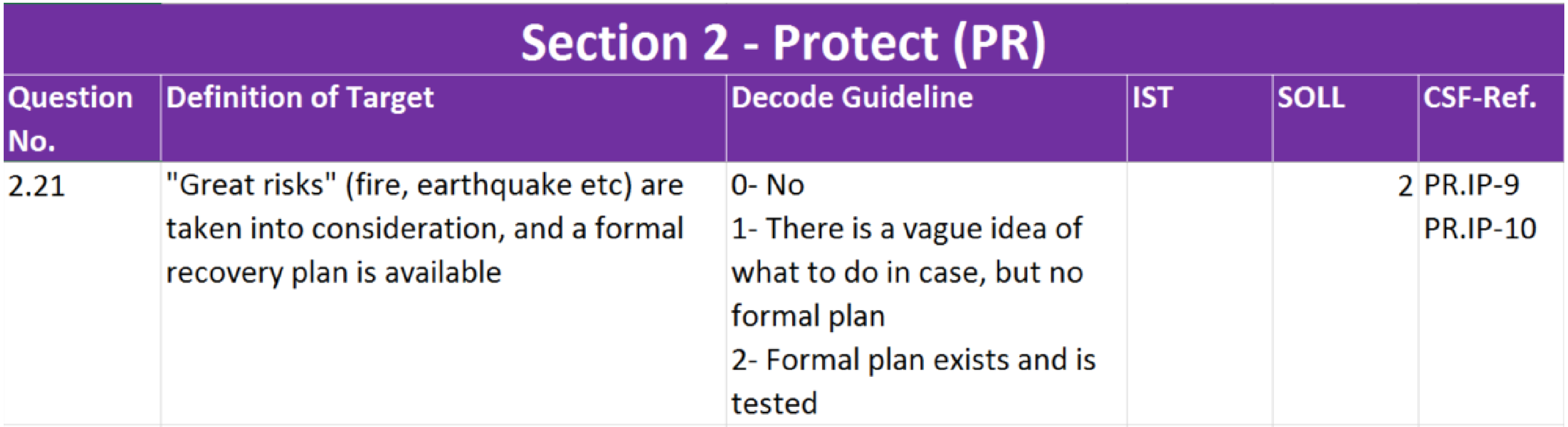
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.18	Information is regularly backed up, following a formal process which includes appointment of roles. The process includes regular tests of backups.	0- No backup ever made 1- Some backup made, irregularly, no assurance 2- Regular backup procedure set up by technical consultant (no roles in internal organisation) - internal and/or external supports used 3- Formal backup process in place - care and protection of backup supports included 4- Same as 3, with specific role formally appointed 5- Same as 3, plus regular test of usability of backup		5	PR.IP-4

Sviluppo di una metodologia semplificata



Section 2 - Protect (PR)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.19 2.20	Cybersecurity is part of human resource management. A formal process is in place for pre-hiring screening, security responsibilities are part of terms and conditions of employment, formal security regulations include human resource considerations.	0- There is no staff, or existing staff is not managed with regard to cybersec. 1- We tell staff they must take care of security, no formal process 2- Formal regulations in T&C (see 1.8, 1.9) 3- Formal employment process includes pre-employment screening for security history		3	PR.IP-11 *(see q. 1.8 - 1.9, ref. ID.GV-3)*

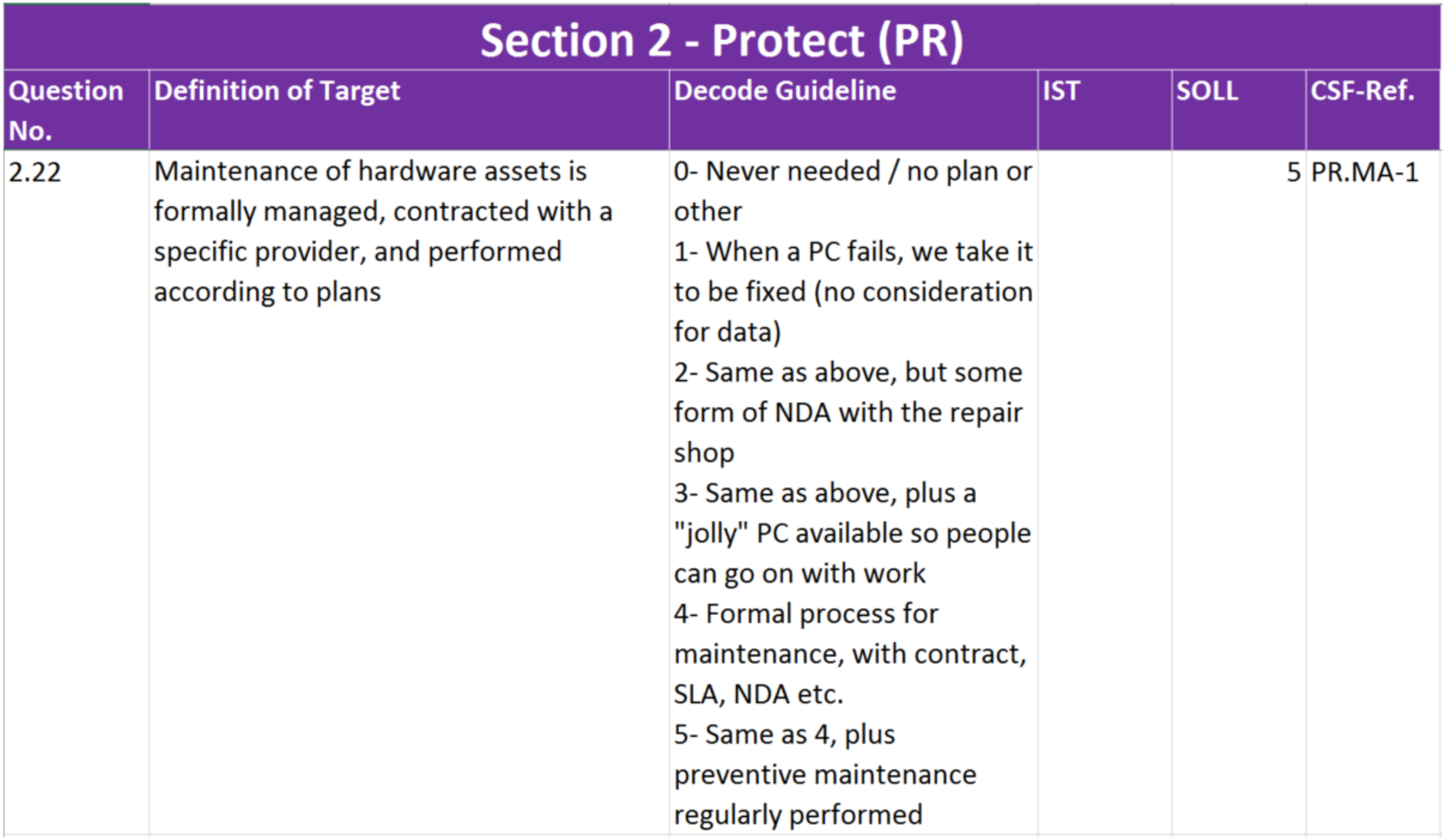
Sviluppo di una metodologia semplificata



Section 2 - Protect (PR)

Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.21	"Great risks" (fire, earthquake etc) are taken into consideration, and a formal recovery plan is available	0- No 1- There is a vague idea of what to do in case, but no formal plan 2- Formal plan exists and is tested		2	PR.IP-9 PR.IP-10

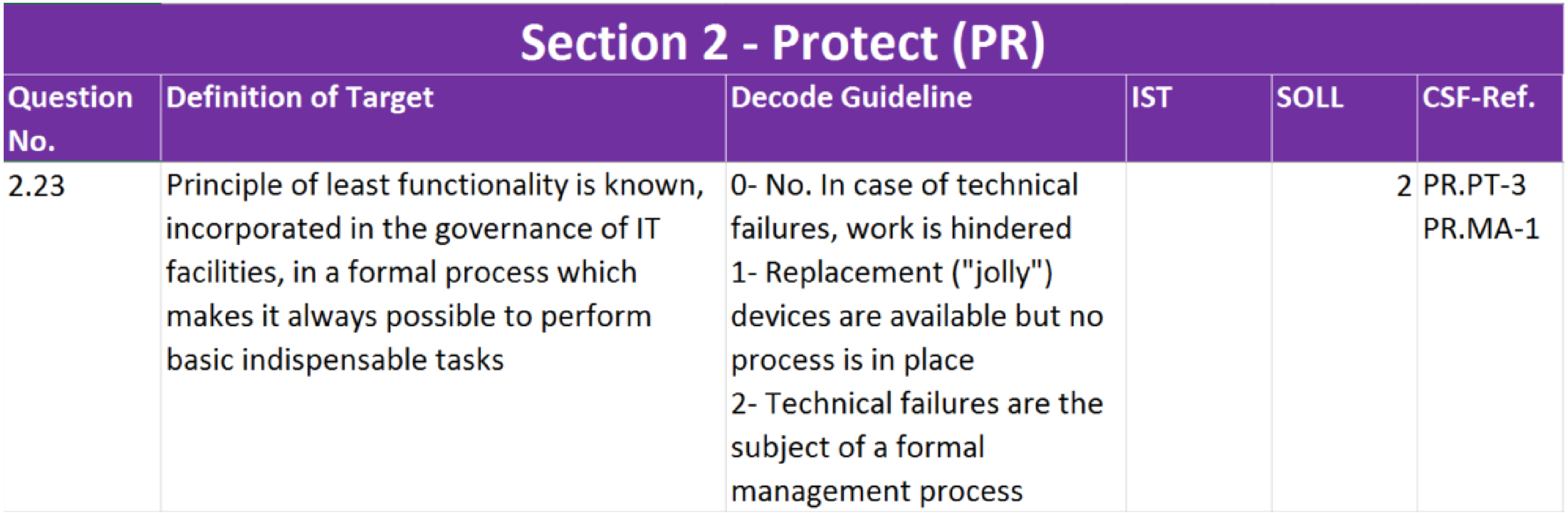
Sviluppo di una metodologia semplificata



Section 2 - Protect (PR)

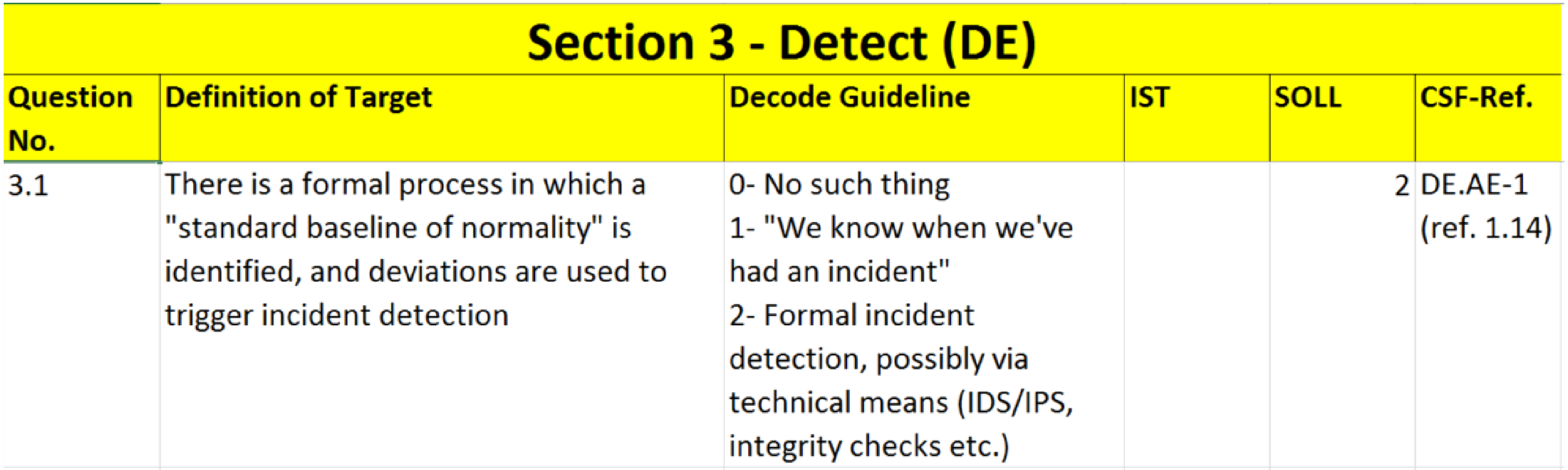
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.22	Maintenance of hardware assets is formally managed, contracted with a specific provider, and performed according to plans	0- Never needed / no plan or other 1- When a PC fails, we take it to be fixed (no consideration for data) 2- Same as above, but some form of NDA with the repair shop 3- Same as above, plus a "jolly" PC available so people can go on with work 4- Formal process for maintenance, with contract, SLA, NDA etc. 5- Same as 4, plus preventive maintenance regularly performed		5	PR.MA-1

Sviluppo di una metodologia semplificata



Section 2 - Protect (PR)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
2.23	Principle of least functionality is known, incorporated in the governance of IT facilities, in a formal process which makes it always possible to perform basic indispensable tasks	0- No. In case of technical failures, work is hindered 1- Replacement ("jolly") devices are available but no process is in place 2- Technical failures are the subject of a formal management process		2	PR.PT-3 PR.MA-1

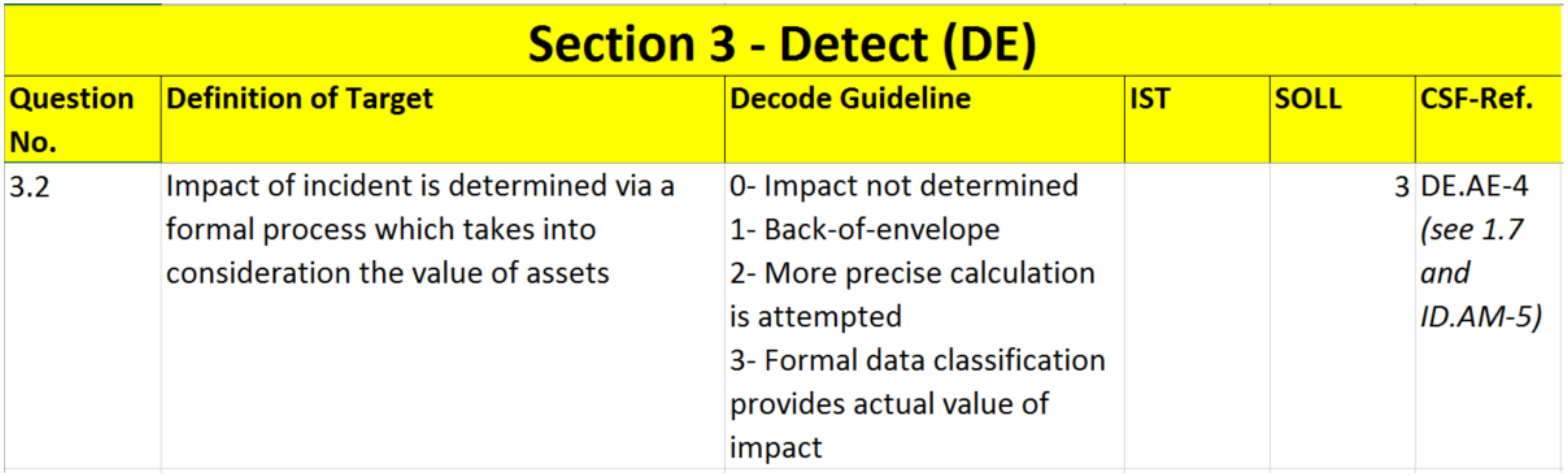
Sviluppo di una metodologia semplificata



Section 3 - Detect (DE)

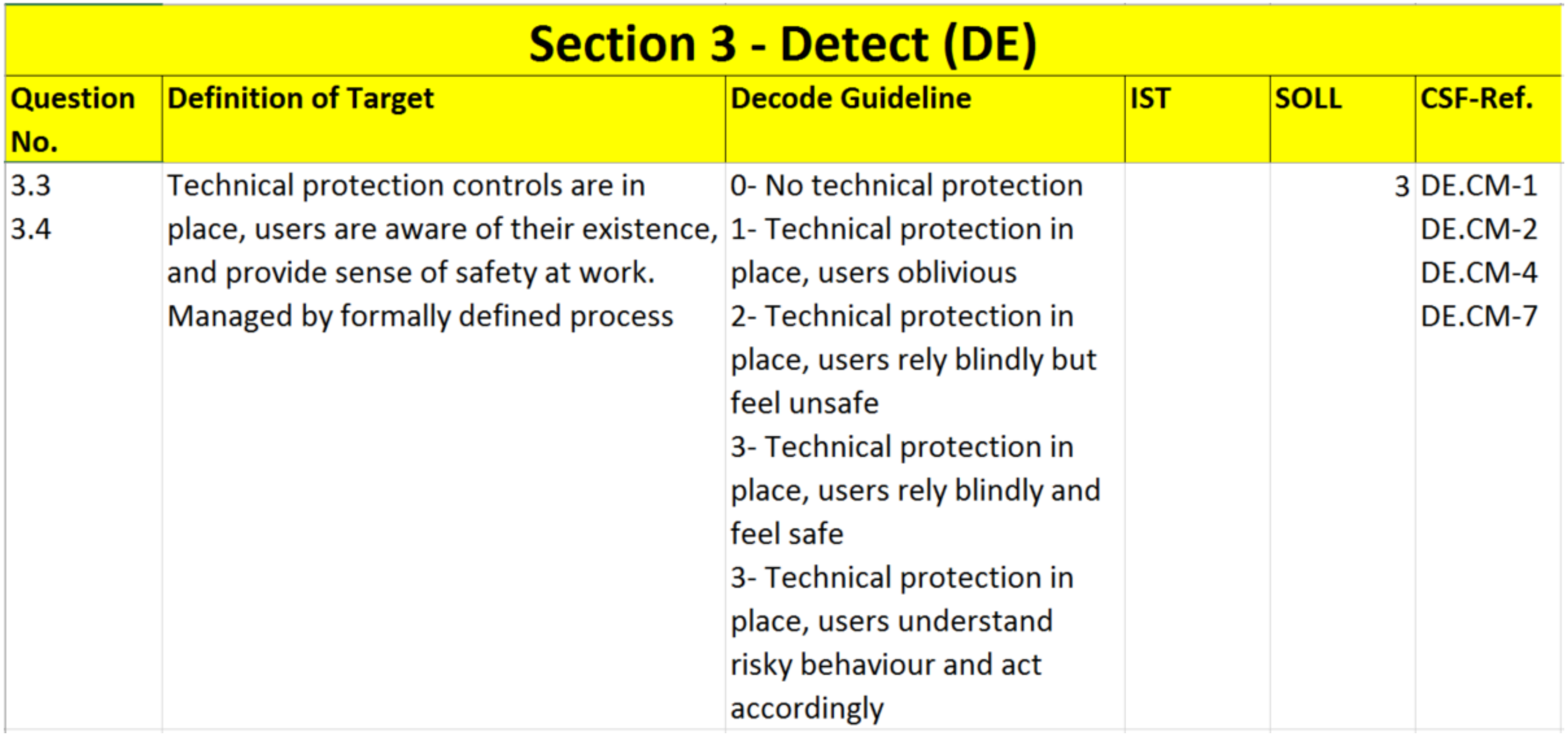
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
3.1	There is a formal process in which a "standard baseline of normality" is identified, and deviations are used to trigger incident detection	0- No such thing 1- "We know when we've had an incident" 2- Formal incident detection, possibly via technical means (IDS/IPS, integrity checks etc.)		2	DE.AE-1 (ref. 1.14)

Sviluppo di una metodologia semplificata



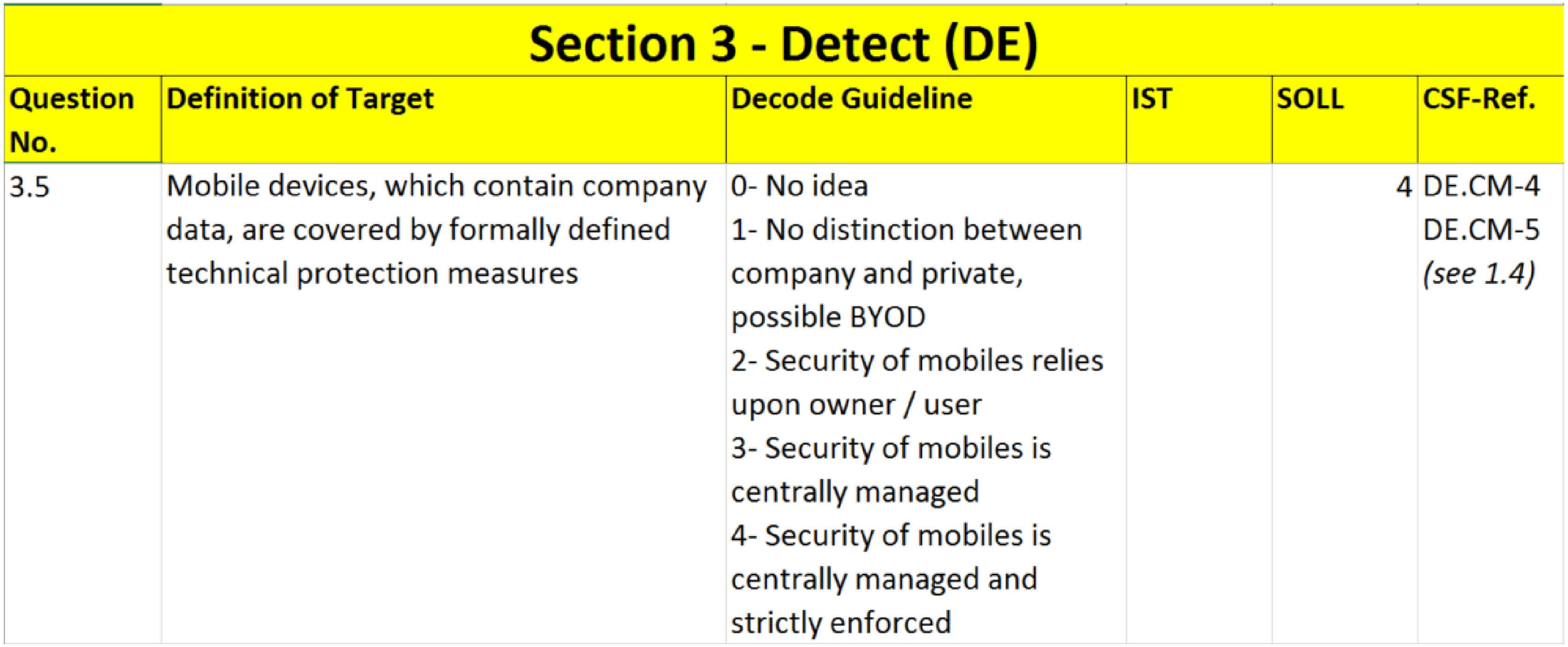
Section 3 - Detect (DE)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
3.2	Impact of incident is determined via a formal process which takes into consideration the value of assets	0- Impact not determined 1- Back-of-envelope 2- More precise calculation is attempted 3- Formal data classification provides actual value of impact		3	DE.AE-4 *(see 1.7 and ID.AM-5)*

Sviluppo di una metodologia semplificata



Section 3 - Detect (DE)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
3.3 3.4	Technical protection controls are in place, users are aware of their existence, and provide sense of safety at work. Managed by formally defined process	0- No technical protection 1- Technical protection in place, users oblivious 2- Technical protection in place, users rely blindly but feel unsafe 3- Technical protection in place, users rely blindly and feel safe 3- Technical protection in place, users understand risky behaviour and act accordingly		3	DE.CM-1 DE.CM-2 DE.CM-4 DE.CM-7

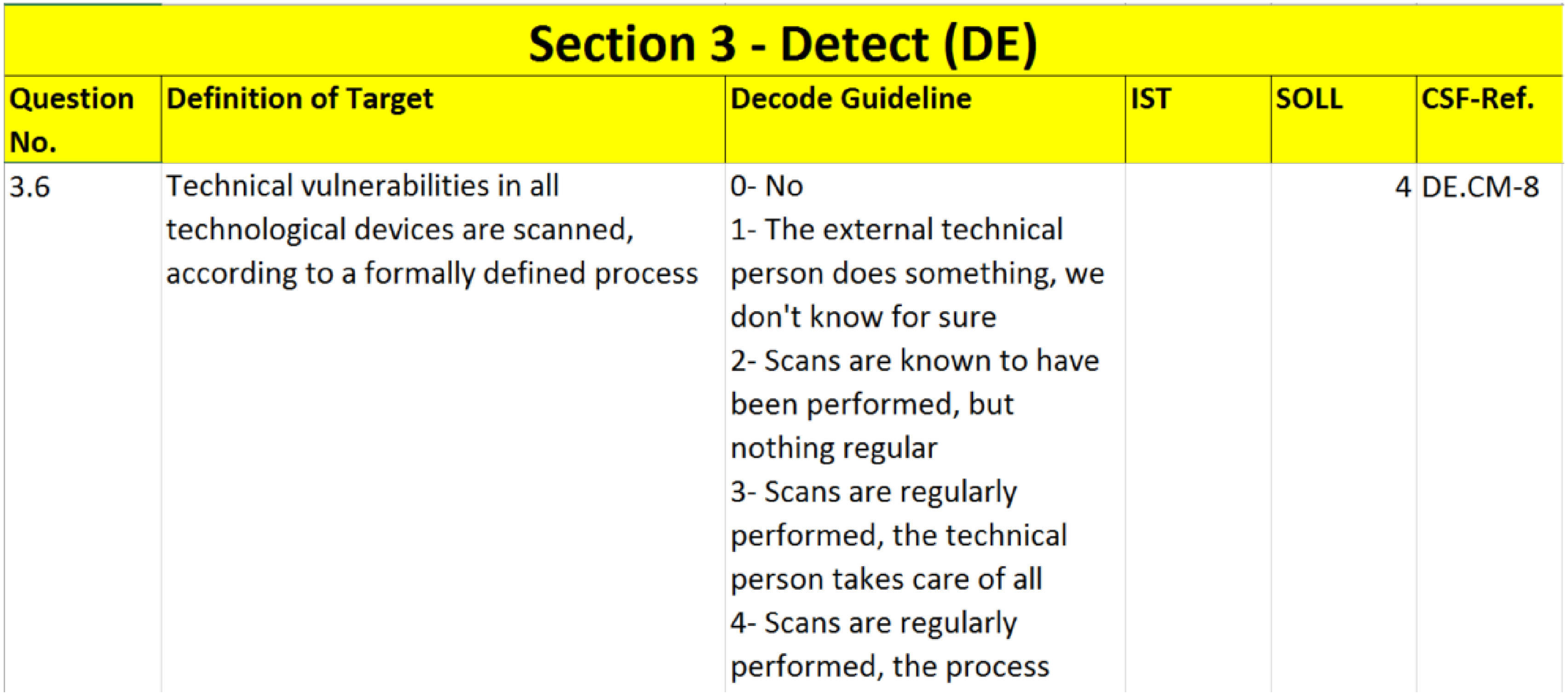
Sviluppo di una metodologia semplificata



Section 3 - Detect (DE)

Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
3.5	Mobile devices, which contain company data, are covered by formally defined technical protection measures	0- No idea 1- No distinction between company and private, possible BYOD 2- Security of mobiles relies upon owner / user 3- Security of mobiles is centrally managed 4- Security of mobiles is centrally managed and strictly enforced		4	DE.CM-4 DE.CM-5 *(see 1.4)*

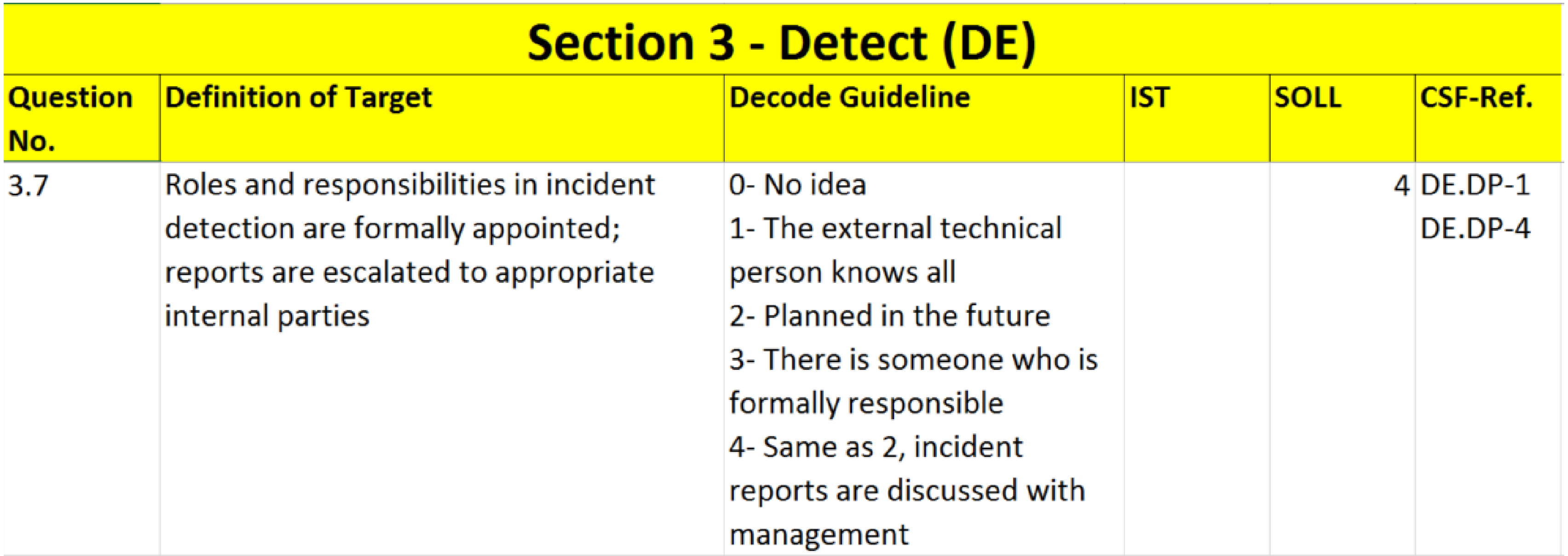
Sviluppo di una metodologia semplificata



Section 3 - Detect (DE)

Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
3.6	Technical vulnerabilities in all technological devices are scanned, according to a formally defined process	0- No 1- The external technical person does something, we don't know for sure 2- Scans are known to have been performed, but nothing regular 3- Scans are regularly performed, the technical person takes care of all 4- Scans are regularly performed, the process		4	DE.CM-8

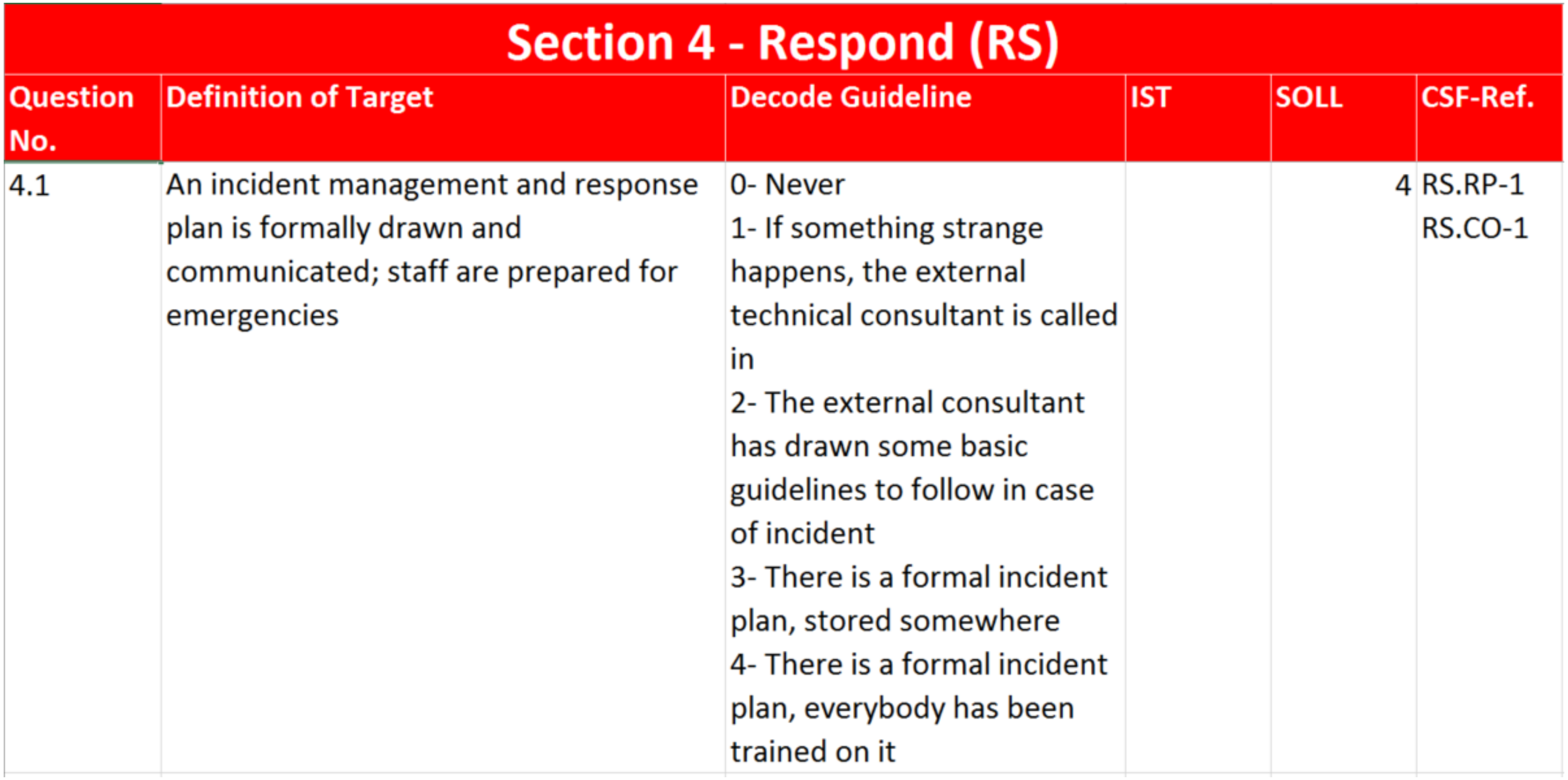
Sviluppo di una metodologia semplificata



Section 3 - Detect (DE)

Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
3.7	Roles and responsibilities in incident detection are formally appointed; reports are escalated to appropriate internal parties	0- No idea 1- The external technical person knows all 2- Planned in the future 3- There is someone who is formally responsible 4- Same as 2, incident reports are discussed with management		4	DE.DP-1 DE.DP-4

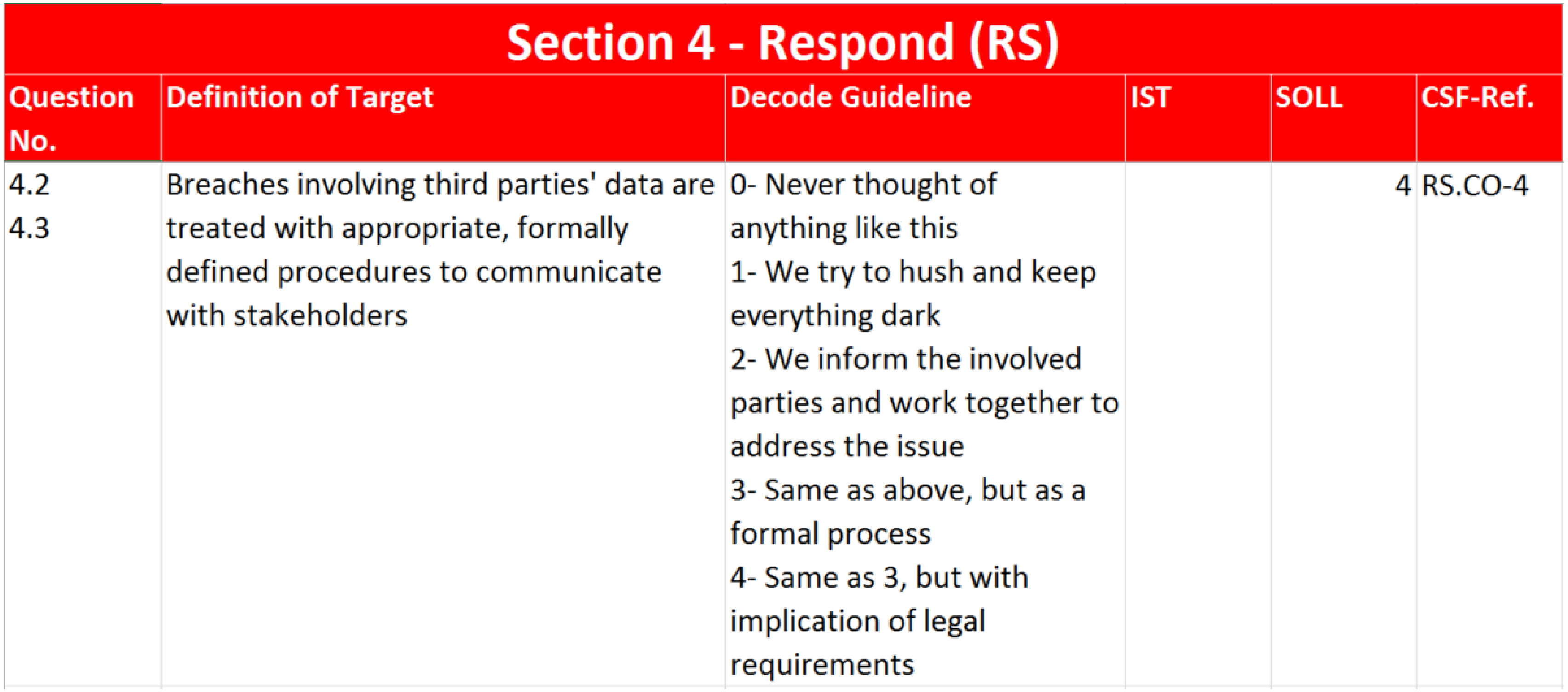
Sviluppo di una metodologia semplificata



Section 4 - Respond (RS)

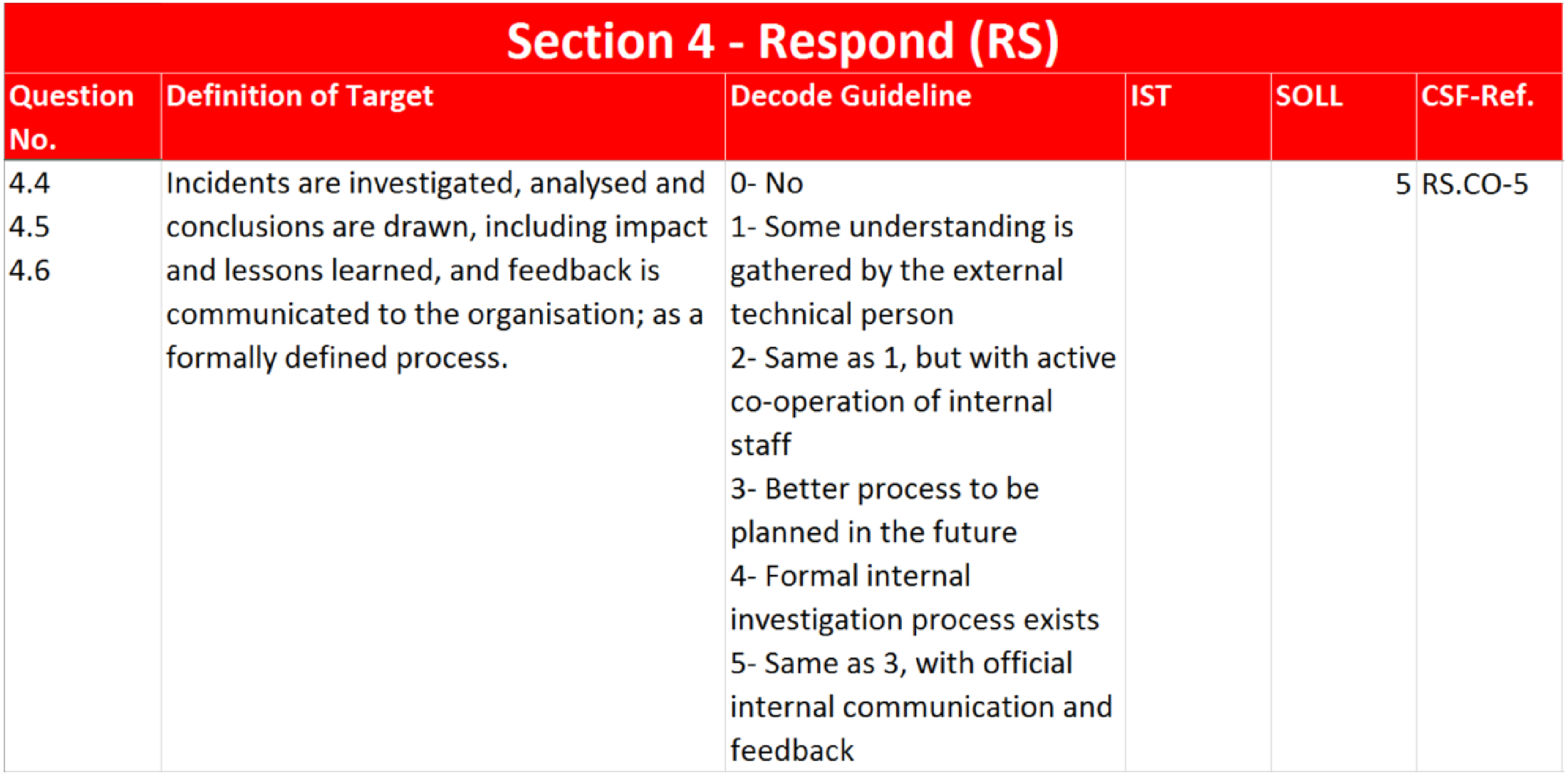
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
4.1	An incident management and response plan is formally drawn and communicated; staff are prepared for emergencies	0- Never 1- If something strange happens, the external technical consultant is called in 2- The external consultant has drawn some basic guidelines to follow in case of incident 3- There is a formal incident plan, stored somewhere 4- There is a formal incident plan, everybody has been trained on it		4	RS.RP-1 RS.CO-1

Sviluppo di una metodologia semplificata



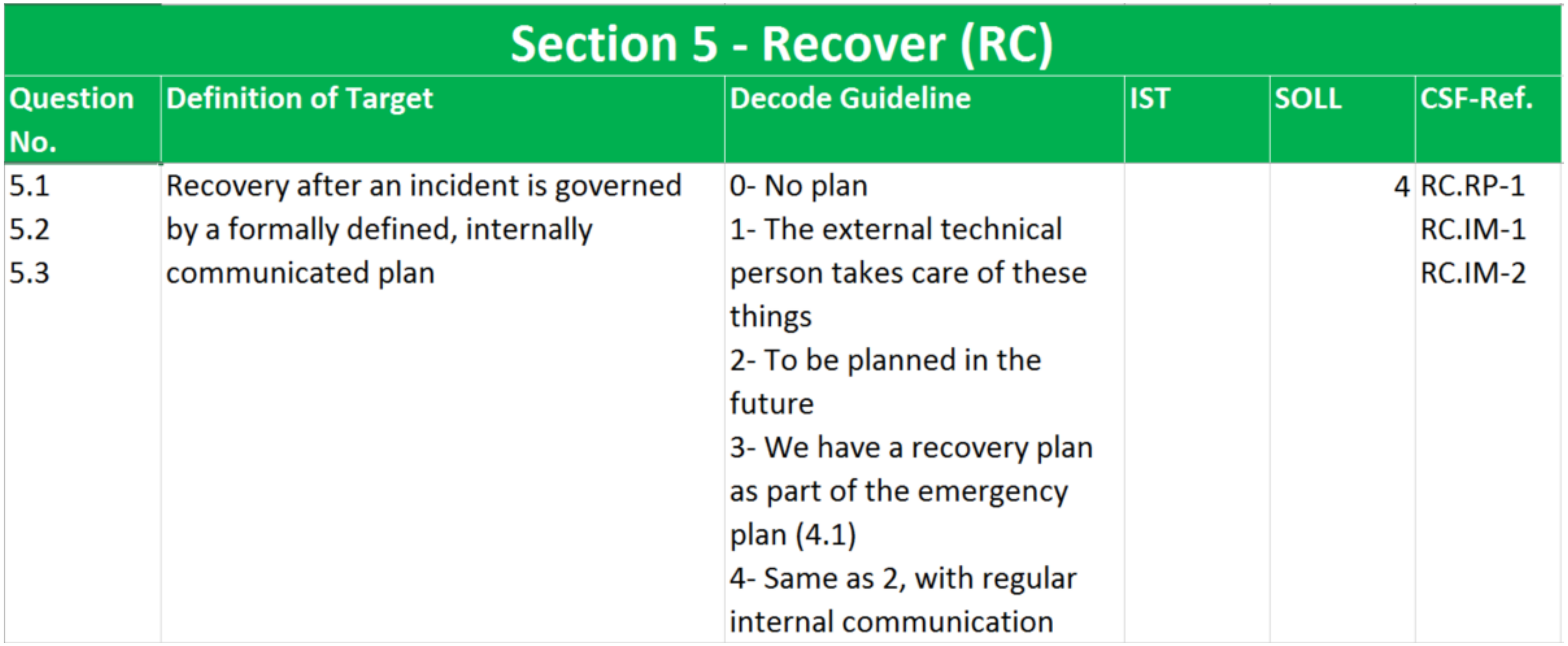
Section 4 - Respond (RS)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
4.2 4.3	Breaches involving third parties' data are treated with appropriate, formally defined procedures to communicate with stakeholders	0- Never thought of anything like this 1- We try to hush and keep everything dark 2- We inform the involved parties and work together to address the issue 3- Same as above, but as a formal process 4- Same as 3, but with implication of legal requirements		4	RS.CO-4

Sviluppo di una metodologia semplificata



Section 4 - Respond (RS)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
4.4 4.5 4.6	Incidents are investigated, analysed and conclusions are drawn, including impact and lessons learned, and feedback is communicated to the organisation; as a formally defined process.	0- No 1- Some understanding is gathered by the external technical person 2- Same as 1, but with active co-operation of internal staff 3- Better process to be planned in the future 4- Formal internal investigation process exists 5- Same as 3, with official internal communication and feedback		5	RS.CO-5

Sviluppo di una metodologia semplificata



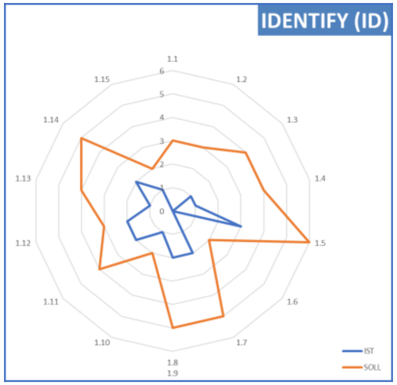
Section 5 - Recover (RC)					
Question No.	Definition of Target	Decode Guideline	IST	SOLL	CSF-Ref.
5.1 5.2 5.3	Recovery after an incident is governed by a formally defined, internally communicated plan	0- No plan 1- The external technical person takes care of these things 2- To be planned in the future 3- We have a recovery plan as part of the emergency plan (4.1) 4- Same as 2, with regular internal communication		4	RC.RP-1 RC.IM-1 RC.IM-2

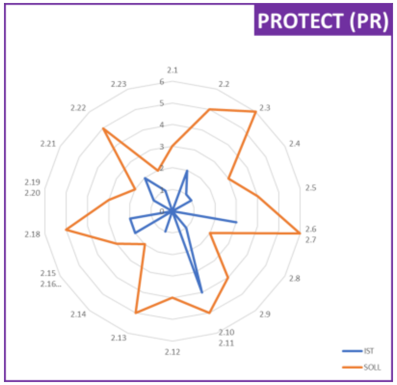
Sviluppo di una metodologia semplificata

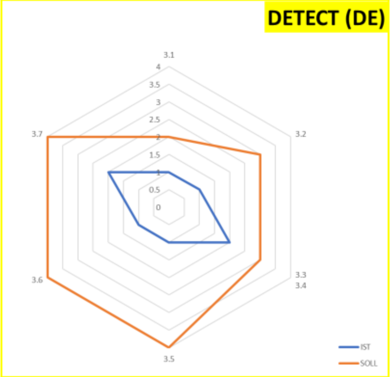
- Risultato dell’assessment
  - Visualizzazione grafica del gap mediante «radar map»
  - Rapporto dettagliato
    - Stima di ciascun rischio
    - Ordine di priorità
    - Misure immediate
  - Executive Summary
    - Security Score 1-10
  - Risk Heat Map
    - In corso di sviluppo

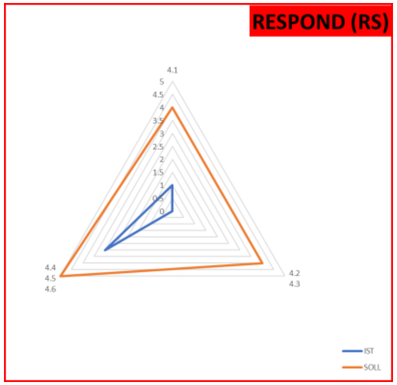
Sviluppo di una metodologia semplificata

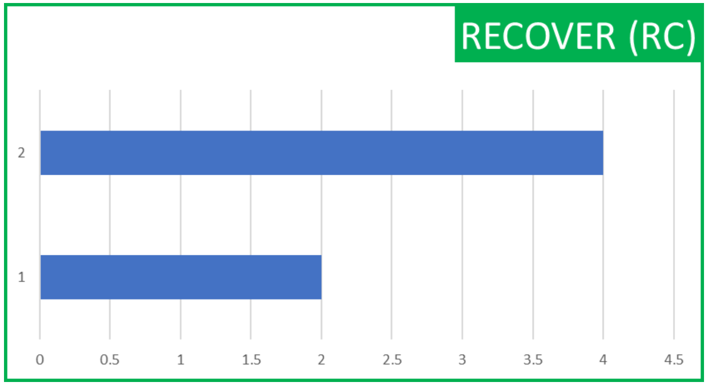
- Gap analysis





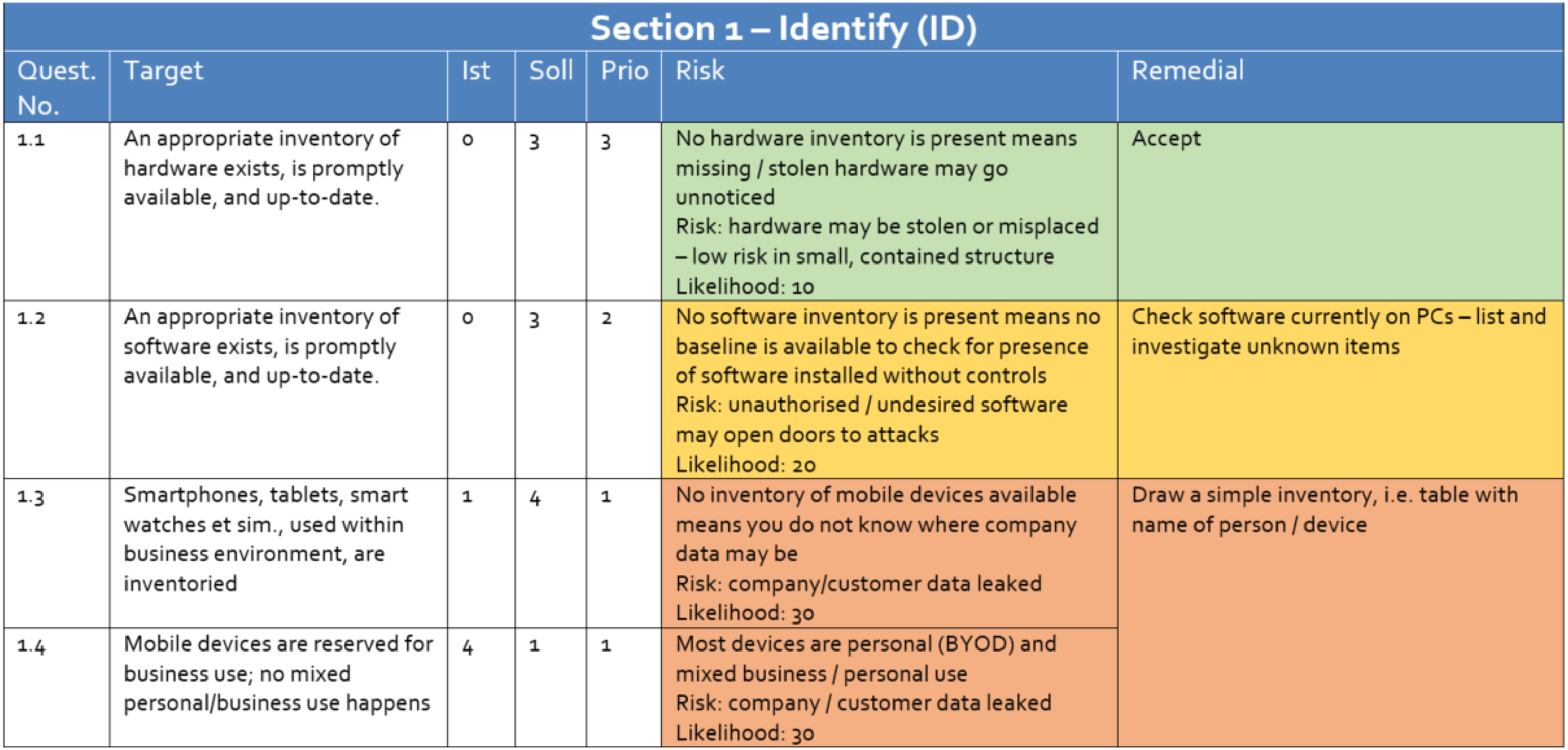






Sviluppo di una metodologia semplificata

- Rapporto dettagliato

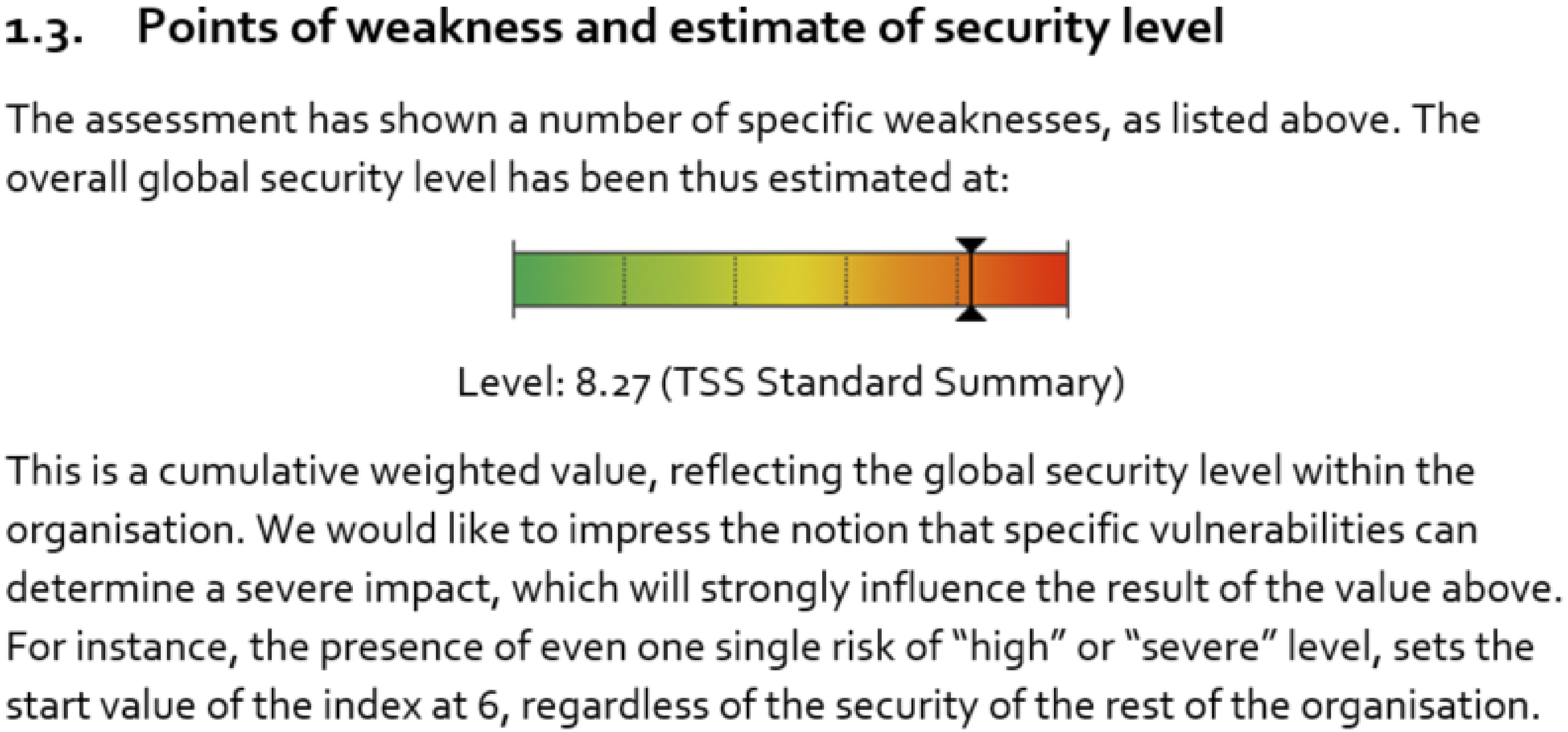


Section 1 – Identify (ID)

Quest. No.	Target	Ist	Soll	Prio	Risk	Remedial
1.1	An appropriate inventory of hardware exists, is promptly available, and up-to-date.	0	3	3	No hardware inventory is present means missing / stolen hardware may go unnoticed Risk: hardware may be stolen or misplaced – low risk in small, contained structure Likelihood: 10	Accept
1.2	An appropriate inventory of software exists, is promptly available, and up-to-date.	0	3	2	No software inventory is present means no baseline is available to check for presence of software installed without controls Risk: unauthorised / undesired software may open doors to attacks Likelihood: 20	Check software currently on PCs – list and investigate unknown items
1.3	Smartphones, tablets, smart watches et sim., used within business environment, are inventoried	1	4	1	No inventory of mobile devices available means you do not know where company data may be Risk: company/customer data leaked Likelihood: 30	Draw a simple inventory, i.e. table with name of person / device
1.4	Mobile devices are reserved for business use; no mixed personal/business use happens	4	1	1	Most devices are personal (BYOD) and mixed business / personal use Risk: company / customer data leaked Likelihood: 30	

Sviluppo di una metodologia semplificata

- Executive Summary



1.3. Points of weakness and estimate of security level

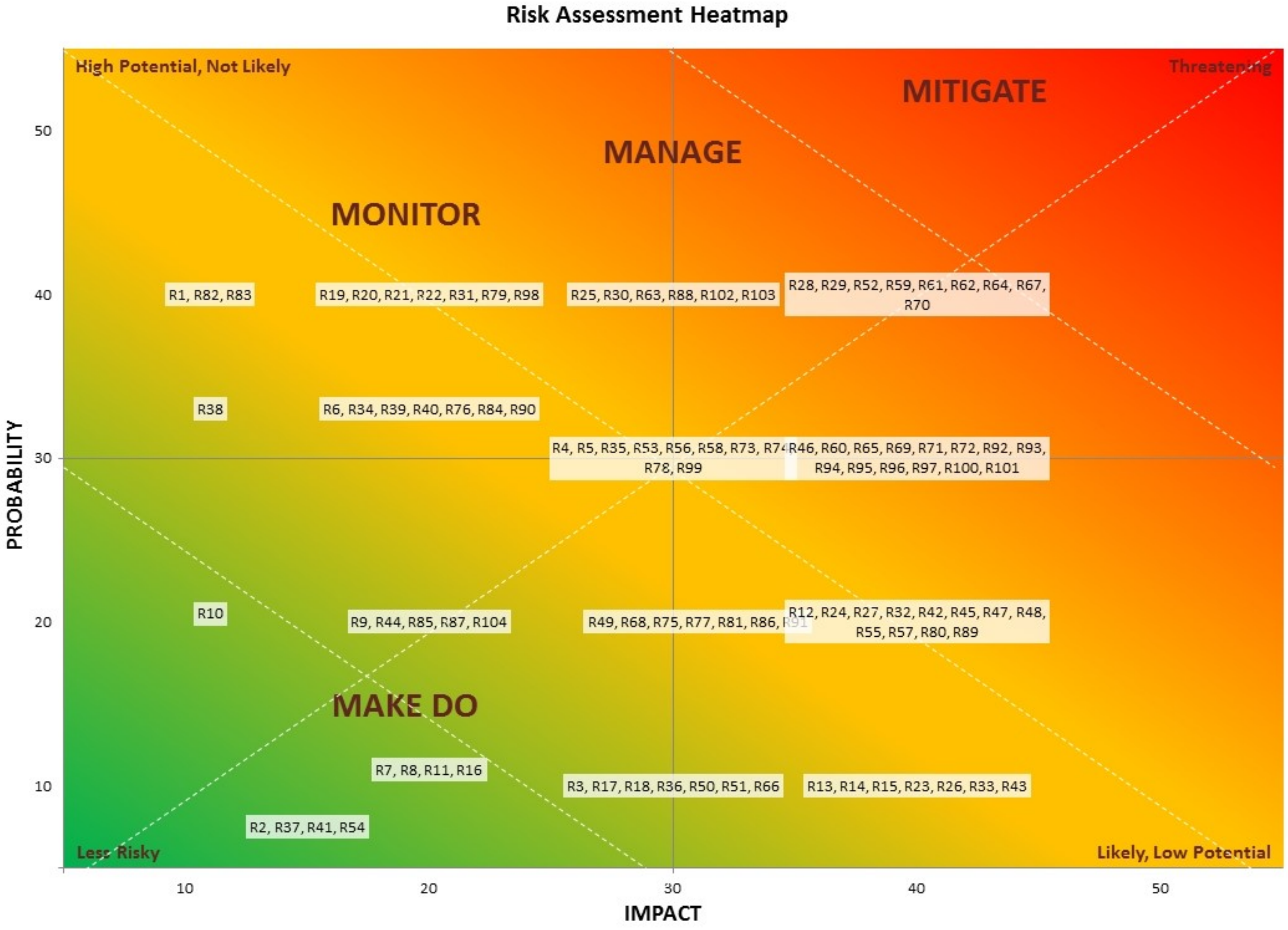
The assessment has shown a number of specific weaknesses, as listed above. The overall global security level has been thus estimated at:

Level: 8.27 (TSS Standard Summary)

This is a cumulative weighted value, reflecting the global security level within the organisation. We would like to impress the notion that specific vulnerabilities can determine a severe impact, which will strongly influence the result of the value above. For instance, the presence of even one single risk of "high" or "severe" level, sets the start value of the index at 6, regardless of the security of the rest of the organisation.

Sviluppo di una metodologia semplificata

- Risk Assessment Heatmap



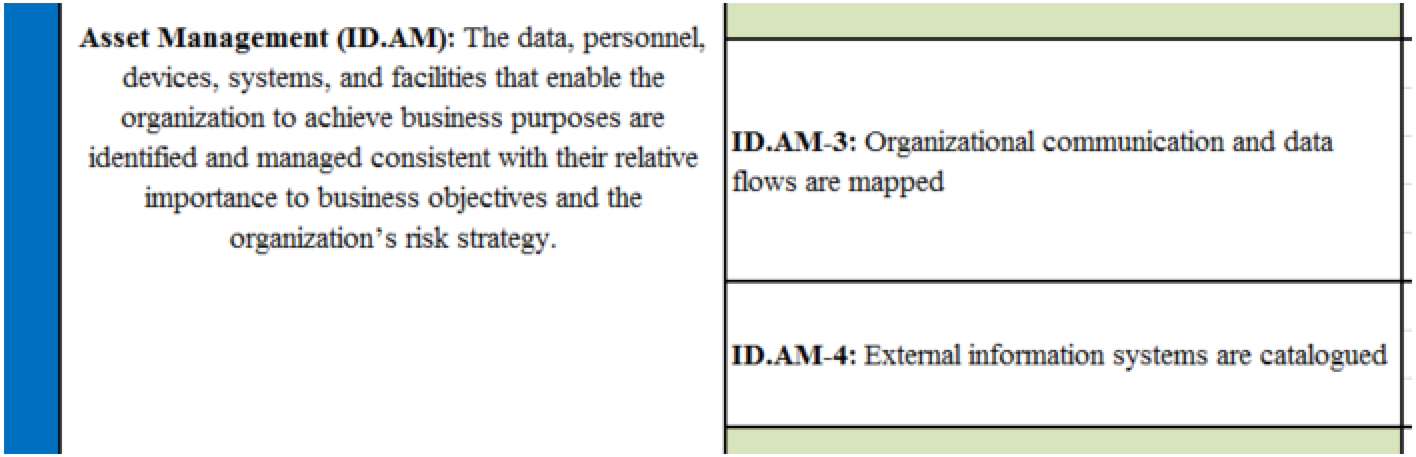
Sviluppo di una metodologia semplificata

- Follow-up
  - Il risultato dell'assessment è un check-up che mostra la distanza tra una situazione ideale (teorica) e lo stato attuale
  - Nel rapporto sono indicate alcune contromisure immediate che possono ridurre i livelli rilevati di alcuni specifici rischi
  - In entrambi i casi è previsto un follow-up, con lo sviluppo di un processo di sicurezza

Sviluppo di una metodologia semplificata

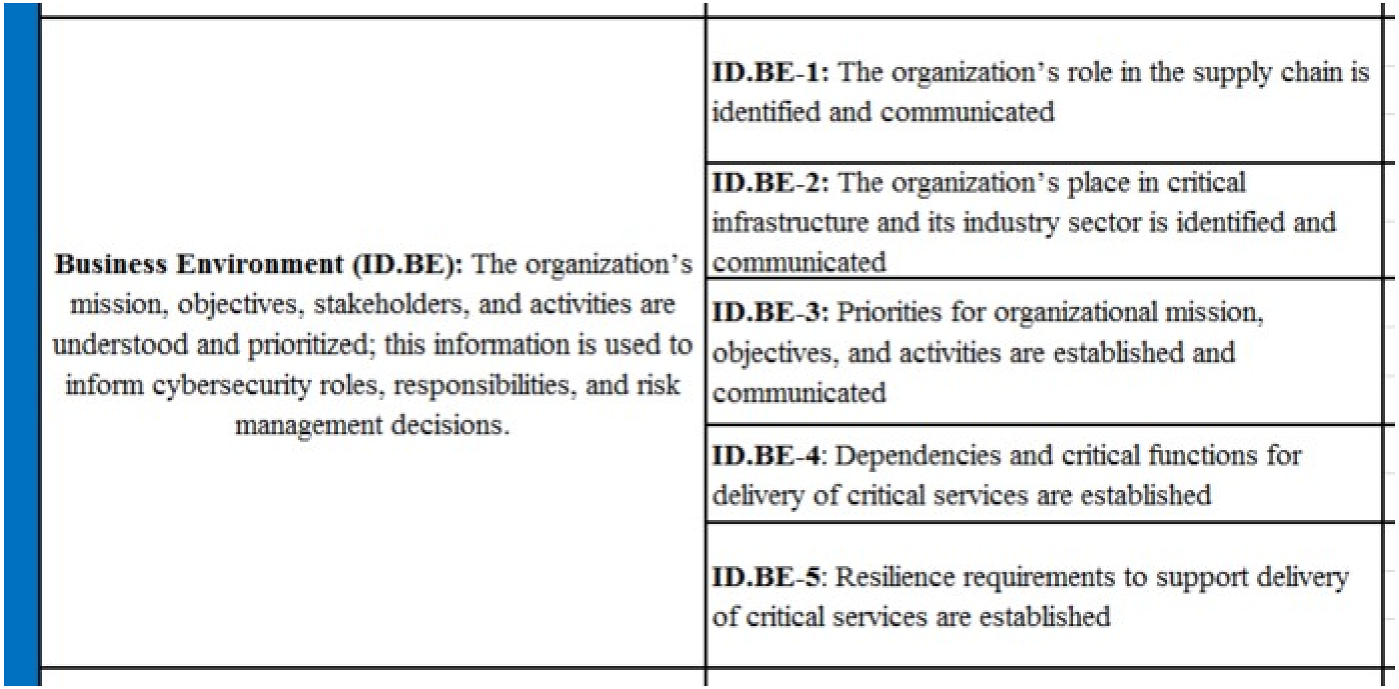
- Criteri di semplificazione
  - Confronto con «Controlli Essenziali di Cybersecurity» (CEC)
  - CEC: approccio «bottom-up»
  - TSS: approccio «top-down»
  - Alcuni esempi di sottocategorie eliminate

Sviluppo di una metodologia semplificata



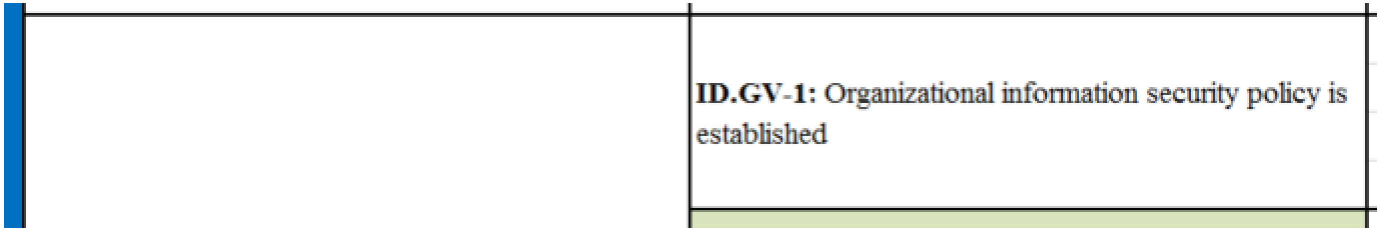
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-3:** Organizational communication and data flows are mapped
	ID.AM-4: External information systems are catalogued

Sviluppo di una metodologia semplificata



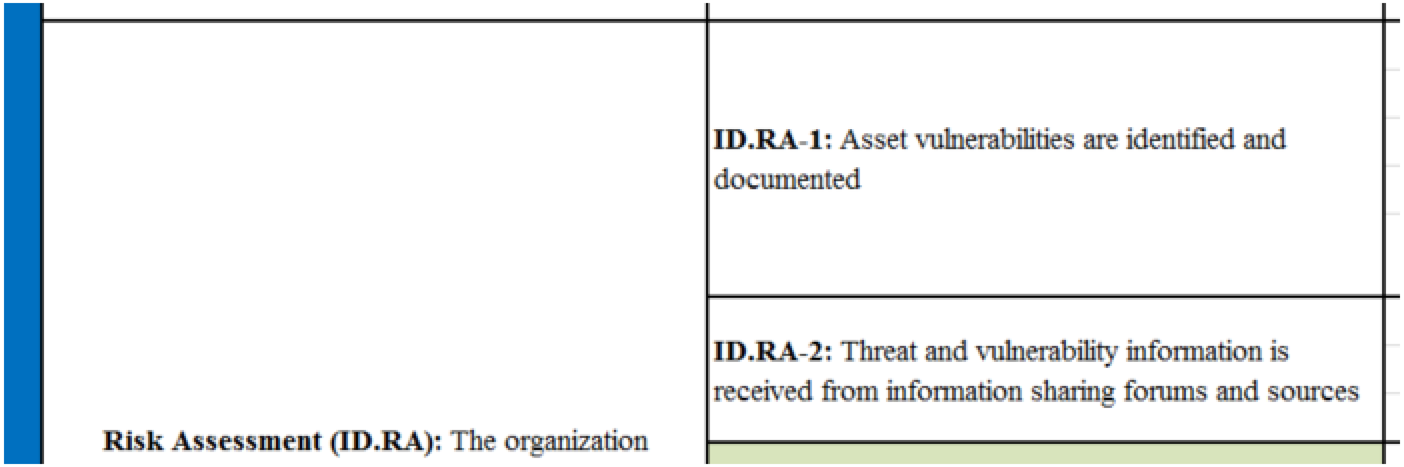
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established
	ID.BE-5: Resilience requirements to support delivery of critical services are established

Sviluppo di una metodologia semplificata



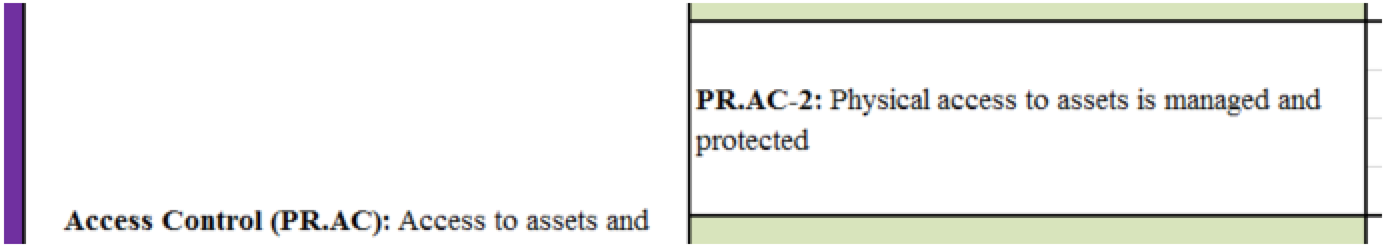
	ID.GV-1: Organizational information security policy is established

Sviluppo di una metodologia semplificata



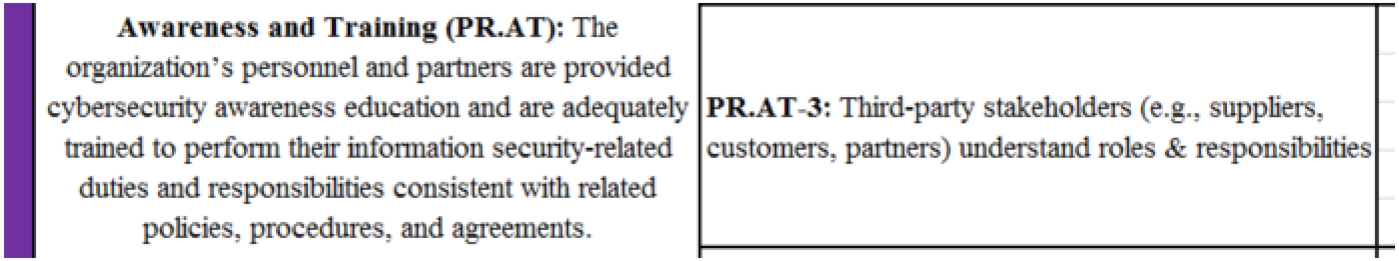
Risk Assessment (ID.RA): The organization	**ID.RA-1:** Asset vulnerabilities are identified and documented
	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources

Sviluppo di una metodologia semplificata



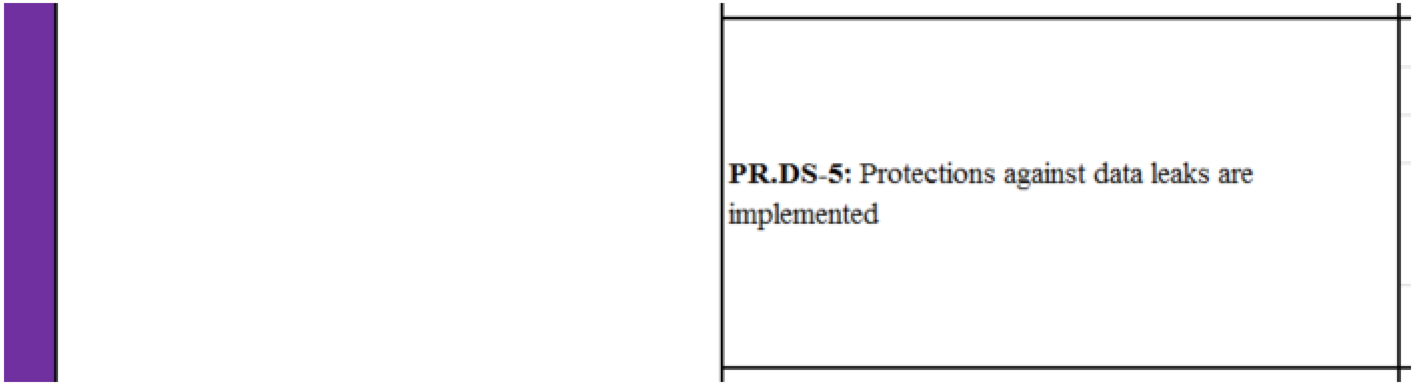
Access Control (PR.AC): Access to assets and	**PR.AC-2:** Physical access to assets is managed and protected

Sviluppo di una metodologia semplificata



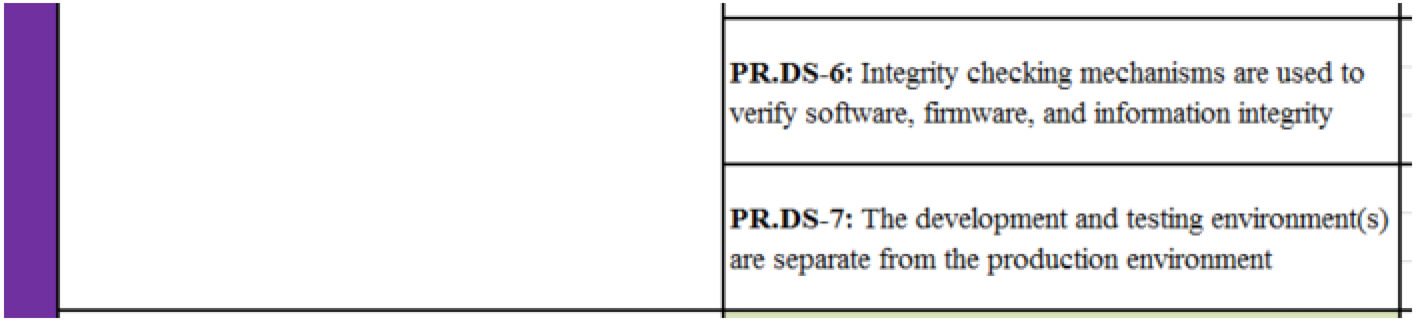
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities

Sviluppo di una metodologia semplificata



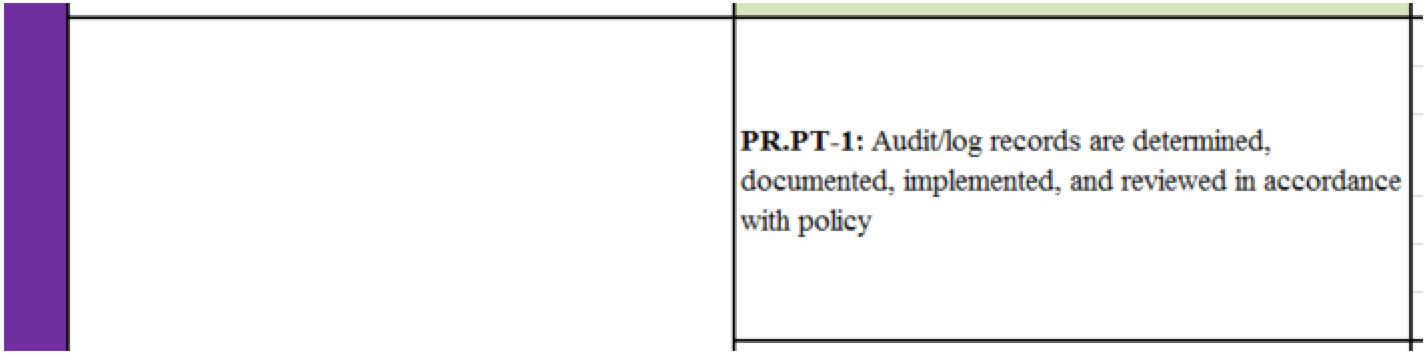
PR.DS-5: Protections against data leaks are implemented

Sviluppo di una metodologia semplificata



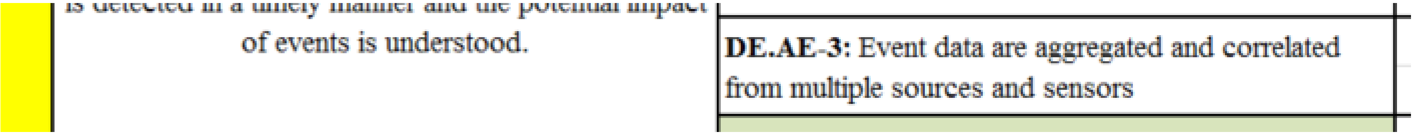
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
		PR.DS-7: The development and testing environment(s) are separate from the production environment

Sviluppo di una metodologia semplificata



PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

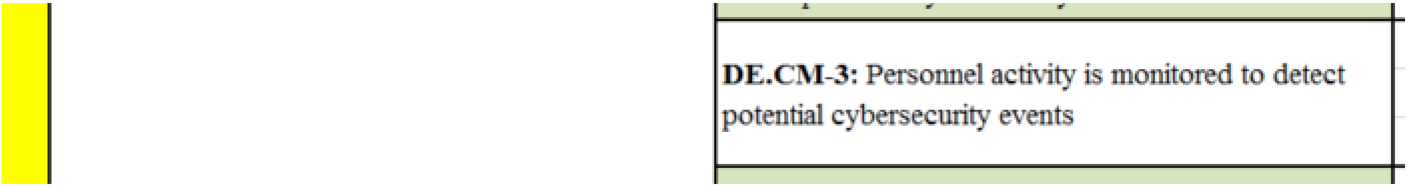
Sviluppo di una metodologia semplificata



is detected in a timely manner and the potential impact of events is understood.

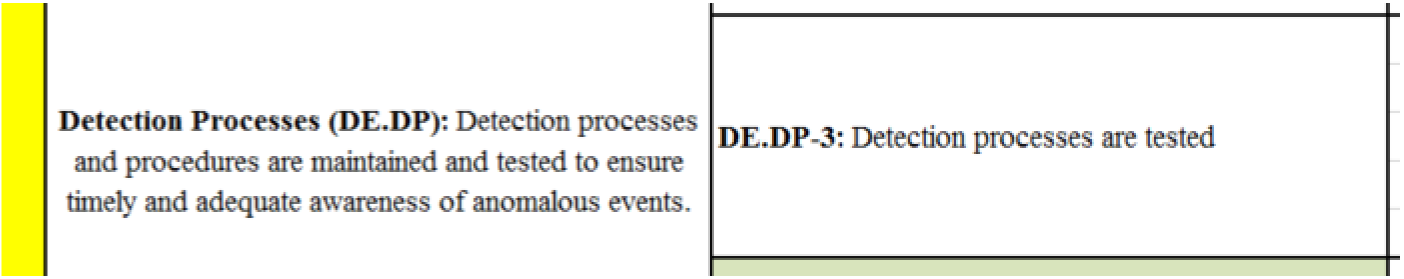
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors

Sviluppo di una metodologia semplificata



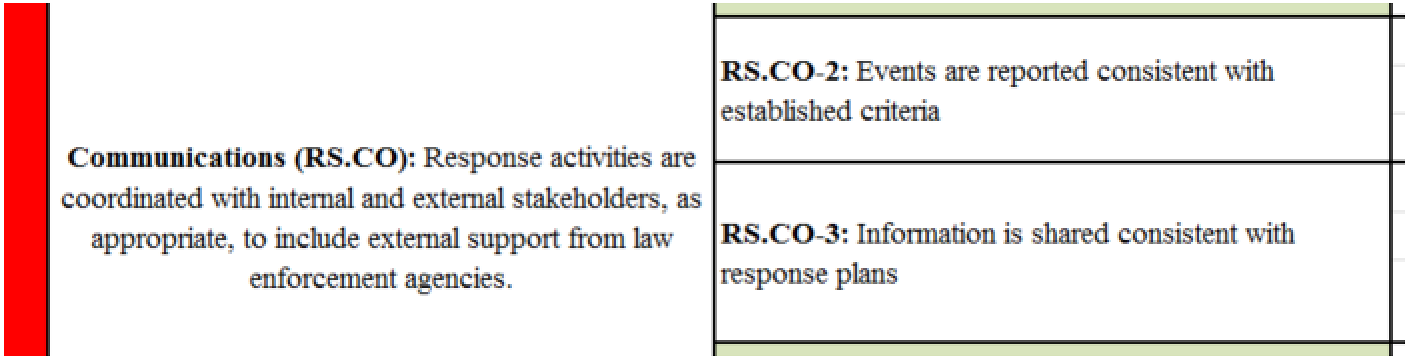
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

Sviluppo di una metodologia semplificata



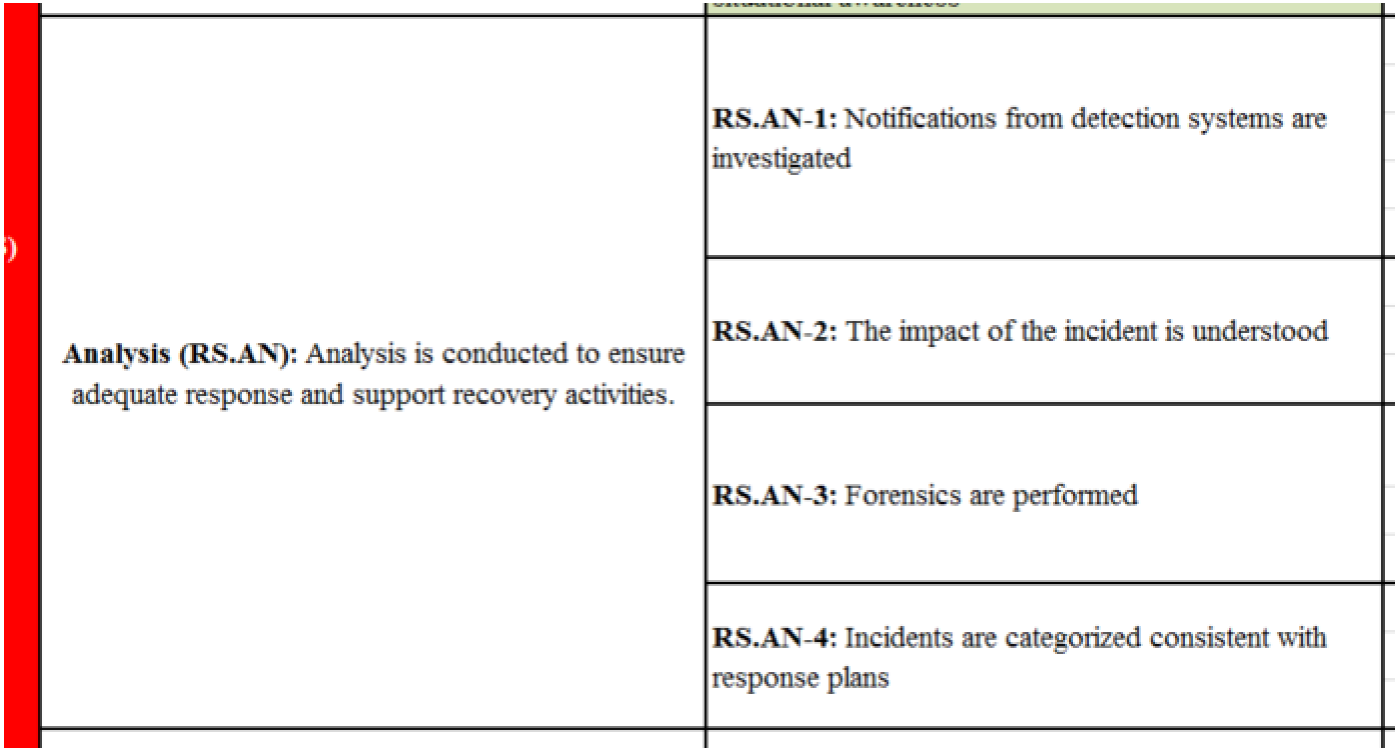
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-3:** Detection processes are tested

Sviluppo di una metodologia semplificata



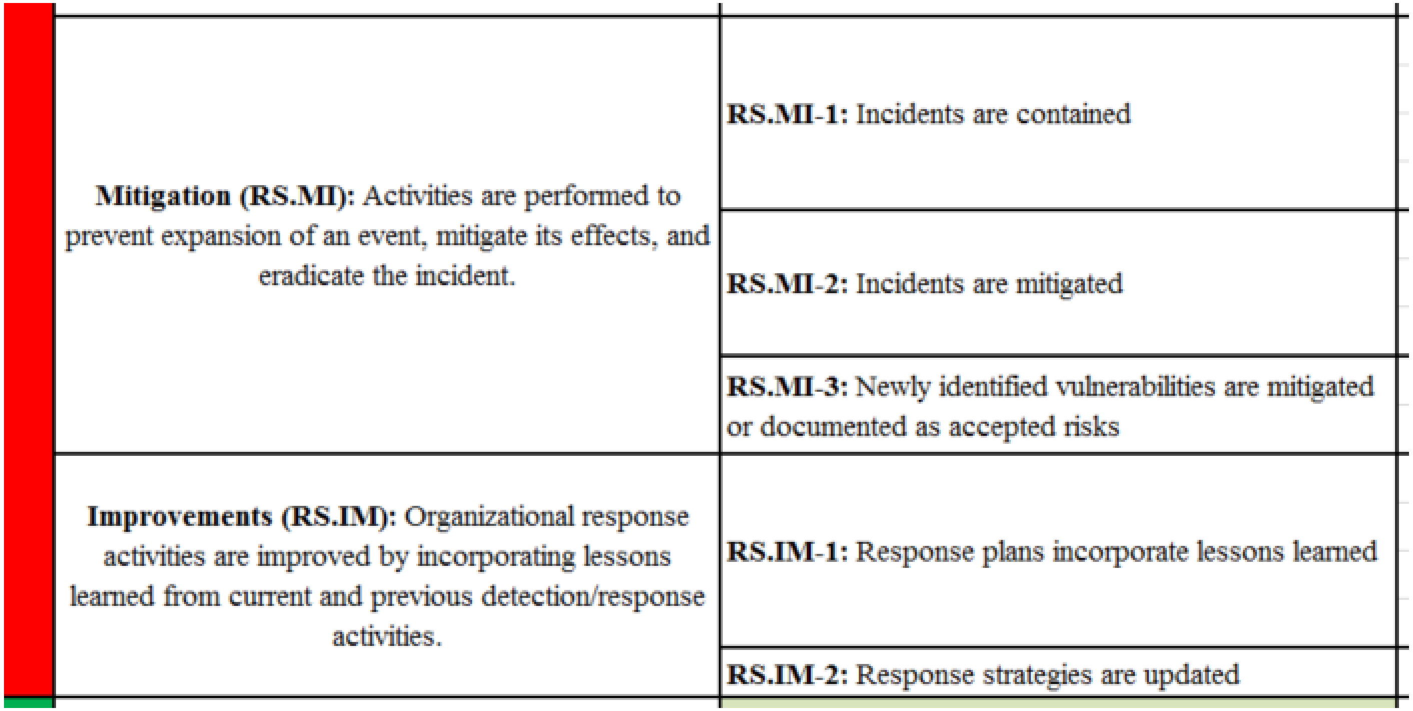
🟥	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-2:** Events are reported consistent with established criteria
		RS.CO-3: Information is shared consistent with response plans

Sviluppo di una metodologia semplificata



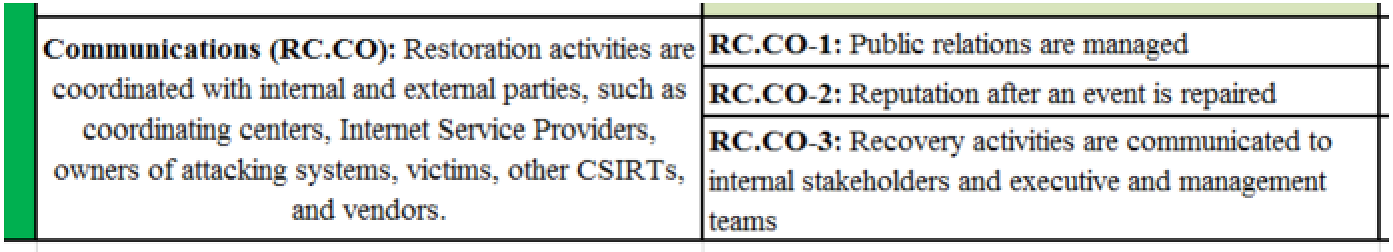
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated
	RS.AN-2: The impact of the incident is understood
	RS.AN-3: Forensics are performed
	RS.AN-4: Incidents are categorized consistent with response plans

Sviluppo di una metodologia semplificata



Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained
	RS.MI-2: Incidents are mitigated
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned
	RS.IM-2: Response strategies are updated

Sviluppo di una metodologia semplificata



Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed
	RC.CO-2: Reputation after an event is repaired
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams

Agenda

- Presentazione relatore
- Diciotto anni di esperienza con l'ISO 27001 (e BS7799 prima): successi e insuccessi in Italia e all’estero
- Obiettivi di sicurezza delle strutture di dimensioni minori
- Sviluppo di una metodologia semplificata e sua applicazione
- ➡ Conclusioni e prospettive
- Q&A
- Bibliografia

Conclusioni e prospettive

- Risultati sul campo
  - Approccio promettente
  - Serve approccio analogo per il follow-up (sviluppo processo), tagliato su esigenze del target
  - Lavoro in corso: riduzione dell’elemento personale nella valutazione dei rischi

Agenda

- Presentazione relatore
- Diciotto anni di esperienza con l'ISO 27001 (e BS7799 prima): successi e insuccessi in Italia e all’estero
- Obiettivi di sicurezza delle strutture di dimensioni minori
- Sviluppo di una metodologia semplificata e sua applicazione
- Conclusioni e prospettive
- ➡ Q&A
- Bibliografia

Q&A

Agenda

- Presentazione relatore
- Diciotto anni di esperienza con l'ISO 27001 (e BS7799 prima): successi e insuccessi in Italia e all’estero
- Obiettivi di sicurezza delle strutture di dimensioni minori
- Sviluppo di una metodologia semplificata e sua applicazione
- Conclusioni e prospettive
- Q&A
- Bibliografia

Bibliografia

- National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity
  https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
- VdS (Vertrauen durch Sicherheit): VdS 3473 - Cyber-Security für kleine und mittlere Unternehmen (KMU)
  https://vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf
- National Cyber Security Centre: The Critical Security Controls for Effective Cyber Defense
  https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/2014-04-11-critical-security-controls.pdf
- 2016 Italian Cybersecurity Report
  http://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf
- Zurich Schweiz: Schweizer KMU sind nicht vor Cybercrime geschützt
  https://www.zurich.ch/-/media/zurich-site/news-download/2016/20161123-schweizer-kmu-sind-nicht-vor-cybercrime-geschuetzt/kmu-schweiz-sind-nicht-vor-cybercrime-geschuetzt.pdf?la=de

Bibliografia

- Computerworld, Ein Drittel der Schweizer KMU hat keine Cybersicherheits-Strategie
  http://www.computerworld.ch/news/security/artikel/ein-drittel-der-schweizer-kmu-hat-keine-cybersicherheits-strategie-72947/
- Swisscom, Cyber Security 2017: Data Breaches & Bug Bounties
  https://www.swisscom.ch/it/business/enterprise/downloads/security/security-report.html
- +Finance: Le PMI sottovalutano il pericolo degli attacchi informatici
  https://plusfinance.postfinance.ch/it/le-pmi-sottovalutano-il-pericolo-degli-attacchi-informatici-289935
- S. Cattaneo: «Aziende a prova di hacker», Supsi
  http://www.supsi.ch/dti/dms/dti/docs/eventi-comunicazione/news/incident_response_manager-1.pdf

Contatti

- stefano@toriasecuresystems.com

Grazie…