TL GROUP
AN ALLIANCE BETWEEN TECH AND LEGAL EXPERTS

DIGITAL WORKING GROUP – CCIFC

CYBER SAFETY 101:
PREPARE FOR THE QUESTIONS PRC AUTHORITIES MAY ASK YOU AFTER A CYBER BREACH

01. About us

A group organization bringing Technology and Legal together

TL Group is the result of a joint-venture between Leaf and TekID to bridge **digital security** and **cyber regulatory framework** in a holistic approach since worldwide countries are increasingly asking for Cyber space sovereignty.

It is nowadays much harder, if not impossible, to achieve satisfying results without involving these two skills alongside.

02. About us

A Digital Risks Intelligence company specialized in cyber security

TekID is a company delivering business intelligence through a methodology called A.I.M. to evaluate risks in Cyber space, Innovation programs and IT Transformation

TekID Purpose is to helps organizations mitigate cyber threats and digitalization risks, by providing business intelligence beyond technical aspects and issues.

It can be to manage compliance programs (CSL, GDPR, ISO, SOC, SOX, PCI, …), Evaluate technology solutions, audit your company (Security Audit, Penetration test, SAPIN2, FCPA, …), perform a Computer Forensic Investigation and Cyber Threats Intelligence (CFI, CTI) or to have technology experts working side by side with you.

A corporate law firm specialized in Transactions in China

We are corporate lawyers based in China. Our firm has been licensed by the Ministry of Justice. Our team is composed of Chinese and internationally qualified attorneys.

Our experience allows us to fully understand the legal implications and risks of doing business in China.

Our methodology implies that we work in bi-cultural team to provide efficient solutions to navigate through the complex legal environment around the world.

LAW FIRM BRIDGING EUROPE & ASIA

TL GROUP

DEALING WITH A CYBER SECURITY BREACH

03. Raising the alert!

BY FAILING TO PREPARE, YOU ARE PREPARING TO FAIL

One of the major problem in crisis management is to accept / identify the existence of the crisis

Raising an alert is a combination of intelligent, reasonable and logic ways of thinking which tend to disappear or being blurred under unstable emotions and stressful environment.

How to prevent it? Just like military do to ensure their soldiers to be operational when under fire: Drill test should be done, frequently, until appropriate response become part of an automatic and spontaneous response from your organization.

An incident has happened, do not think it may not be a problem.
With or without investigation from the authority something already happened.
Breath…don't act in a rush (because you are now prepared thanks to EUCC) your next actions will be critical.

04. Containment

An incident has happened, and you have raised an Alert, but it will, most likely, **take sometimes for your crisis organizations to fall into place and being operational**. In the meantime, **primary containment of the Cyber Incident cannot wait** and should be ensured.

A Cyber Breach can use many techniques with very different targets. No matter if the attack is trying to achieve a data breach, impersonate users, compromise services, hijack communications or steal Intellectual Property, you most stop its spreading immediately.

Depending on the criticality of the attack(s) and the targeted system(s), you may not be able to contain the attack without shutting down core infrastructure / system. This could be highly disruptive to your business but in today's world it is a must do – both from hackers' capabilities and regulatory obligations – and you should proceed in such way.

Containment does not mean resolutions of the Cyber incident, not yet.
It mean that you have took preventive measures to stop the spreading of the attack and its severity.
Your containment actions should be provided to the CIRT as

05. Build up an action plan

An incident has happened, you have raised an Alert and the threat is contained!
It is now time for your **CIRT (Cyber Incident Response Team)** to gather and build up an action plan.

In every company, the CIRT may take various form and be composed of different persons. However, here is the main similarities that should be held by the CIRT:

- A clear description and/or organizational chart with definition of hierarchical, escalation and reporting lines
- Members from both technical (IT) and business units (Finance manager, board members, CEO, …)
- Decision power to ensure swift response and engage company in remediation of the crisis
- Communication spokespersons capable to communicate on behalf of the company

During a time of Cyber crisis they should be responsible in designing the proper action plan which should include, at least, the following points:

- Appoint adequate response team across the company
- Implement a crisis reporting process
- Provide / continue the initial response to the threat and start investigation of Cyber incident
- Remediation plan to ensure business recovery
- Determine proper PR communications strategy and reporting
- Analyze law enforcement requirements and initiate compliance response

06. GENERAL REMARKS – Avoid conflict of interest

When facing a Cyber crisis, you may end up in a difficult position where the **company interest are in conflict with the Cyber crisis management.**

What are the most common conflict of interest?
The absolute necessity for a company, specially when financial loss are involved, is to restore the activities delivered by the impacted services from the attacks despite Cyber and crisis best practices. It also can be a conflict in advising internally, on matters which can be difficult at a company level due to cross-department implications. Legal affairs are sensible when your company is victim of a cyber attack, evaluating the liabilities and company legal stance becomes sensitive.

How to prevent such conflict of interest?
Having a CIRT does not completely erase such conflict of interest despite their required independence in the crisis remediation. Gathering partners and external consultant are key to ensure fact-based and objective analysis of problems and solutions and advising you properly.

07. GENERAL REMARKS - Management crash-test

Time of crisis can reveal the best out of your employees… or the worst. It is established that there is direct correlation in the positive or negative resolution of a cyber crisis based on the quality of management within the company. During time of crisis it is commonly overlooked thinking that it is normal due to the pressure.

What are the most common management mistakes?
The absence or fight for responsibility, a management by fear, internal politics and financial considerations, lack of support. They all have different implications, but they will all results in improper collaboration and biased communications which will drive the company crisis management in an improper way.

How to prevent such misbehavior?
When a CIRT is not implemented before or during the crisis, such misbehavior could become very difficult to strangle. At that moment, a good approach could be to outsource the crisis management to a third party or for a sponsor (CEO, Legal representative or other executive member) to take the leadership of the crisis.

08. GENERAL REMARKS - Return On Experience (ROE)

Not only ROE are key and best practices in many industries and activities, it is even more important when facing a legal investigation or liabilities.

What impact when we miss to write the ROE?
Authorities (and insurance, if any) will always require specific supporting evidences and report. Failing to provide such documents can results in refusal of the claim or intangible information. Therefore the company would have to support higher liabilities has it already suffered

Can the ROE be drafted afterward?
Legally or in terms of compliance it could. Technically, it may not be possible anymore. During stages of containment and business continuity you may ending deleting evidences (logs, servers, network connection, …) which were part of your evidences. It is also far more difficult to transcript afterward, specifically when a crisis last for days or weeks.

How to implement a proper and mandatory ROE?
Specific software can be implemented, and it should further be designed by the CIRT how to collect, centralize and analyze information throughout the whole crisis. It is also part of the CIRT responsibility to document the crisis through reporting. In most unprepared organizations, and email thread with enclosed evidences can constitute a good enough crisis tracking.

09. Wrapping up

In practice, facing an investigation is effectively crisis management, and like for any crisis, failing to plan is a plan to fail when it comes to responding to it. These plans need to be stress tested and need full support from top management to invest in the necessary people and processes.

Spending some time developing protocols to manage an investigation before it arises will make a big difference to the ability of your organization to respond in a strategic and considered way.

One the most difficult challenge is when the organization itself is reluctant to accept the fact that the investigation is a serious thing and will not be that easy to manage. This comes when an organization is in denial, believing it has a robust compliance program, or that compliance gaps can be explained away, or worse yet, that they simply believe that they can negotiate with regulators or con them.

Another big challenge is when the organization does not respect the investigation, with internal fights and a negligent or hostile approach, because it believes that nothing could ever go wrong. They will not get fined or suffer other consequences. Not them. Not to us.

That really does send a very, very clear message, not only internally, but externally as well. It's actually an indication that there's a problem with the culture, there's a problem with the compliance program, there's generally a problem with governance overall.

TL GROUP

REPORTING CYBER BREACHES & REGULATORY EXPECTATIONS

10. Regulatory considerations before crisis

BEFORE CRISIS

1. Awareness of the risks in case of cybersecurity breaches:

- You cannot avoid to deal with it because of the high level of risk
- Corporate risks: fines and interruption of activities
- Personal risks: fines and jail time (3Y>7Y if the circumstances are especially serious)

2. Prevent by knowing the legal framework applicable to CSL

- What is your qualification?
  - Network Operator (NOP) / Critical Infrastructure Information Operator (CIIO)
- Determine your level?
  - MLPS provides several levels from 1 to 5 with hierarchical protection system
  - Determination according to GA/T 1389—2017 Information security technology - Guidelines for grading of classified protection of cyber security
  - Levels shall be self assessed and communicated to the PRC authorities
- Know your obligations:
  - Obligation to define and implement disaster backup, incident protocols and organize incident-specific training
  - Obligation to do self assessment and to disclose it to the authorities
  - Obligation to ensure stability and continuity of the services

3/ Prevent by knowing the legal framework applicable to investigations in China

- Can privileged material be lawfully protected from seizure?
  - wide powers of authorities to size documents. No right to resist the disclosure.
- Are search warrants a feature of law enforcement in China?
  - Pursuant to PRC Criminal Procedure law, a search warrant released by head of the PSB or chief prosecutor is normally required. However, search may be conducted without warrants where a person under investigation may destroy evidence of a crime. In practice, PRC laws imposes few limitations on authorities executing search operations.
  - No concept of attorney-client privilege exists in China.
- How to respond to the authorities?
  - Possible to enter into a dialogue with the investigating authority to clarify the scope of evidence sought. The authorities are free to accommodate any request.

11. Regulatory considerations during reporting

SELF ASSEMENT / REPORTING

Main principles of the reporting for self assessment

Form to be filled in by the tier-2 or higher "recording-filing organization".

Table 1: Information for organizations

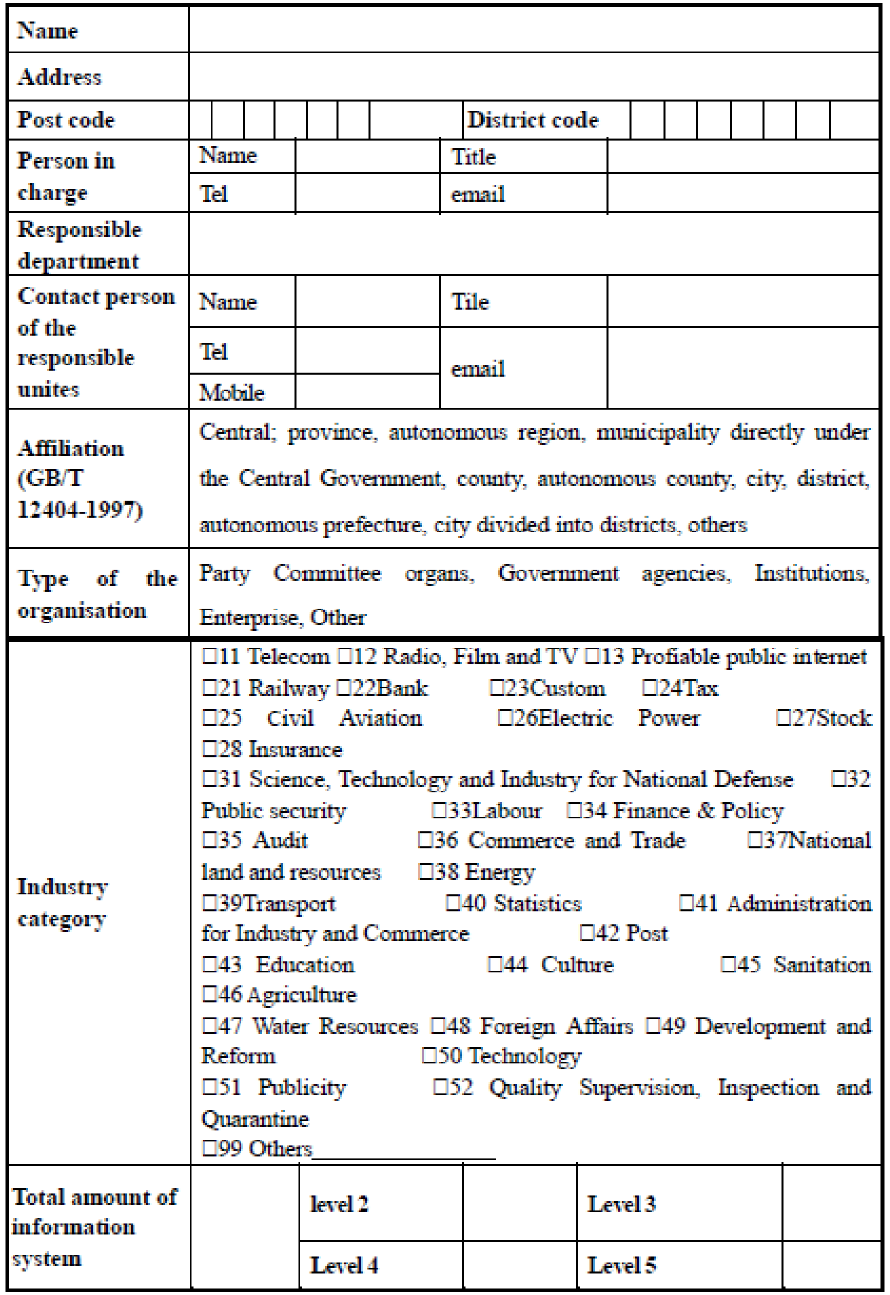
Table : Basic information for information system

Table 3: Information for classification of information system

Table 2 and Table 3 shall be filled by each information system.
The content that needs to be submitted by tier-3 or higher system shall be filled in Table 4.

Form to be submitted to the PSB or specific authorities (MIIT?) = public security organs that accept record-filing after the completion of system construction, rectification and evaluation, etc.

Table 1 Basic information of organization



Name					
Address					
Post code			District code		
Person in charge	Name		Title		
	Tel		email		
Responsible department					
Contact person of the responsible unites	Name		Tile		
	Tel		email		
	Mobile				
Affiliation (GB/T 12404-1997)	Central; province, autonomous region, municipality directly under the Central Government, county, autonomous county, city, district, autonomous prefecture, city divided into districts, others				
Type of the organisation	Party Committee organs, Government agencies, Institutions, Enterprise, Other				
Industry category	□11 Telecom □12 Radio, Film and TV □13 Profiable public internet □21 Railway □22Bank □23Custom □24Tax □25 Civil Aviation □26Electric Power □27Stock □28 Insurance □31 Science, Technology and Industry for National Defense □32 Public security □33Labour □34 Finance & Policy □35 Audit □36 Commerce and Trade □37National land and resources □38 Energy □39Transport □40 Statistics □41 Administration for Industry and Commerce □42 Post □43 Education □44 Culture □45 Sanitation □46 Agriculture □47 Water Resources □48 Foreign Affairs □49 Development and Reform □50 Technology □51 Publicity □52 Quality Supervision, Inspection and Quarantine □99 Others________________				
Total amount of information system		level 2		Level 3	
		Level 4		Level 5	

12. Regulatory considerations during reporting

SELF ASSEMENT / REPORTING

Main principles of the reporting for self assessment

Form to be filled in by the tier-2 or higher "recording-filing organization".

Table 1: Information for organizations

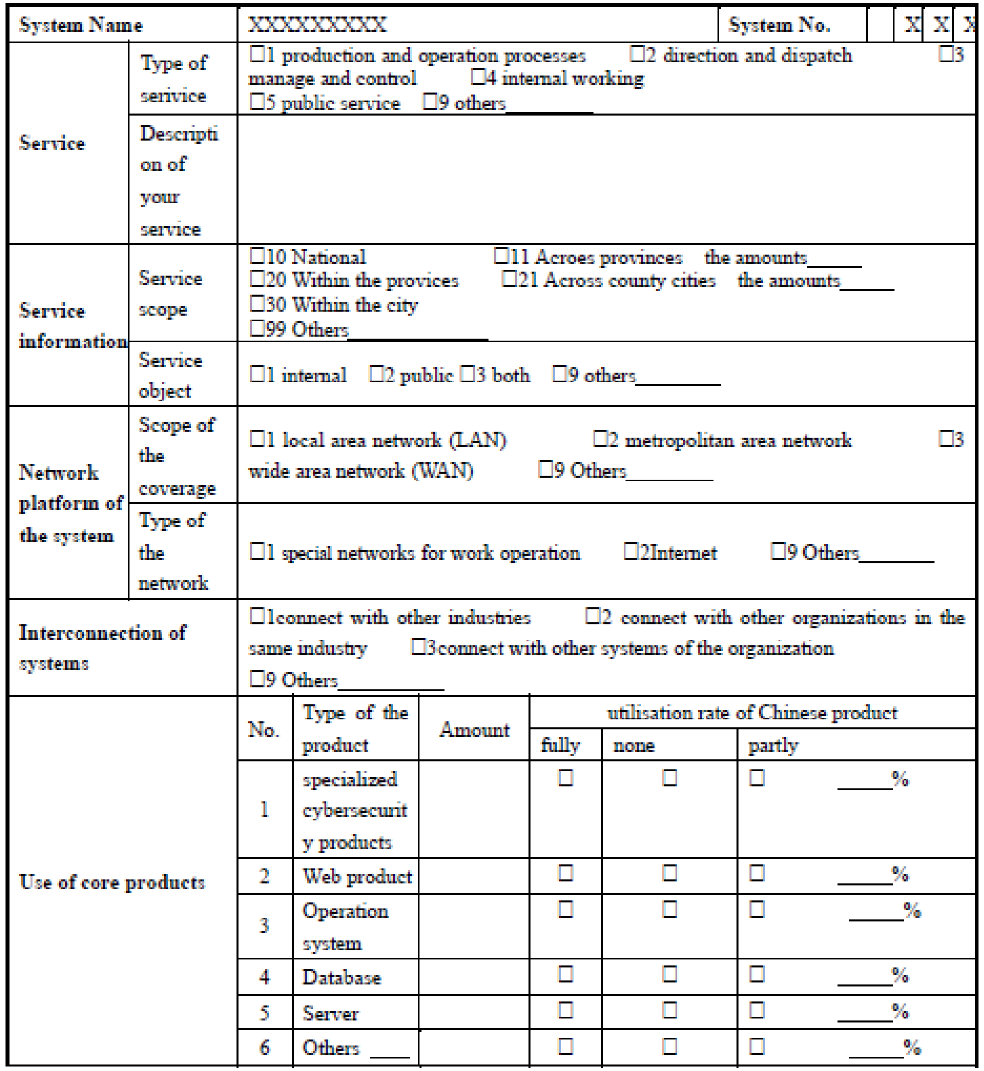
Table : Basic information for information system

Table 3: Information for classification of information system

Table 2 and Table 3 shall be filled by each information system.
The content that needs to be submitted by tier-3 or higher system shall be filled in Table 4.

Form to be submitted to the PSB or specific authorities (MIIT?) = public security organs that accept record-filing after the completion of system construction, rectification and evaluation, etc.

Table 2 Information of information system



System Name		XXXXXXXXXX			System No.		X X X
Service	Type of serivice	□1 production and operation processes □2 direction and dispatch □3 manage and control □4 internal working □5 public service □9 others________					
	Description of your service						
Service information	Service scope	□10 National □11 Acroes provinces the amounts_____ □20 Within the provices □21 Across county cities the amounts_____ □30 Within the city □99 Others____________					
	Service object	□1 internal □2 public □3 both □9 others________					
Network platform of the system	Scope of the coverage	□1 local area network (LAN) □2 metropolitan area network □3 wide area network (WAN) □9 Others________					
	Type of the network	□1 special networks for work operation □2Internet □9 Others_______					
Interconnection of systems		□1connect with other industries □2 connect with other organizations in the same industry □3connect with other systems of the organization □9 Others_________					
Use of core products		No.	Type of the product	Amount	utilisation rate of Chinese product		
					fully	none	partly
		1	specialized cybersecurity products		□	□	□ _____%
		2	Web product		□	□	□ _____%
		3	Operation system		□	□	□ _____%
		4	Database		□	□	□ _____%
		5	Server		□	□	□ _____%
		6	Others ____		□	□	□ _____%

13. Regulatory considerations during reporting

SELF ASSEMENT / REPORTING

Main principles of the reporting for self assessment

Form to be filled in by the tier-2 or higher "recording-filing organization".

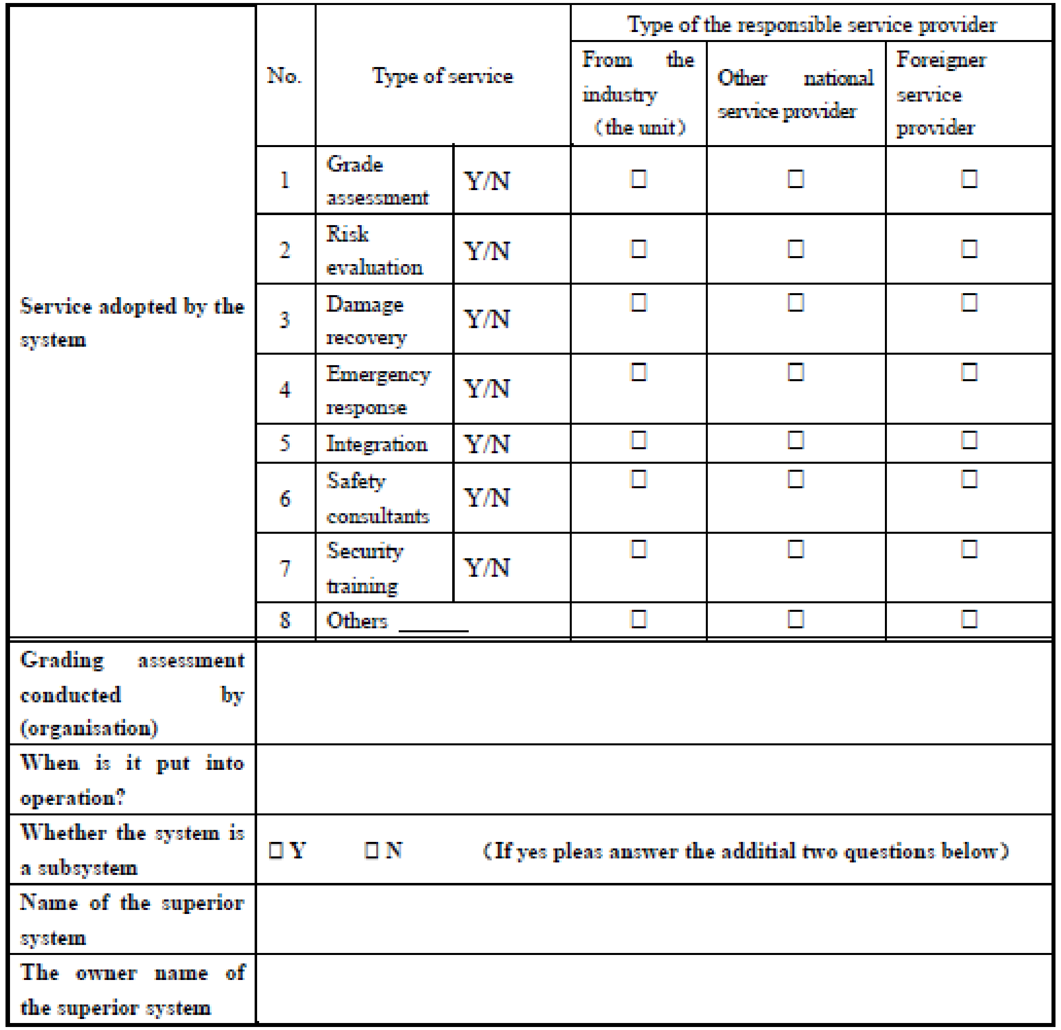
Table 1: Information for organizations

Table : Basic information for information system

Table 3: Information for classification of information system

Table 2 and Table 3 shall be filled by each information system.
The content that needs to be submitted by tier-3 or higher system shall be filled in Table 4.

Form to be submitted to the PSB or specific authorities (MIIT?) = public security organs that accept record-filing after the completion of system construction, rectification and evaluation, etc.



	No.	Type of service		Type of the responsible service provider		
				From the industry （the unit）	Other national service provider	Foreigner service provider
Service adopted by the system	1	Grade assessment	Y/N	□	□	□
	2	Risk evaluation	Y/N	□	□	□
	3	Damage recovery	Y/N	□	□	□
	4	Emergency response	Y/N	□	□	□
	5	Integration	Y/N	□	□	□
	6	Safety consultants	Y/N	□	□	□
	7	Security training	Y/N	□	□	□
	8	Others ______		□	□	□
Grading assessment conducted by (organisation)						
When is it put into operation?						
Whether the system is a subsystem	□ Y □ N （If yes pleas answer the additial two questions below）					
Name of the superior system						
The owner name of the superior system						

14. Regulatory considerations during reporting

SELF ASSEMENT / REPORTING

Main principles of the reporting for self assessment

Form to be filled in by the tier-2 or higher "recording-filing organization".

Table 1: Information for organizations

Table : Basic information for information system

Table 3: Information for classification of information system

Table 2 and Table 3 shall be filled by each information system.
The content that needs to be submitted by tier-3 or higher system shall be filled in Table 4.

Form to be submitted to the PSB or specific authorities (MIIT?) = public security organs that accept record-filing after the completion of system construction, rectification and evaluation, etc.

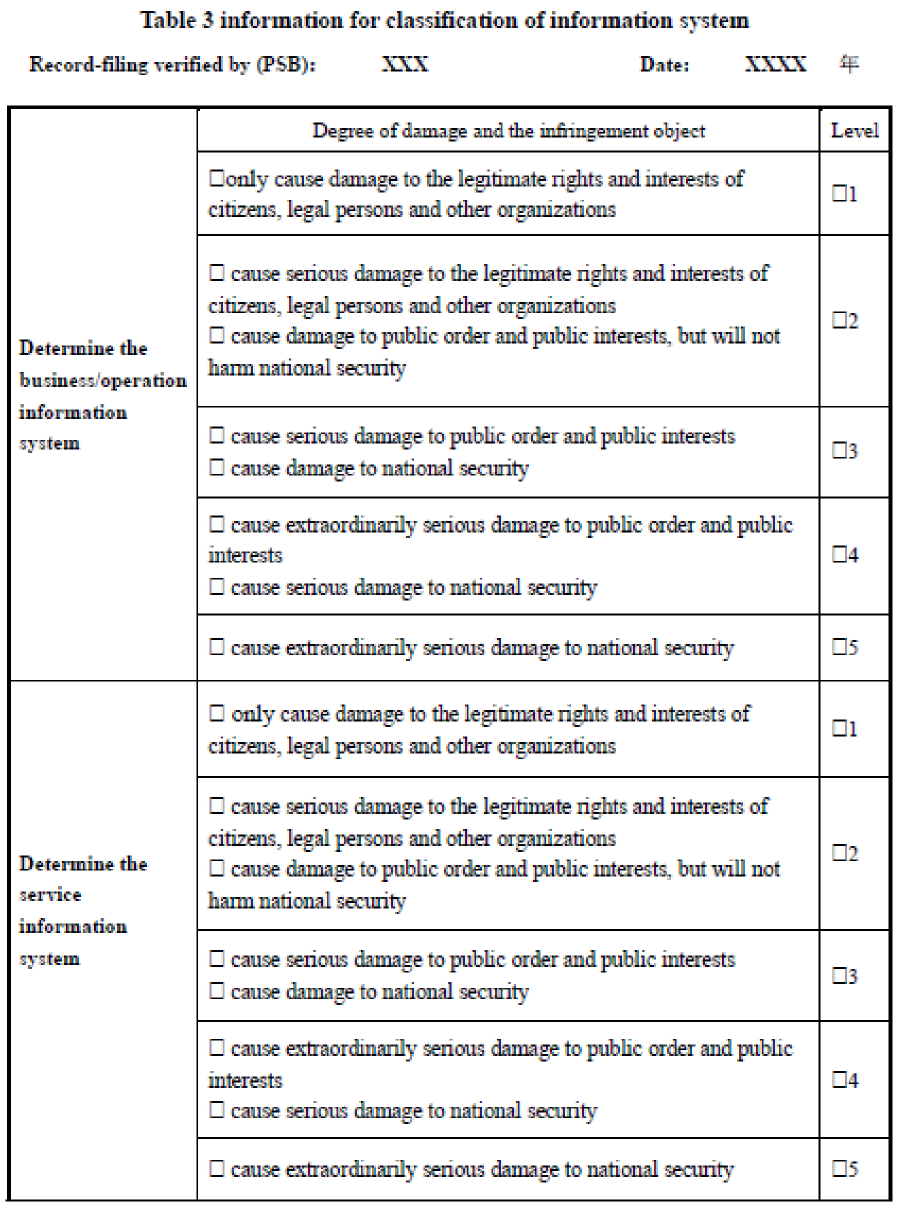


Table 3 information for classification of information system

Record-filing verified by (PSB): XXX **Date:** XXXX 年

	Degree of damage and the infringement object	Level
Determine the business/operation information system	☐only cause damage to the legitimate rights and interests of citizens, legal persons and other organizations	☐1
	☐ cause serious damage to the legitimate rights and interests of citizens, legal persons and other organizations ☐ cause damage to public order and public interests, but will not harm national security	☐2
	☐ cause serious damage to public order and public interests ☐ cause damage to national security	☐3
	☐ cause extraordinarily serious damage to public order and public interests ☐ cause serious damage to national security	☐4
	☐ cause extraordinarily serious damage to national security	☐5
Determine the service information system	☐ only cause damage to the legitimate rights and interests of citizens, legal persons and other organizations	☐1
	☐ cause serious damage to the legitimate rights and interests of citizens, legal persons and other organizations ☐ cause damage to public order and public interests, but will not harm national security	☐2
	☐ cause serious damage to public order and public interests ☐ cause damage to national security	☐3
	☐ cause extraordinarily serious damage to public order and public interests ☐ cause serious damage to national security	☐4
	☐ cause extraordinarily serious damage to national security	☐5

15. Regulatory considerations during reporting

SELF ASSEMENT / REPORTING

Main principles of the reporting for self assessment

Form to be filled in by the tier-2 or higher "recording-filing organization".

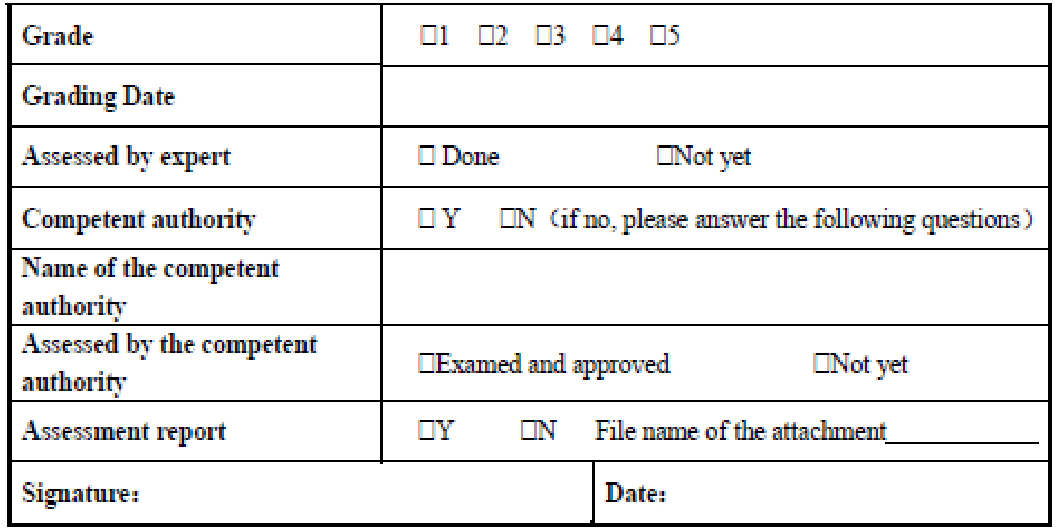
Table 1: Information for organizations

Table : Basic information for information system

Table 3: Information for classification of information system

Table 2 and Table 3 shall be filled by each information system.
The content that needs to be submitted by tier-3 or higher system shall be filled in Table 4.

Form to be submitted to the PSB or specific authorities (MIIT?) = public security organs that accept record-filing after the completion of system construction, rectification and evaluation, etc.



Grade	□1 □2 □3 □4 □5
Grading Date	
Assessed by expert	□ Done □Not yet
Competent authority	□ Y □N（if no, please answer the following questions）
Name of the competent authority	
Assessed by the competent authority	□Examed and approved □Not yet
Assessment report	□Y □N File name of the attachment___________
Signature:	Date:

16. Regulatory considerations during reporting

SELF ASSEMENT / REPORTING

Main principles of the reporting for self assessment

Form to be filled in by the tier-2 or higher "recording-filing organization".

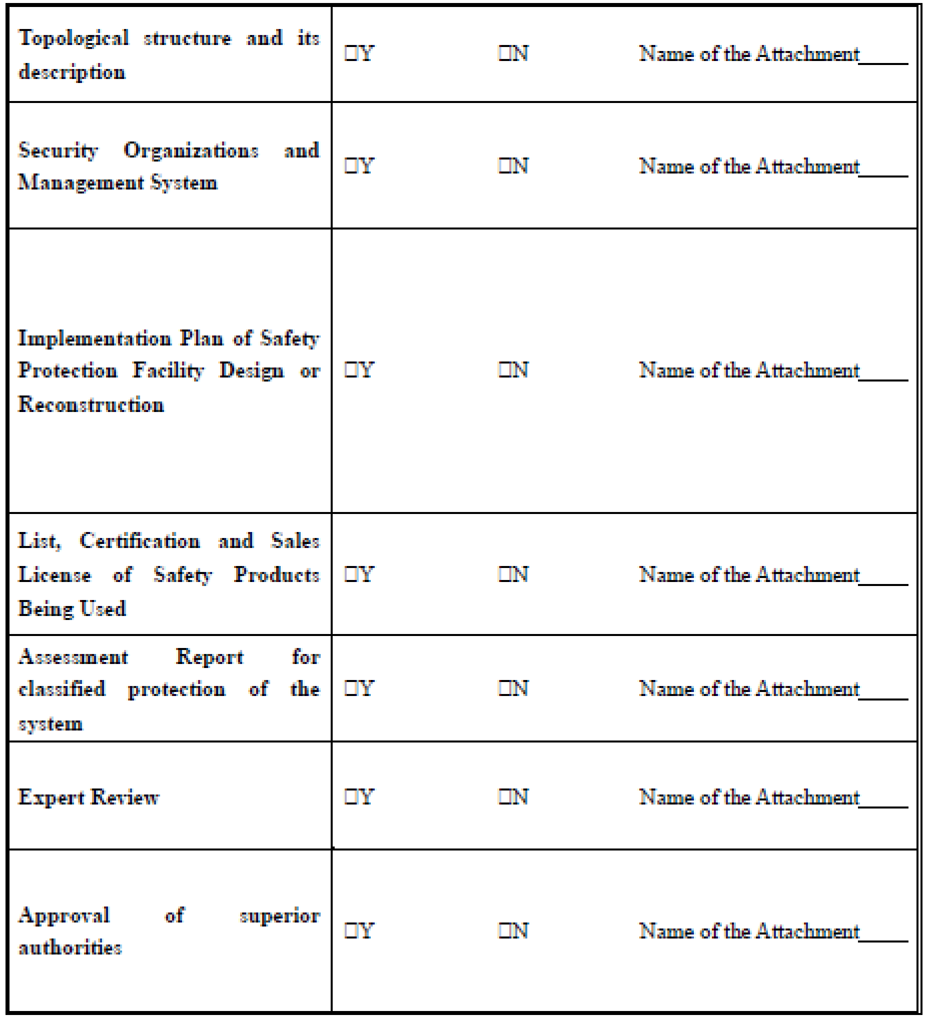
Table 1: Information for organizations

Table : Basic information for information system

Table 3: Information for classification of information system

Table 2 and Table 3 shall be filled by each information system.
The content that needs to be submitted by tier-3 or higher system shall be filled in Table 4.

Form to be submitted to the PSB or specific authorities (MIIT?) = public security organs that accept record-filing after the completion of system construction, rectification and evaluation, etc.



Topological structure and its description	□Y	□N	Name of the Attachment____
Security Organizations and Management System	□Y	□N	Name of the Attachment____
Implementation Plan of Safety Protection Facility Design or Reconstruction	□Y	□N	Name of the Attachment____
List, Certification and Sales License of Safety Products Being Used	□Y	□N	Name of the Attachment____
Assessment Report for classified protection of the system	□Y	□N	Name of the Attachment____
Expert Review	□Y	□N	Name of the Attachment____
Approval of superior authorities	□Y	□N	Name of the Attachment____

17. General considerations and regulators expectations

1. CSL are transversal matters / generates conflict of interests.

- ➢ Difficult to have a process and methodology
- ➢ Difficult for companies to define the proper level of management to involve
- ➢ Can you deal with these complexities without external assistance?

2. China wants to create a cyberspace

- ➢ Safe
- ➢ Controlled

3. New model different from GDPR

- ➢ Holistic approach not only related to data as it includes the infrastructures, systems and organizations safeguards
- ➢ Personal criminal liabilities of the executives and corporate structures

4. Implementation of the control

- ➢ Control in case data breach have started
- ➢ Controls of the implementation of the regulations have started

TL GROUP

CYBER BREACH

CHECKLIST WORKGROUP

20. Checklist workgroup

The first 24hours
TL Group 10 steps check list

01. Acknowledge and accept the cyber incident

02. Mobilize the incident response team

03. Secure systems and ensure containment

04. Ensure business continuity

05. Bring in forensic firms to conduct a thorough investigation and document everything

06. Manage relations (including public and internal)

07. Address legal and regulatory requirements

08. Mitigate liability

09. Notify law enforcement if needed

10. Review protocols and define learnings

TL GROUP

Y/OUR SPEAKERS

In China since sept **2004**.

Founder of Leaf, a law firm based in Shanghai.

Practicing cross-border M&A and PE for **tech companies** in China.

Involved in several **crisis and investigations from authorities**.

Co-founder of TL Group, in alliance with TEKID, to create a team of **Tech and Legal** experts

Bruno Grangier

LEAF Founder
b.grangier@leaf-legal.com
(+86) 136 6182 8004

BAR ADMISSIONS

- Paris Bar
- Foreign-Registered Lawyer in China

MEMBERSHIP

- CCIFC
- EO
- BenCham

QUALIFICATIONS

- LL.M in compared Chinese Law
- Business & corporate law DJCE

LANGUAGES

- French
- English

Maxime came to Shanghai after JW & Associates won the security contest organized by the Shanghai Science and Technology Institute. He was in charge of adapting the organization structure to a worldwide market, globalizing and improving internal processes, integrating and issuing new regulations, market and strategic analysis to provide forecast and put forward a new direction for the company.

Alongside his professional duties, Maxime is also officiating at the International Association for Privacy Professional (IAPP) as Shanghai Chapter co-chairman. He is also an active ICT Working group member of the European Chamber of Commerce in China (EUCCC) where he attends seminars, working meetings, and is involved in EUCCC position paper reviewing activities.

Maxime OLIVA

TEKID CEO
maxime.oliva@tek-id.com

EDUCATION

- Master in IT Project Management

MEMBERSHIP

- EUCCC ICT Group
- IAPP Shanghai chapter co chairman

EXPERTISES

- PMP
- ITIL V3
- Microsoft expert certificates

LANGUAGES

- French
- English