Risk-Based Approach in Cyber Security

International ICT Conference 2018

Sustainable Development Goals for Smart society

Kathmandu, Nepal

June 17-18, 2018

Pramod Parajuli

IT Consultant and Risk Specialist

Datum Systems Pvt. Ltd.

pramod@datum.com.np

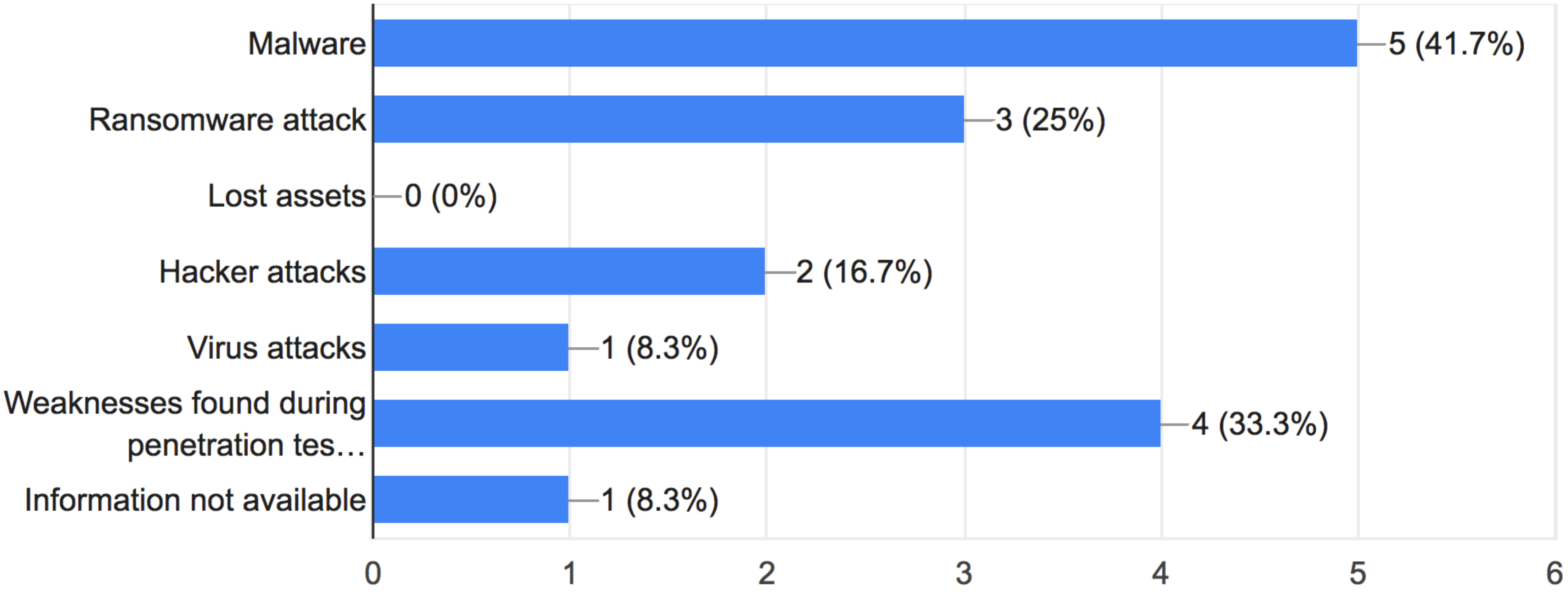
AGENDA

- Summary of a quick survey on cyber security
- Why compliance and frameworks are not sufficient?
- Risk-Based Approach
    - Types of risks
    - Scientific risk analysis
- C2M2

A quick survey on cyber security in Nepali organizations (Survey summary of Nepal, 2018 compared with Deloitte. Survey Summary, 2014)

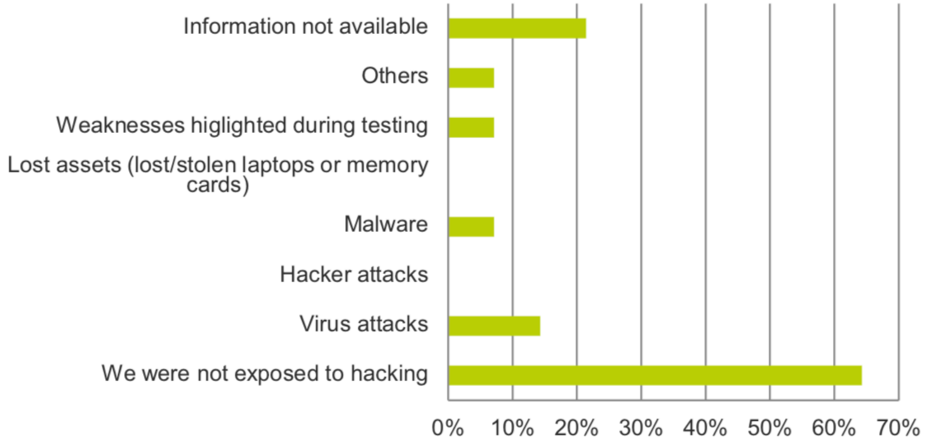
Have you suffered any cyber-security breach in the last 12 months?

12 responses



Source: *Cyber Security in Nepali Organizations - Survey*, npCert, 2018

Question 1: Have you suffered a breach in the last 12 months (multiple answers possible)?

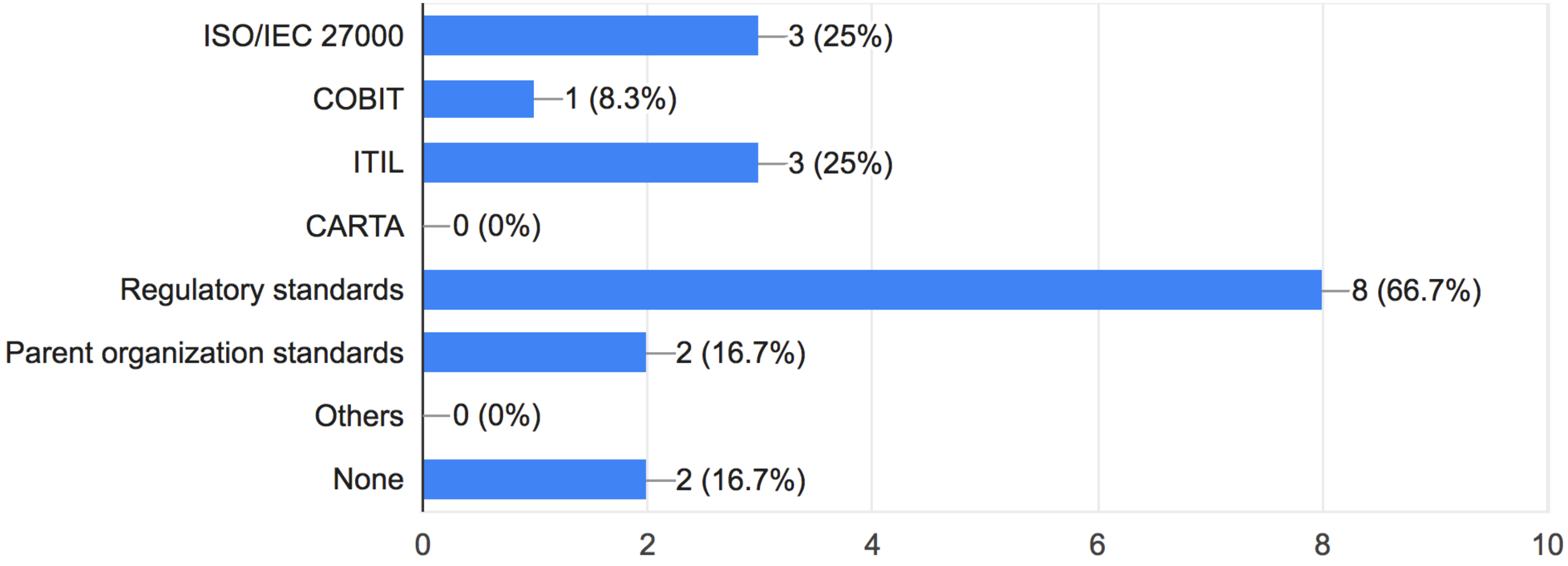


The majority of companies have not been exposed to cybersecurity incidents. However, evidence is insufficient as to whether this is reality or merely perception.

Source: *Central Asian Information Security Survey Results*, Deloittee, 2015

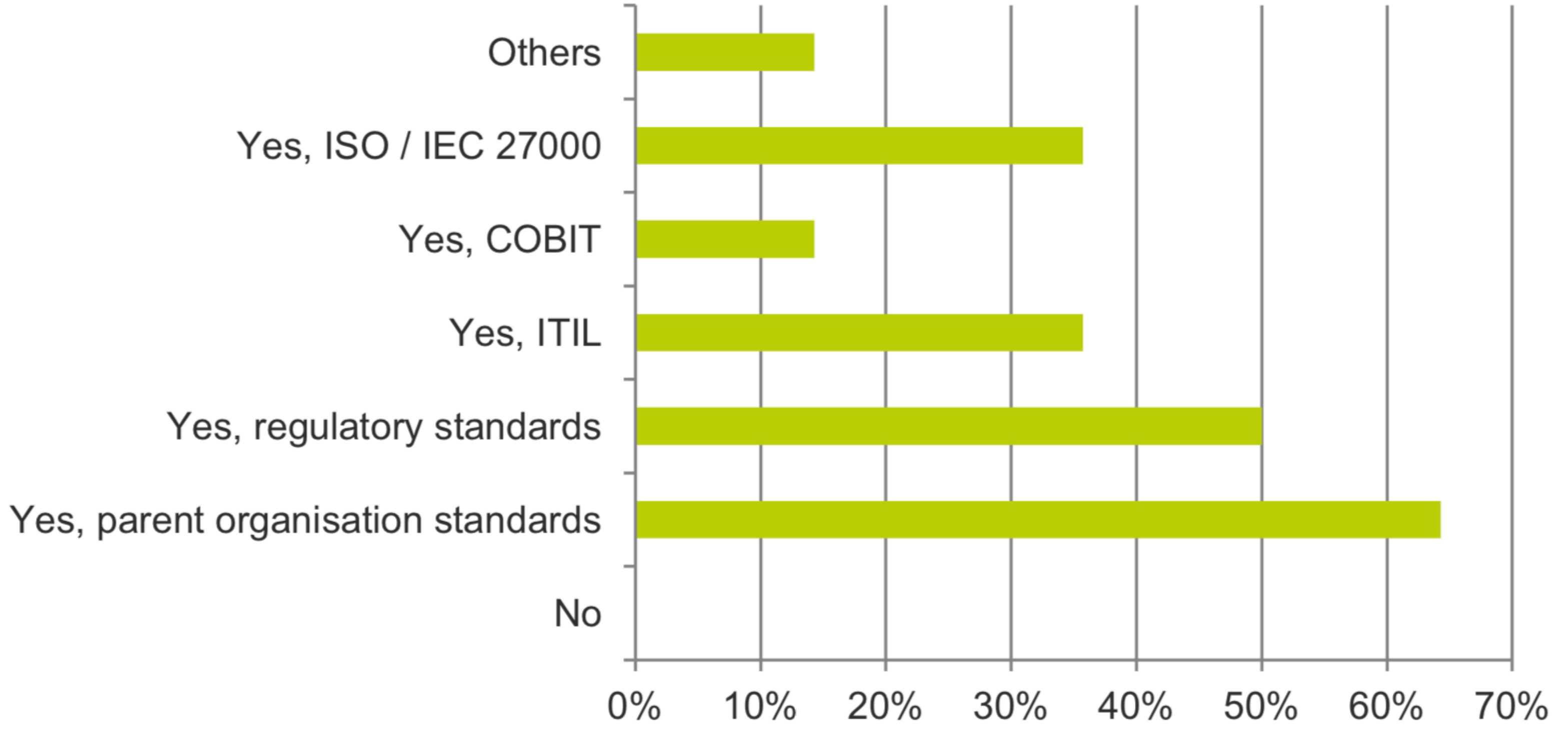
What security frameworks and/or standards your IT department has adopted?

12 responses



Source: *Cyber Security in Nepali Organizations - Survey*, npCert, 2018

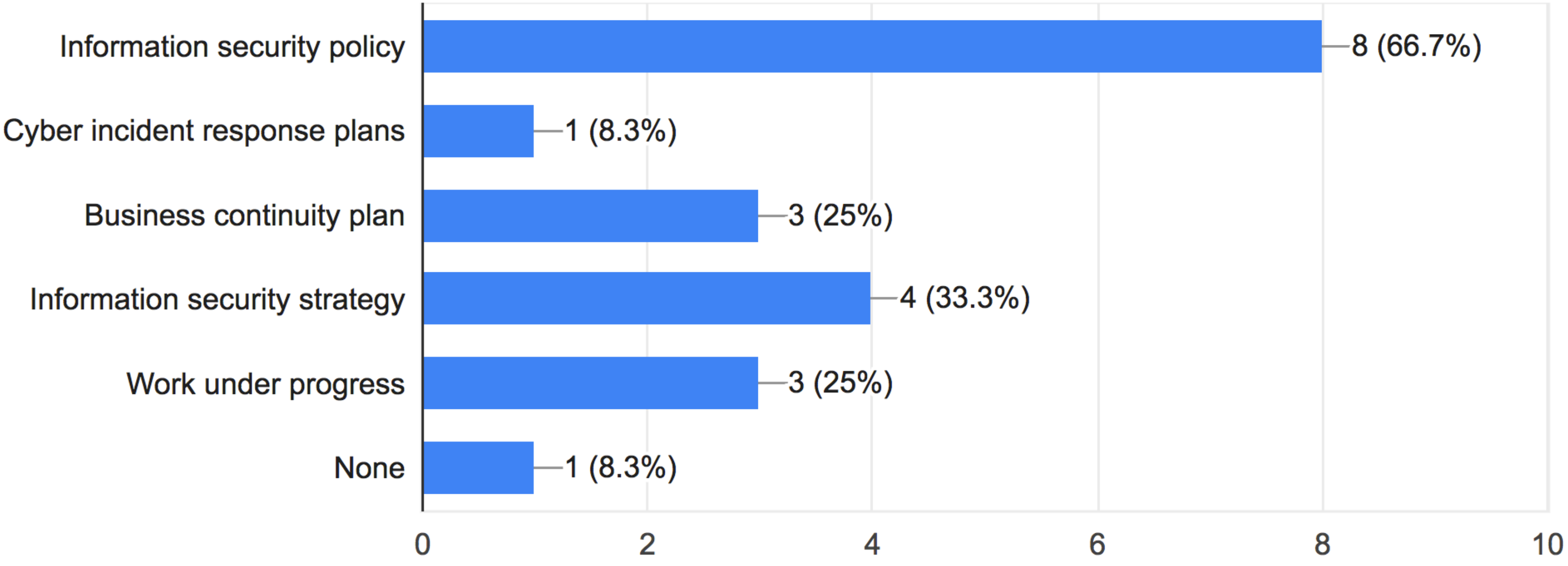
Question 4: Does your organisation adhere to IT process or security frameworks and/or standards, and if so, which ones (multiple answers possible)?



Source: *Central Asian Information Security Survey Results*, Deloittee, 2015

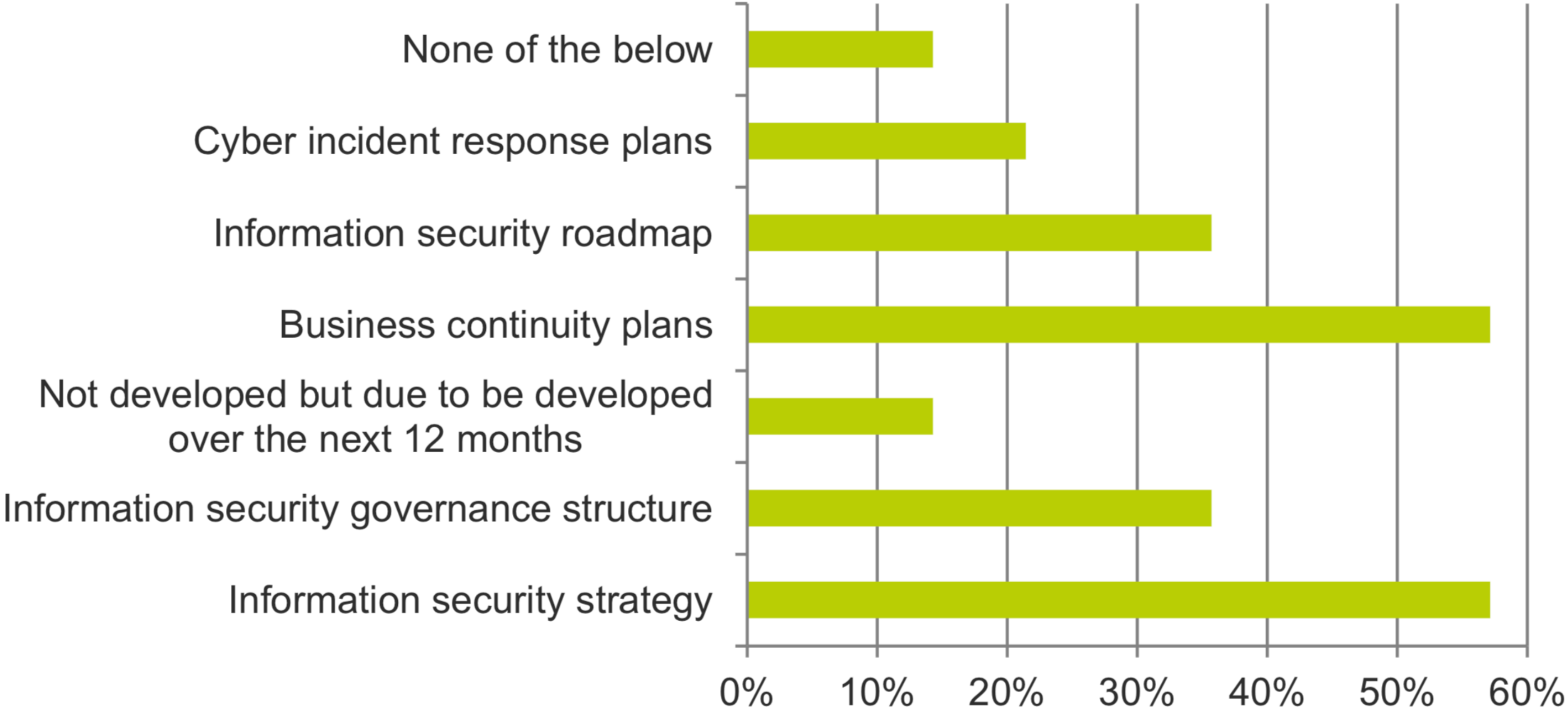
Which of the following policies/procedures are documented in your organization and in effect?

12 responses



Source: *Cyber Security in Nepali Organizations - Survey*, npCert, 2018

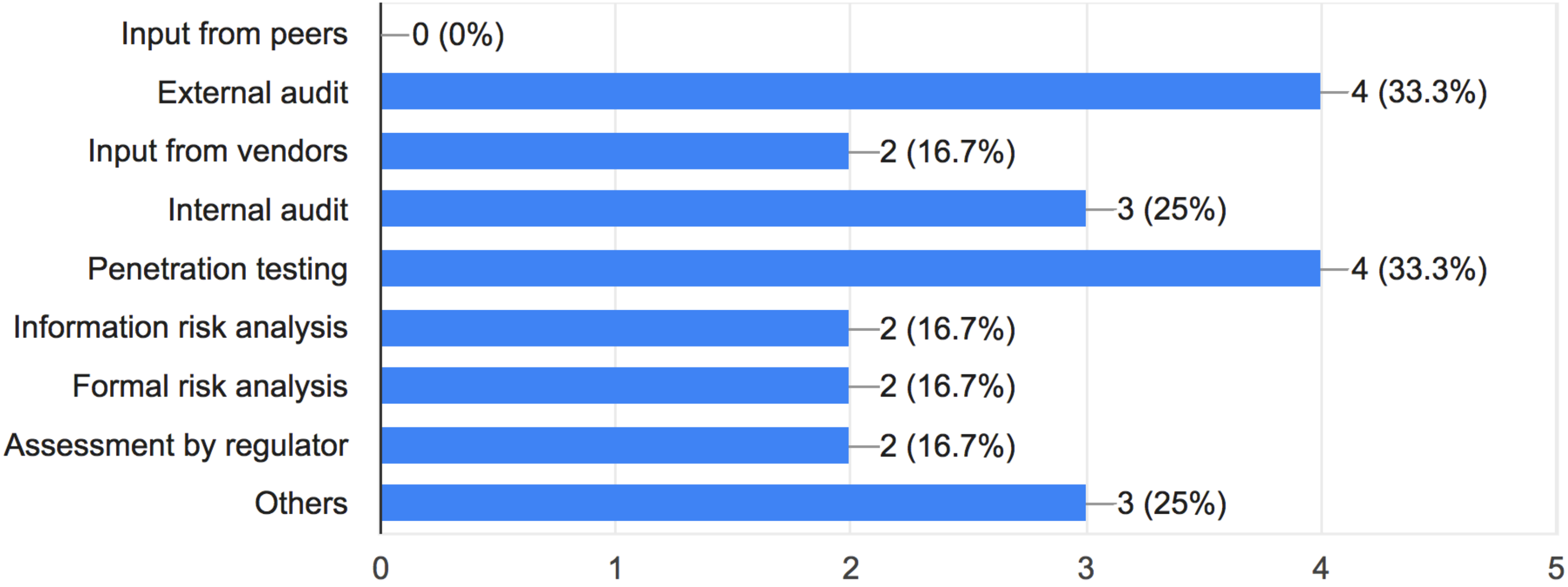
Question 6: Which of the following (policies / procedures) has your organisation documented and approved (multiple answers possible)?



Source: *Central Asian Information Security Survey Results*, Deloittee, 2015

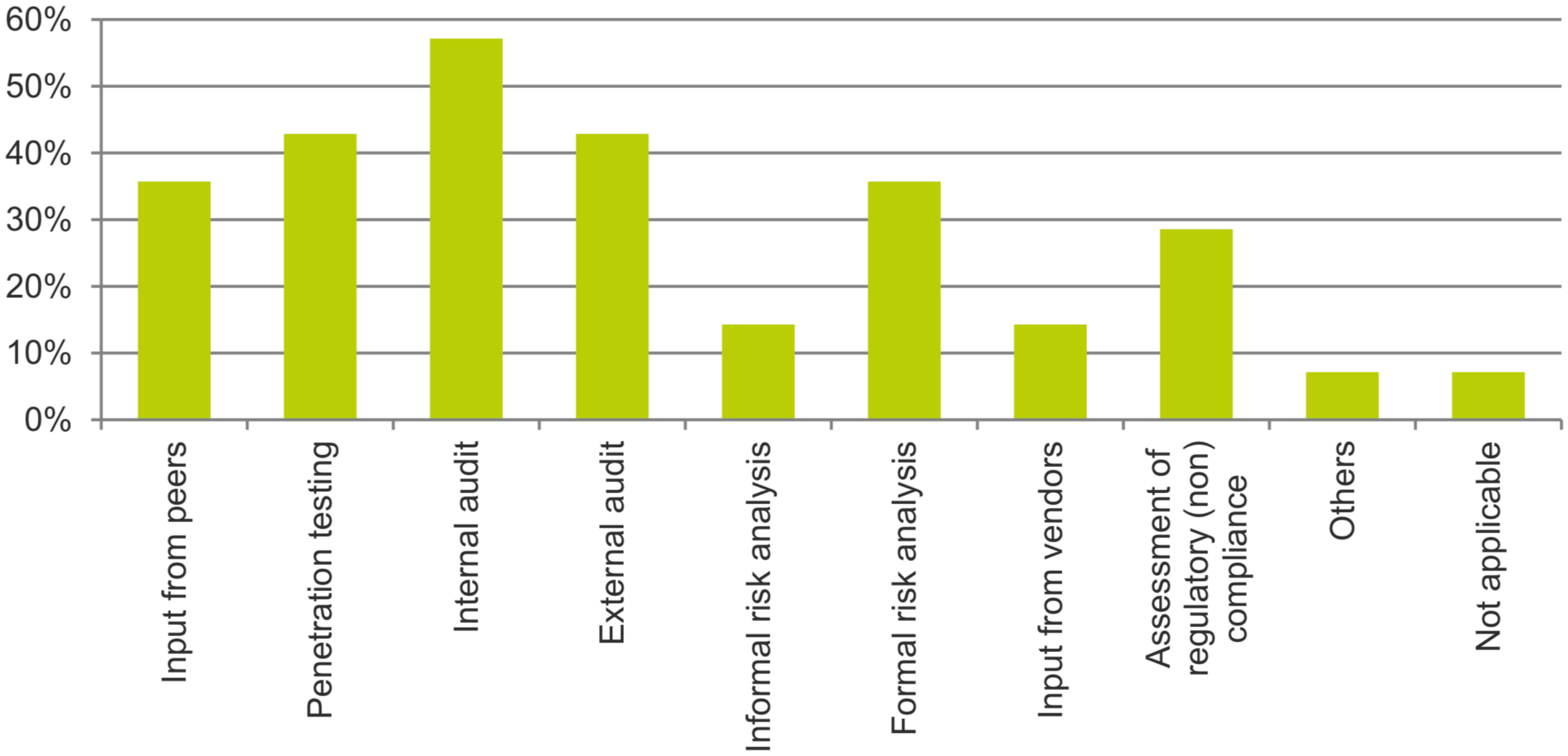
How do you highlight information security weaknesses, risks, and non-compliance in your organization?

12 responses



Source: *Cyber Security in Nepali Organizations - Survey*, npCert, 2018

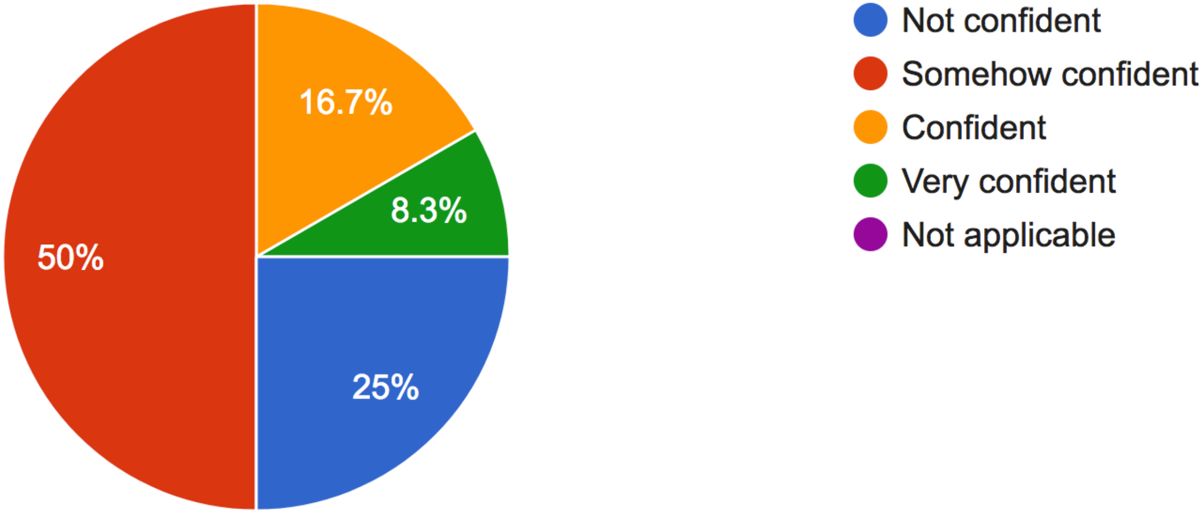
Question 25: How do you highlight information security weaknesses, risks and non-compliance in your organisation (multiple answers possible)?



Source: *Central Asian Information Security Survey Results*, Deloittee, 2015

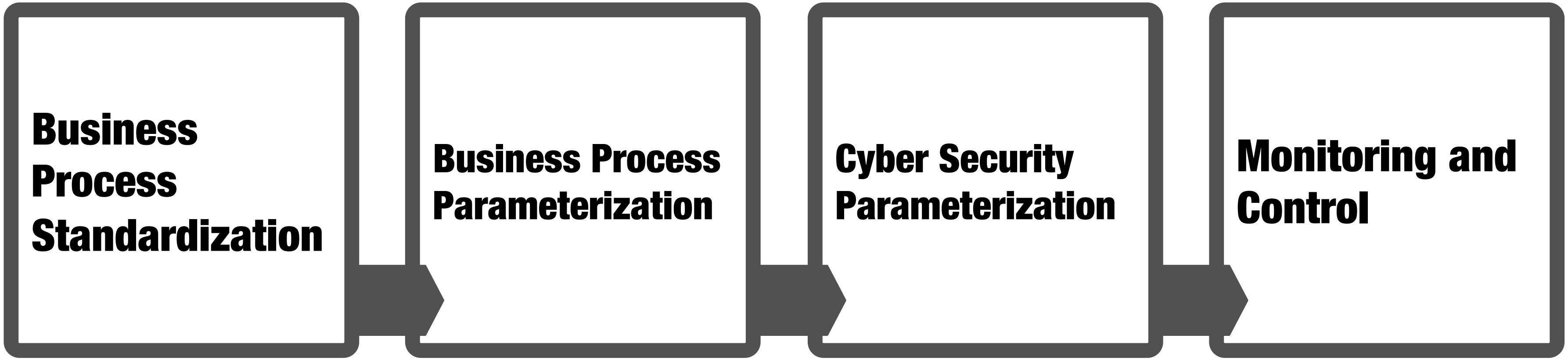
How confident are you in information security practices of your third parties?

12 responses



Source: *Cyber Security in Nepali Organizations - Survey*, npCert, 2018

CYBER SECURITY AND BUSINESS PROCESS



Business Process Standardization

Business Process Parameterization

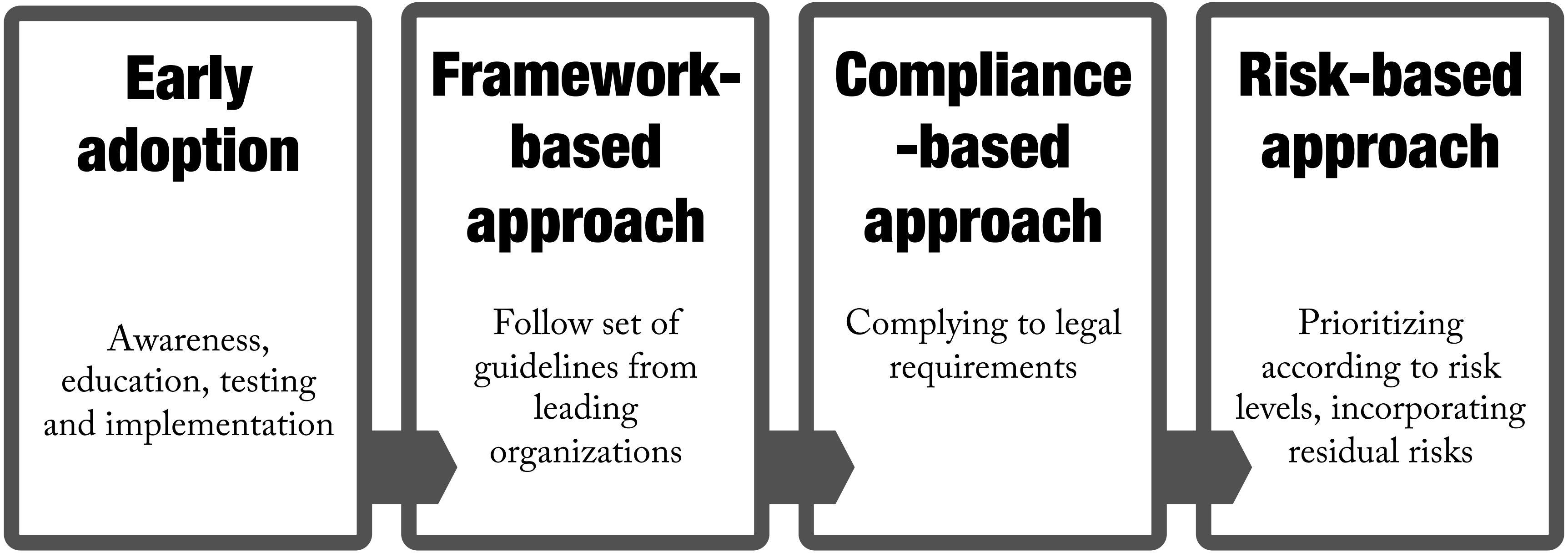
Cyber Security Parameterization

Monitoring and Control

And yet, attacks are happening!

New threats, sophisticated tools, dynamic workflows, complexity of systems, complexity of services and containers, human elements, cost-based approach!

EVOLUTION



Early adoption

Awareness, education, testing and implementation

Framework-based approach

Follow set of guidelines from leading organizations

Compliance-based approach

Complying to legal requirements

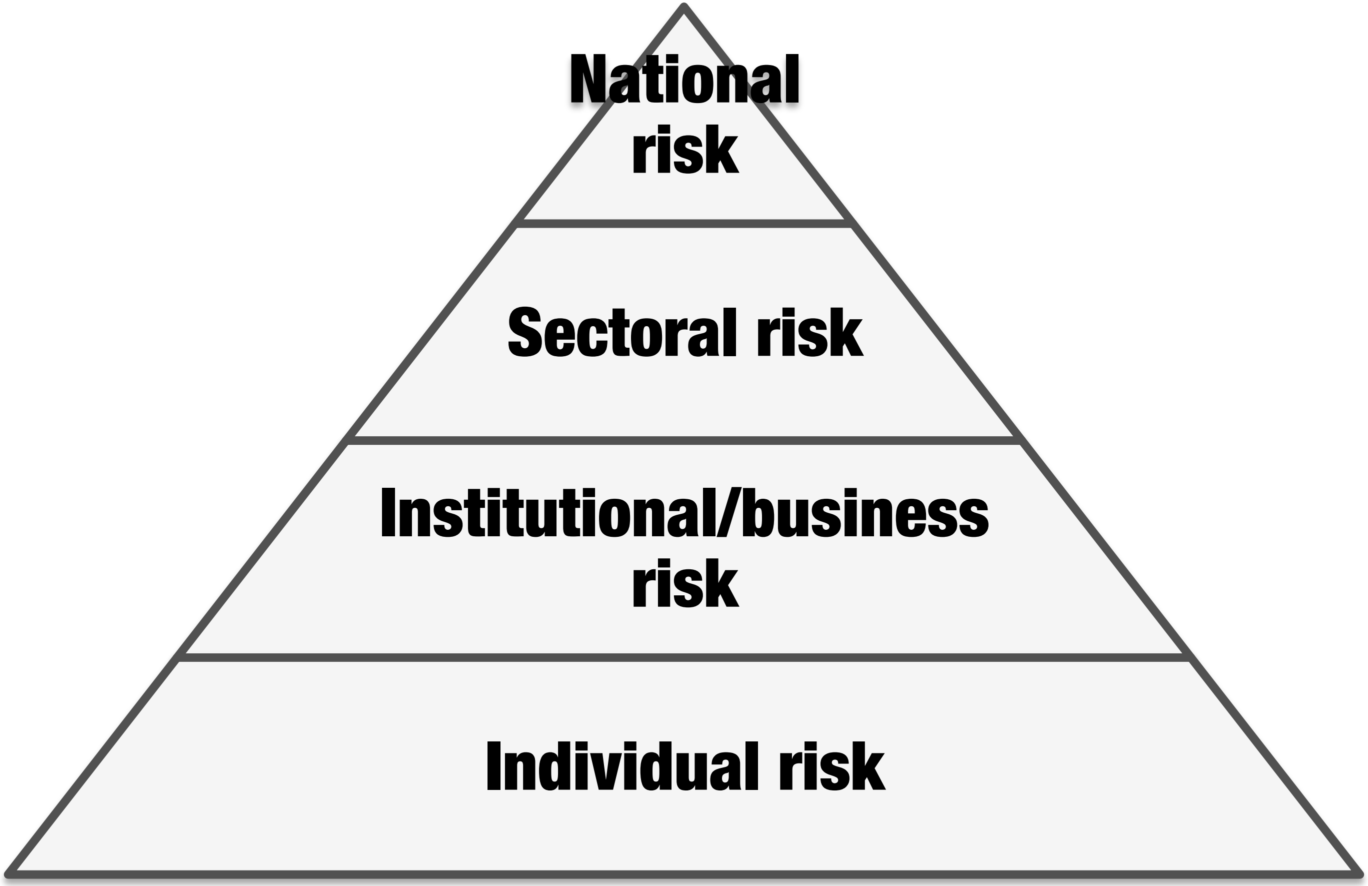
Risk-based approach

Prioritizing according to risk levels, incorporating residual risks

RISKS

- Information not available to right person/entity in right time.
- Service not available to right person/entity in right time.
- Difficulty in meeting business-level QoS assurance.
- Non-compliance.

IMPACT OF RISKS



National risk

Sectoral risk

Institutional/business risk

Individual risk

TYPES OF RISKS

- **Inherent risks** - can be expected to occur, their impact can be estimated and assigned to particular event.
- **Residual risks** – are amount of risk left after inherent risks has been reduced by applying risk measures and controls.

$$residual\ risk = inherent\ risk - impact\ of\ risk\ controls$$

RISK-BASED APPROACH (RBA)

- Scientific risk analysis of
  - people,
  - products,
  - processes, and
  - systems.
- For **higher level risks**, take **enhanced measures** to manage and mitigate those risks.
- For **lower level risks, simplified measures** may be permitted.
- However, lower level of risks can not be exempted!

ORAGNIZATIONS NEED TO MANAGE RISKS RELATED TO

People

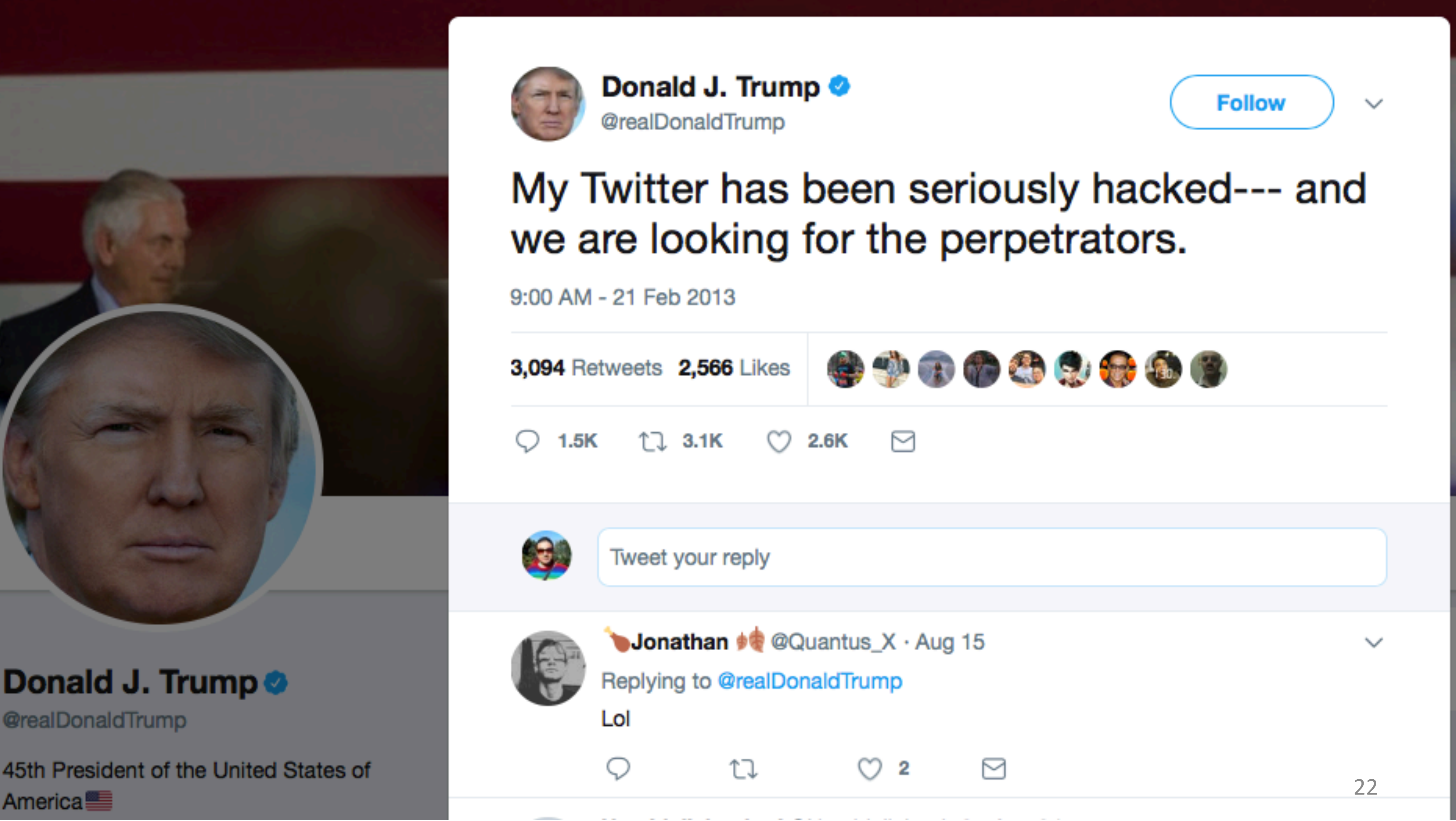
Products

Processes

Systems

PEOPLE

- Customers
- Customer associates
- Customer’s customers
- Vendors, contractors, sub-contractors
- Employees!



Donald J. Trump
@realDonaldTrump

Follow

My Twitter has been seriously hacked--- and we are looking for the perpetrators.

9:00 AM - 21 Feb 2013

3,094 Retweets 2,566 Likes

🍗Jonathan 🍂 @Quantus_X · Aug 15
Replying to @realDonaldTrump
Lol

Donald J. Trump
@realDonaldTrump

45th President of the United States of America

PRODUCTS

- The instruments that carry value and that allow exchange of value (bills, cards, crypto currency…).
- Value exchange services (transfers, withdrawals, deposits, loan, crypto-currency exchange, FOREX, …).
- Value distribution channels (Internet banking, SMS, electronic pay systems, …).

EXAMPLE - Services delivery

- What is at the stake if service is not delivered?
- What will happen if wrong service is delivered?
- What will happen if Quality of Service is compromised?
- Who will be affected?
- How will it affect overall business objectives?

PROCESSES

- Objectives
- Quality standards to achieve
- Business workflow: flow of events
- Reporting workflow
- Roles and responsibilities
- Record keeping standard
- Exceptions and escalation

EXAMPLE - Procurement

- Does the procurement policy compromise quality of product or service that we're procuring/providing?
- Is the vendor able to comply with our security requirements?

RISK ANALYSIS TOOLS

Medium	High	Very high
Low	Medium	High
Very low	Low	Medium

frequency

impact

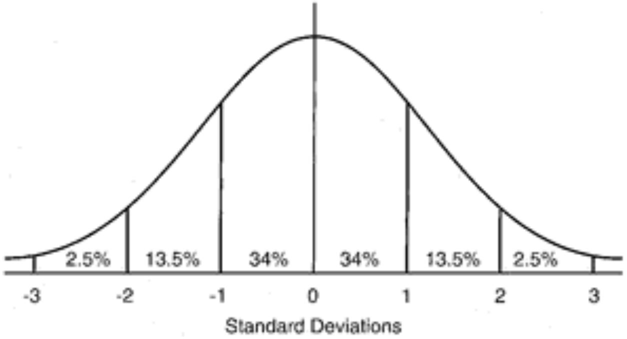
SCIENTIFIC RISK MEASURE

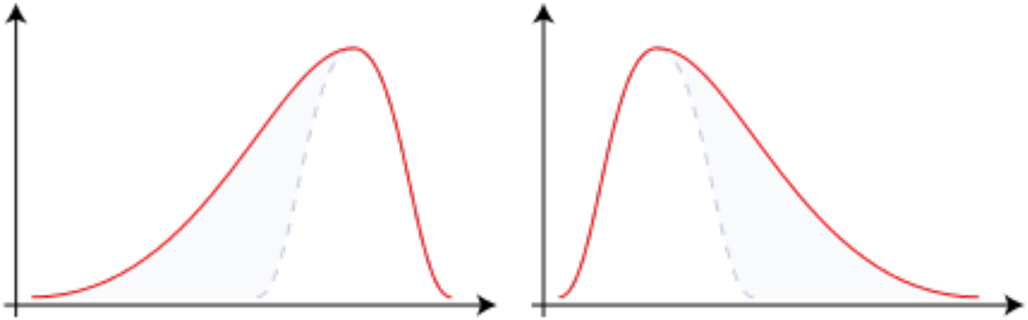
$$Risk = \sum_{s \in C} \left(\max(s) + \sum_{x \in s, x \neq \max(s)} sensitivity\left(\max(s), x\right) \right)$$

$$C = \{risk\ \ category_0,\ risk\ \ category_1, \ldots\ldots\}$$

$$sensitivity(y, x) = \left(y \times \frac{x}{100} \right) \%$$

RISK DISTRIBUTION

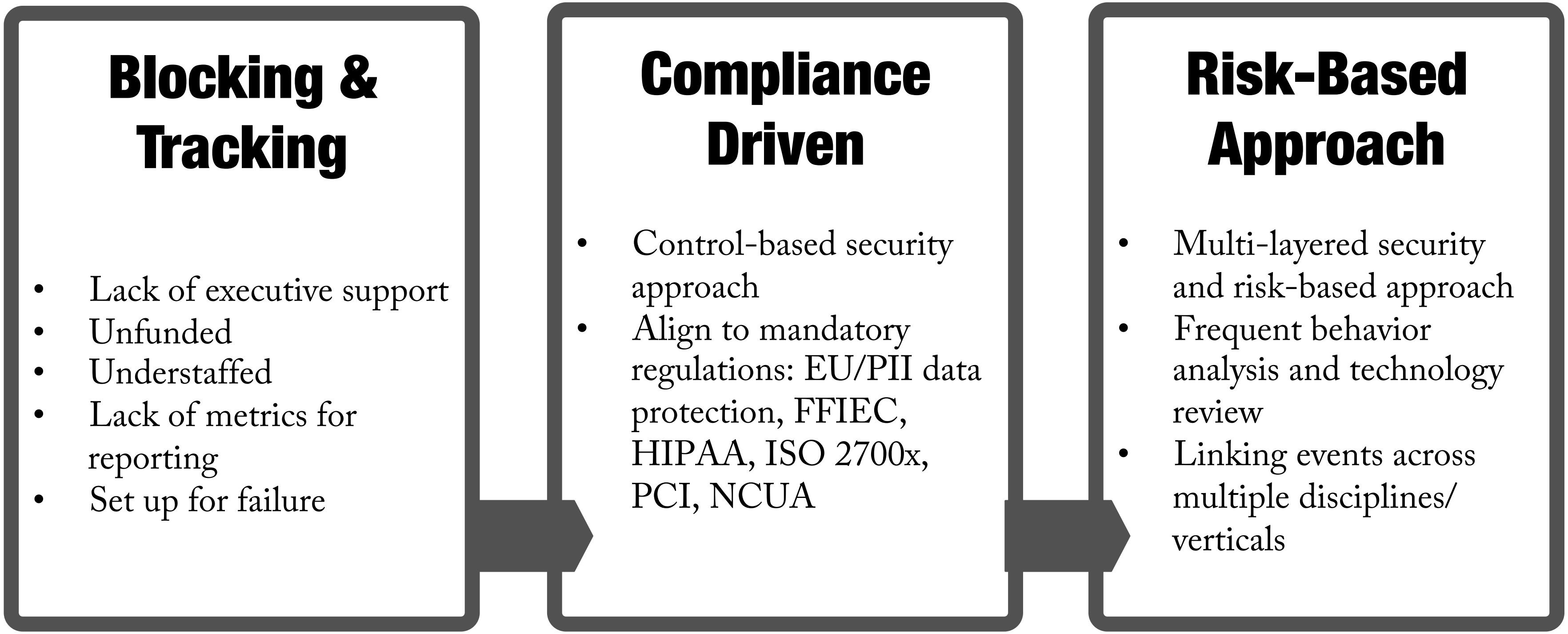




Negative Skew

Positive Skew

CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)



Blocking & Tracking

- Lack of executive support
- Unfunded
- Understaffed
- Lack of metrics for reporting
- Set up for failure

Compliance Driven

- Control-based security approach
- Align to mandatory regulations: EU/PII data protection, FFIEC, HIPAA, ISO 2700x, PCI, NCUA

Risk-Based Approach

- Multi-layered security and risk-based approach
- Frequent behavior analysis and technology review
- Linking events across multiple disciplines/ verticals

CONCLUDING REMARKS

- Risk-based approach is being used by Banking and Finance Institutions in Nepal for auditing and compliance.
- Risk-based approach in cyber security empowers businesses to conduct their businesses with confidence towards smart society.

Thank you.