



31
st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Standards for Privacy Protection

DSCI approach

Kamlesh Bajaj
CEO

Data Security Council of India

Int'l Conference of Privacy Commissioners

Madrid, 4 – 6 November, 2009

PRIVACY:
TODAY IS
TOMORROW



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Agenda

1 Standards for Privacy Protection- DSCI Approach

- Proposal for International Standards- DSCI's understanding
- Clarification required
- Best Practices as route to data protection
- BCR for service providers
- Clear and simple rules

2 DSCI as a SRO for Data Protection

- Outsourcing a real risk, but manageable
- DSCI approach to self regulation
- DSCI as a SRO
- IT Act (Amendment) 2008
- DSCI Framework
- SRO Roadmap

PRIVACY:
TODAY IS
TOMORROW



31

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

AEPD WG Objectives

AEPD WG Objective

- Clarify the role of document
- Review controller/processor notions
- Review filing system
- Reduce bureaucratic requirements
- Set accountability principles
- Adapt concept of sensitive data
- Promote international data transfers, if recipient offers an adequate level of data protection
- Inform individuals of security breaches
- Broaden supervisory authority concept
- Enhance international cooperation
- Encourage proactive measures
- Analyse relevant law



DSCI Welcomes

Clarity of rules and standards on

- *Outsourcing,*
- *International data transfers,*
- *Role of self-regulatory organizations*

TODAY'S
TOMORROW



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Outsourcing and International Data Transfers

– *our understanding*

Outsourcing an organizational decision so..



Openness principle; Consent of data subjects is not applicable to international data transfers

Para 14 Explanatory note: Data transfer to States where establishment of a level of privacy protection similar to that of these standards, are not respected



These guarantees might be offered by that recipient by virtue of agreements entered into with the transmitter of the information, or through binding corporate rules



Extend BCRs to Service Providers

Clarification required

..... Improvements in the Standards – but clarifications necessary

Role of supervisory authority

Once a responsible person or entity/independent body verifies that the level of protection by the recipient in the destination State is similar to that in his own State, international transfers should begin.

.... Why should the supervisory authority verify?

Countries with **data protection laws** and/or rules as ensuring an **adequate level of protection** of personal data

*Current system for assessing third countries is too cumbersome and lengthy – it verifies the equivalence of a third country law with the Directive. Even with “similar” data protection instead of “adequate”, supervisory authorities are required to verify that recipient affords data protection. **This should not be the case.***

Para 13 on Provision of services - **supplier guarantee** of a level of protection similar to that in the document

Responsible person or entity/independent body may obtain assurance (for example, an auditor’s report), contractual obligation, or other representation (for example, written annual confirmation)

What would be the new position of supplier organizations based outside EU ?. Will the more generic requirement of “recipient affording a similar level of protection to that one provided in the document” as mentioned in 14.1, ease the cross-border data flows?



31st

Madrid, 4th, 5th and 6th, November 2019
international conference
of data protection
and privacy commissioners

Self-Regulatory Organizations (SROs) – *Role clarification*

Acceptance of self-regulation in the standards

DSCI Welcomes this change

Whether SROs, if responsible for all these programs in a country, and if they fulfill the criteria of impartiality and independence, and enforceability; will be treated at par with statutory regulators by EU?

Provision of service for a claim or complaint may be free to a data subject

SRO should be free to charge a fee for dispute resolution between responsible person or entity and a service provider.

PRIVACY:
TODAY'S
TOMORROW

Whether EU would accept online dispute resolution (ODR) mechanism, if implemented by SRO?



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Best Practices approach - *as a route to data security*

Global data flows are the norm

Multinationals operating across the globe transfer data of their customers, suppliers, employees including their personal data

Social networking sites like Myspace, Facebook, Orkut

Personal data of all signed-up users stored in any of their data centres across the globe

SWIFT and IATA members

Retain financial & travel related data of customers, that contains personal data, in their data centres anywhere in the world.

E-commerce transactions, google searches, amazon and ebay purchases

Personal data shared by individuals if they want to avail of the services provided by sites.

Approach to data protection has to be based on a different paradigm. Technology will continue to overwhelm the “adequacy” norm.

..... Best Practices Approach to data protection is the key



31

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

BCR Approach for Service Providers

Extend the concept of BCRs to all service providers

Treat global service providers at par with MNCs ; subject them to the same process of approval as afforded to MNCs

An MNC can implement BCRs to show compliance with the data protection requirements of a country in the EU - irrespective of where it is processed

Best Practices Approach – BCRs - enable a service provider located in a non-EU country such as India to demonstrate compliance with data protection requirements of an EU country where the client is located, and/or where the data is originating.

PRIVACY:
TODAY IS
TOMORROW

Proper protection and privacy should be based on the tenet of best practices, in the form of BCRs, followed by service providers.

..... Focus should be global rather than provincial



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Accountability Principle

– *providing business with clear and simple rules*

APEC Approach

EU may consider this as a route to ensure consumer trust and business confidence in cross-border data flows

Preventing harm' approach

Emphasize best practices and international standards in cross-border data flows, rather than the process-oriented approach of the Directive to approve standard contractual clauses, BCRs, or other similar instruments by supervisory authorities.

Accountability Principle. Will help reduce bureaucratic controls



31

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Outsourcing offshore is a real risk but manageable

Secure Outsourcing operations

- ❑ Use of best practices and standards for managing security
- ❑ Control Principles- Scenario based control selection, security requirement translations into controls,
- ❑ Security controls- Employee Background check, Hardened desktop- SOE, Secured communication channels, Infrastructure security- Layered defense, Physical security, Logical access control, Data Security, Security Officers, DR /BCP
- ❑ Establishment of Assurance mechanisms- Security coordination, Risk Management framework, Security Processes, Security Assessment, Security monitoring & reporting and Incident Management
- ❑ Dedicated standards for building and operating outsourcing locations- Outsourced Delivery Centres [ODC]
- ❑ Compliance support processes- Active compliance support, compliance reporting

DSCI - Data Security & Privacy protection

Outsourcing

Objective

Low-cost resources
Quality & diversity
Scale up & expanding

Consistent data security
Security at Affordable cost
Privacy for customer confidence



Establishment of rules & standards
Promote ethics, quality and best practices



Self-Regulation:

Adoption of best global practices

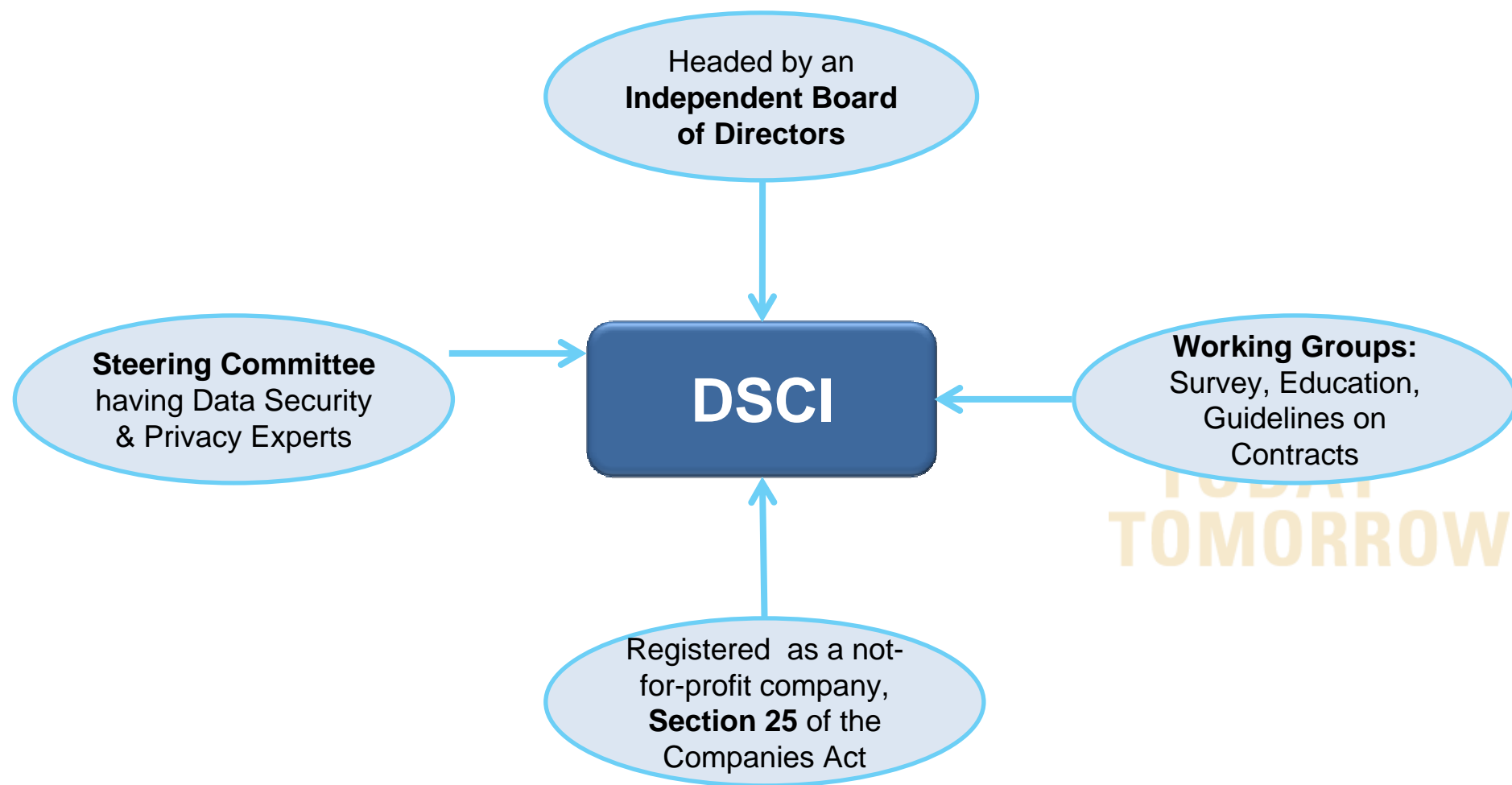
Independent Oversight:

Focused Mission:

Enforcement Mechanism:

As an increasing number of organizations take the decision to send more and more mission critical work offshore, **Security best practices and following some tactical steps** may help to address security issues in global sourcing... *Gartner's Outsourcing & IT Services Summit, 2007*

DSCI Structure



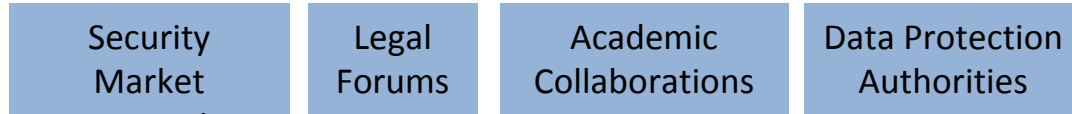
TODAY
TOMORROW



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

DSCI Approach to Self Regulation



Research

Knowledge Collaboration

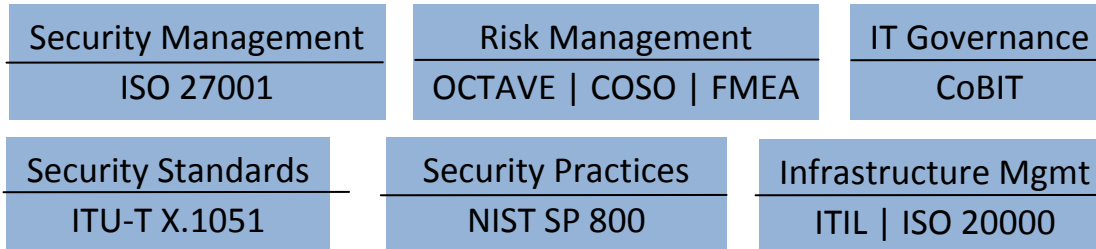
DSCI- A Self Regulatory Org.
 Data Protection
 Best Practices
 Capacity building
 Independent oversight
 Enforcement
 Dispute Resolution
 Cyber Crime Speedier trial

Legal & Regulatory Requirements

Technology and Vendor interactions



Industry best practices





31st

Madrid, 4th, 5th and 6th, November 2019
international conference
of data protection
and privacy commissioners

DSCI Stakeholders

Board of Directors

- NASSCOM representation
- Independent directors
- Eminent Academician

Steering Committee

- Senior security & privacy professionals
- IT/ITES, BFSI Co.
- Client companies, Captive BPO, MNC, Foreign Banks

Working Groups

- Education
- Contract guidelines
- Survey
- Business Model
- Physical Security & BC

DSCI Chapters

- Bangalore, Delhi, Mumbai
- Pune, Kolkatta, Hyderabad, Chennai, Chandigarh
- Will connect to 300 to 500 security professionals from industry

IT/ ITES Industry

- As a NASSCOM members

Other Industry

- Banks, Financial Institutes, Telecom

Legal & Regulatory Authorities

- Data Protection Auth.
- EC
- FTC

Government of India

- CERT-In
- DIT

Sub working groups

- Content vetting

Client

- Big ticket outsourcers

Security Professionals

- Independent security professionals

DSCI as a SRO



ESCALATION

DSCI

DISPUTE RESOLUTION

DSCI Certification

AUDITOR

SELF CHECKS

IT and BPO Companies

FEEDBACK

Standards / Best Practices

Awareness Creation

- Data Security
- Data Privacy
-
- IT/BPO Companies
- Law-Enforcement

- Education
- Training
- Surveys
- Guidelines for Contracts

1

COMPLAINTS



CLIENTS

4

3

2



31

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

IT Act (Amendment) 2008

Sections 43A and 72A

- **Section 43 modified:** The existing Act provides for penalty for damage to computers, computer systems under the title 'Penalty and Adjudication' in section 43 that is widely interpreted as a clause to provide data protection in the country- This section has been **"improved"** to include stealing of **"computer source code"** for which compensation can be claimed. (Computer source has been defined)
- **New Section 43A:** Data protection has now been made more explicit through insertion of a new clause 43A that provides for **"compensation to an aggrieved person"** whose personal data including sensitive personal data may be compromised by a company, during the time it was under processing with the company, for failure to protect such data whether because of negligence in implementing or maintaining reasonable security practices
- **Penalty for breach of confidentiality and privacy:** 72A- punishment for disclosure of information in breach of a lawful contract is prescribed

Improvement to include **"stealing of computer source code"**

Data Protection- explicit new clause 43 A - **"Compensation to an aggrieved person"** whose personal data including **"sensitive personal data"** may be compromised by a company

Compromised because of **"negligence in implementing or maintaining reasonable security practices"**

72 A- Punishment for **"disclosure of information in breach of a lawful contract"**

"Disclosure without the consent" of the subject person **"will constitute a breach"**



31st

Mumbai, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

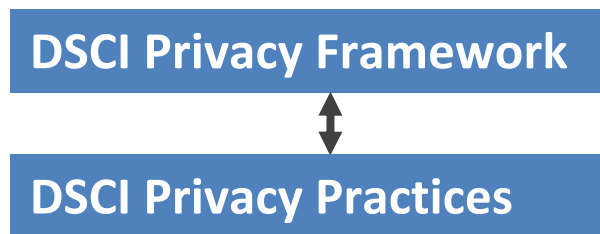
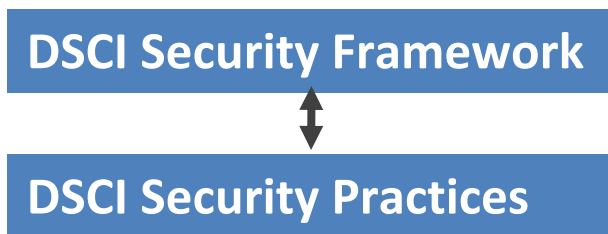
IT Act (Amendment) 2008 – Sections 43A and 72A

The need for data protection was reinforced with the notification of the IT (Amendment) Act, 2008

Service providers in India will be required to implement “**reasonable security practices**” to prevent unauthorized access to personal data of customers being processed by them



PRIVACY:
TODAY IS
TOMORROW





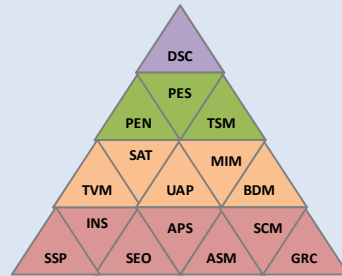
31st

Madrid, 4th, 5th and 6th, November 2019
international conference
of data protection
and privacy commissioners

DSCI- Data Protection Practices

DSCI Security Framework

DSCI Security Practices



DSCI Security Framework (DSF©)

16 Best Practices area

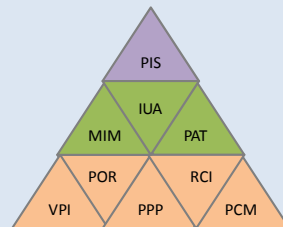
Based on the ISO 27001

Draws upon the tactical recommendations

Takes note of new approaches, technology and tactical mechanisms evolved

DSCI Privacy Framework

DSCI Privacy Practices



DSCI Privacy Framework (DPF©)

9 Best Practices and 12 Privacy Principles

Privacy Policy Guidelines

Privacy Impact Assessment

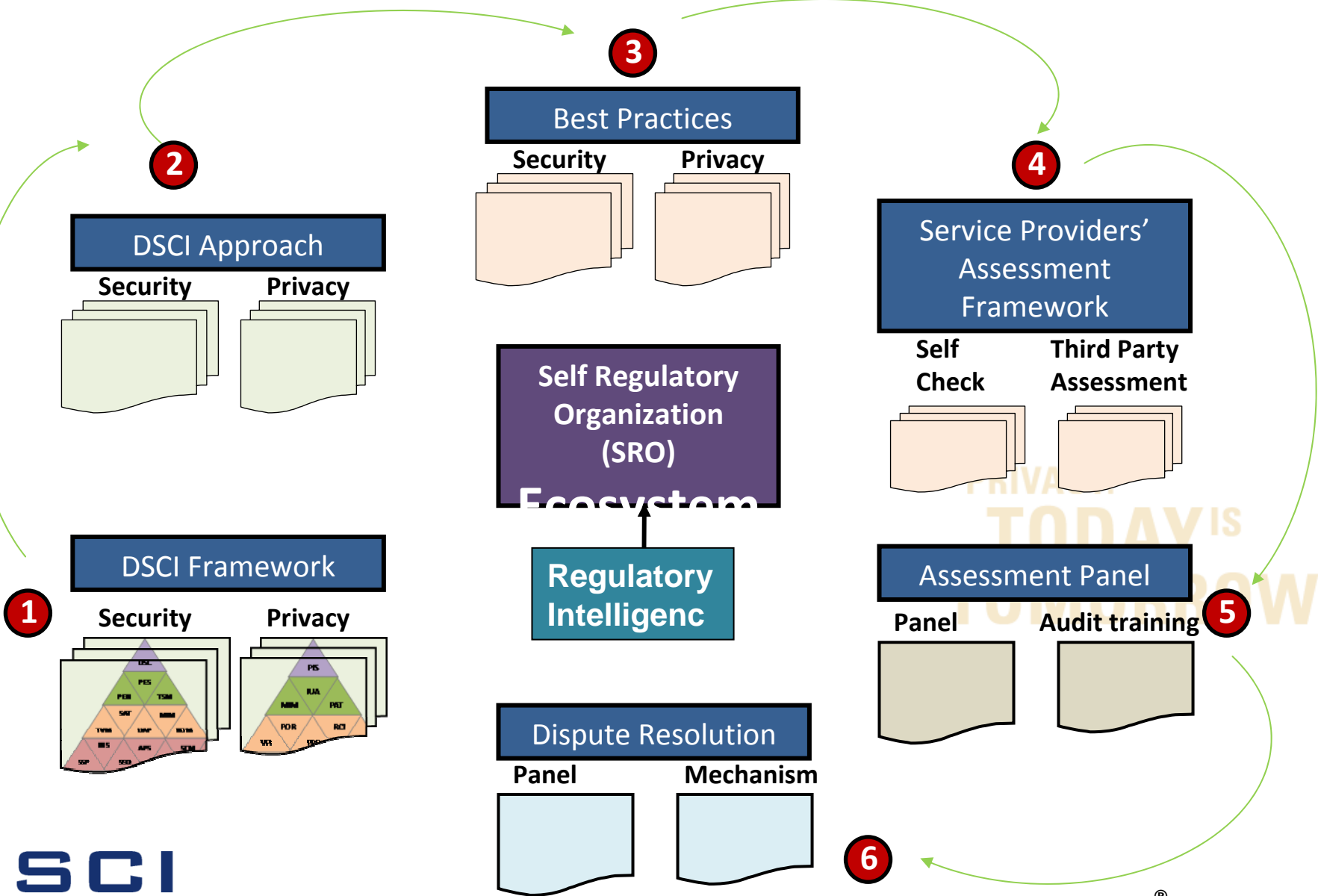
PRIVACY:
TODAY IS
TOMORROW



31st

Madrid, 4th, 5th and 6th, November 2013
international conference
of data protection
and privacy commissioners

SRO Roadmap





31
st

Madrid, 4th, 5th and 6th, November 2009

international conference
of data protection
and privacy commissioners

Thank You

PRIVACY:
TODAY IS
TOMORROW