CalQRisk

COMPLYPORT
COMPLIANCE LEADERSHIP

Risk Adequacy

Embedding the Process

2019-12-05

Embedding A Risk Framework

The last session looked at “How?” to implement a Risk Management Framework

Today we will look at how to embed the processes in an organisation:

1. The Plan-Do-Check-Act system of management
2. Arrangements for managing Risk
3. Arrangements for managing Compliance
4. Checklists
   - Risk Management
   - Compliance Management

Richard Revill, Risk Lead, Complyport Ltd – richard.revill@complyport.co.uk
Gerard Joyce, CTO and Director of Risk Management, CalQRisk Ltd - gjoyce@calqrisk.com

“Build it in

Don’t Bolt it on”

Risk & Compliance

Risk management and Compliance are complimentary functions

At a high level:

- Risk management is forward looking, pre-emptive – what may happen
- Compliance is the present and past, confirmatory – what is happening, what has happened

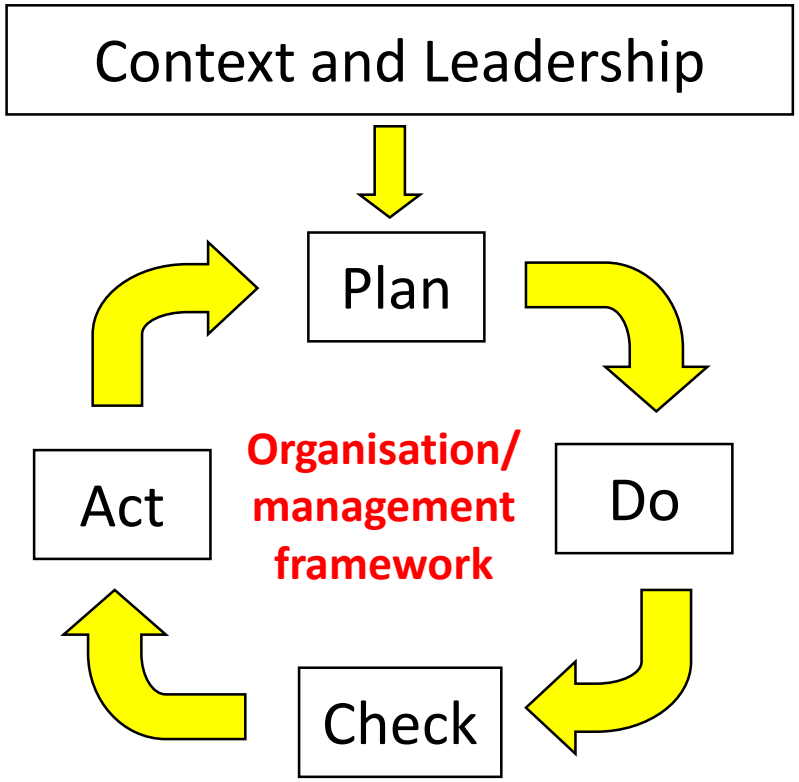
The FCA is focusing on risk management and discouraging "check-box compliance".

Compliance becomes more meaningful in a working risk management framework

CalRisk

COMPLYPORT
COMPLIANCE LEADERSHIP

Plan-Do-Check-Act System of Management



Context

- Objectives
- Scope
- Stakeholders
- Requirements

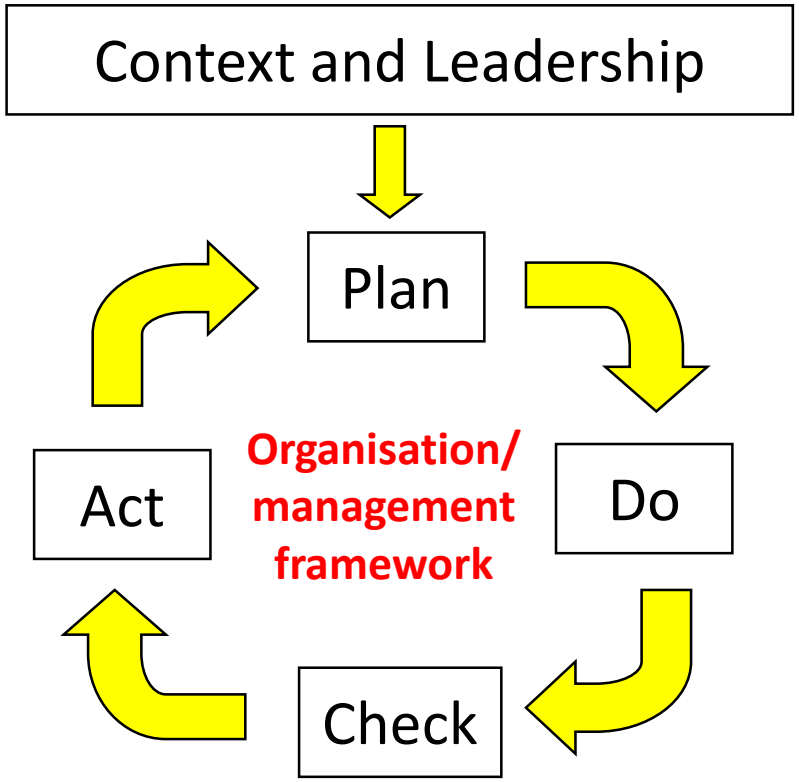
Leadership

- Policy
- Roles, Responsibilities, Authorities
- Resources

CalRisk

COMPLYPORT
COMPLIANCE LEADERSHIP

Plan-Do-Check-Act System of Management



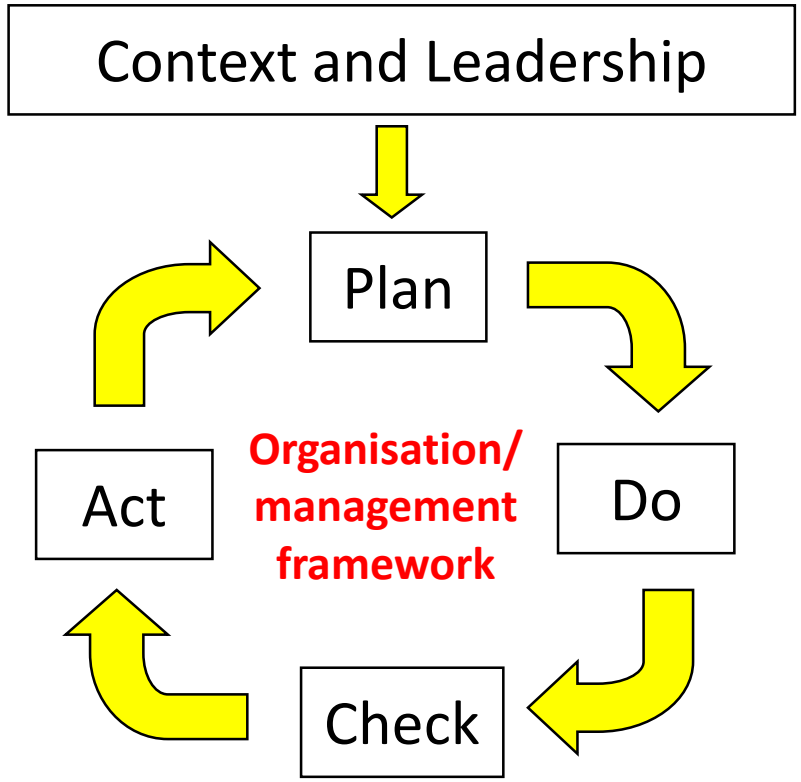
Plan

- Identify Threats & Opportunities
- Actions to address T&O
- Integrate into processes
- How to measure effectiveness
- Establish functional objectives
- Roles and Responsibilities
- Processes
- Training requirements
- Communication
- Documentation required
- How performance measured

CalRisk

COMPLYPORT
COMPLIANCE LEADERSHIP

Plan-Do-Check-Act System of Management



Do

- Implement processes
- Record results

Check

- Monitor operation
- Evaluate performance
- Audit
- Review
- Opportunities for improvement

Act

- Address non-conformity
- Identify causes
- Implement corrective and preventive actions
- Record actions taken

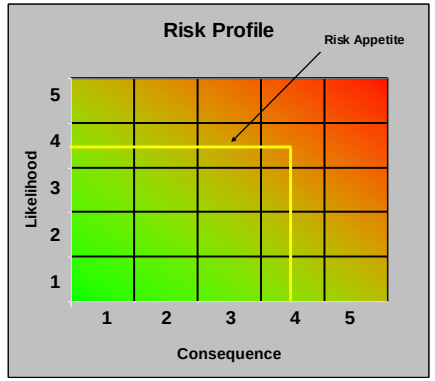
CalRisk

COMPLYPORT
COMPLIANCE LEADERSHIP

Arrangements for Managing Risk

Context

- Organisational Objectives, Risk Management Objectives
- Scope: All activity? All functions?
- Requirements: What's expected, Regulatory requirements, Proportionality



Leadership

- Policy, including commitments, Risk Criteria, Risk Appetite
- Have a Risk / Compliance Officer to lead the initiative with authority
- Provide appropriate resources

CalRisk

COMPLYPORT
COMPLIANCE LEADERSHIP

Arrangements for Managing Risk (cont)

Planning

- Risk assess what could cause failure of the programme and address
- Confirm objectives for each functional area, identify functional leaders
- Understand existing processes, how work is carried out
- Develop a standardised risk assessment process
- Identify training needs for all who have responsibility for managing risk
- Communicate and Consult: policy, implementation
- Decide on how info will be stored, reported, used in decision making
- Consider Key Risk Indicators to record as indication of effectiveness

Arrangements for Managing Risk (cont)

Do

- Train people on assessment process and conduct assessments
- Rank risks and prioritise treatment / actions
- Verify that controls are working / being applied.
- Maintain records

Check

- Are risk management objectives being met?
- Review KRIs

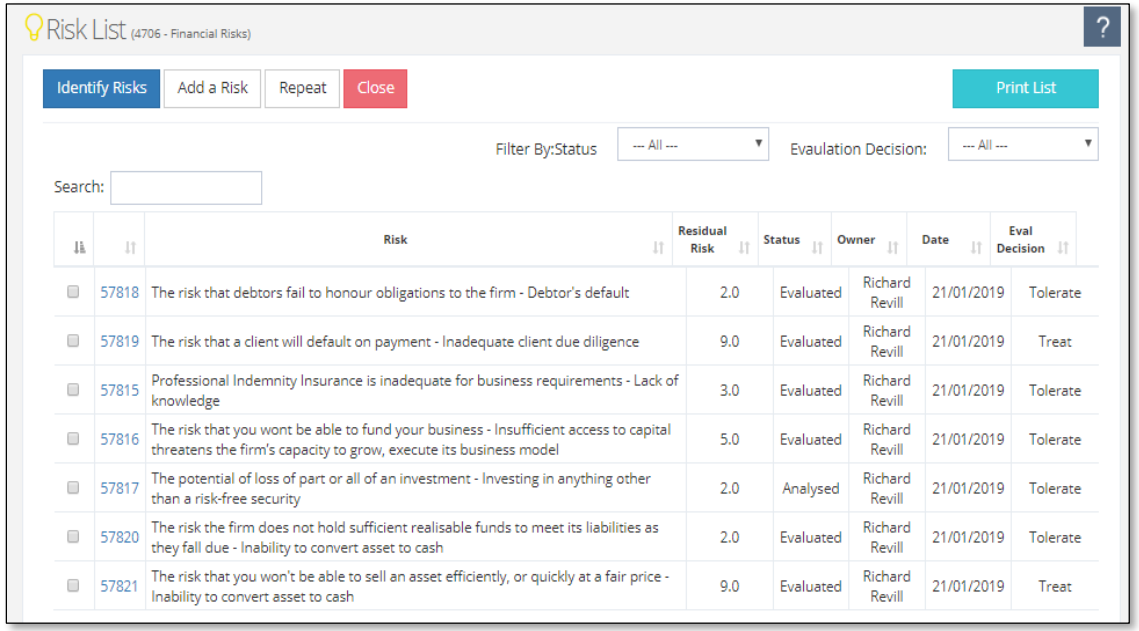
Act

- Modify the framework / arrangements for managing risk

Arrangements for Managing Risk (cont)

Decide how info will be stored, reported & used in decision making; it is critical to maintain records

Origin	Category	Driver	Description	Inherent Likelihood	Inherent Consequence	Mitigation and controls	Residual Likelihood	Residual Consequen	Residual Score
Client	InfoSec	AML / MA	AML policies fail to pick up client with 'black marks' who	4	5	MLRO ensures all support team highly trained with robu	2	5	10
Client	Legal	Compliance Risk	KYC ie classification failure, FCA not involved	5	5	Compliance ensures all support team highly trained wit	3	3	9
Provider	Operational	Supply Chain Failure	Failure of suppliers' supplier	4	4	Supplier should have alternative suppliers to contract w	3	3	9
Provider	Legal	Litigation	Having to sue a provider over failed service or damage cs	5	4	Most suppliers are within the group so litigation implau	3	3	9
Internal	Operational	Lack of Resources	Incidents relating to lack of resource to carry out necess	5	4	Firm is small with relatively flat hierarchy. Unlikely that	3	3	9
Regulator	Regulatory	Regulatory Breach	Breach of any regulatory condition leading to financial p	3	4	Engagement of Complyport a compliance consultant. Im	2	4	8
Client	InfoSec	Personal Data breach	Client confidentiality breach, where data released to in	4	4	strict privacy and security policies in place	2	4	8
Provider	Operational	Withdrawl of Service	Firm is given 3 months notice to terminate all support	3	5	Temporary support staff could be brought in and other s	2	4	8
Provider	InfoSec	Systems Loss	Supplier loses ability to provide systems for one day	4	5	If was a total systems failure for longer than a day then	2	4	8
Market	Strategic	Market Downturn	The industry suffers a decline in attracting new custome	5	5	Strategic decisions to trim overheads. Increase marketi	2	4	8
Market	Competitor	Disruptive Technology	Competitor develops market leading new technology	4	5	The firm has access through the group to high quality lar	2	4	8
Internal	Key-Person	Major Staff Loss	Loss of senior members of staff or significant numbers of	5	4	The firm is committed to providing staff with competitiv	2	4	8
Client	Reputational	Adverse Publicity	Dissatisfied client, forum and social media damage	4	4	Team is consistently reviewing social media and can res	3	2	6
Internal	Legal	HR Litigation	Loss brought about by successful litigation form employe	4	3	The firm has rigid HR processes in place and operates ac	2	3	6
Client	Financial	Bad creditor	The risk that a creditor will not honour its obligations to	3	3	Credit checks and due dligence on client take on	2	3	6
Client	Operational	Failure of Service	Client facing system goes down for 1 day; compensation	4	3	Strong IT systems and back ups	3	2	6
Provider	InfoSec	Data Loss	Supplier loses data from one of its data centers	4	4	Only providers of the highest standing are employed and	2	3	6
Provider	Reputational	Adverse Publicity	If a provider outside the Group is deemed no linger acce	4	5	New providers will be sought.	3	2	6
Internal	Operational	Denial of Premises	Circumstances leading to denial of access to business pr	5	5	Premises are serviced offices with a large provider. Alte	2	3	6
Internal	Operational	Failure of BCP	Business Continuity Plan overly optimistic and not effect	4	4	Elements of BCP regularly tested. Staff required to read	2	3	6
Internal	Operational	Lack of Training	Incidents relating to lack of staff awareness and training	4	3	Training in place for all staff on a regular basis. Firm is sr	3	2	6
Internal	Financial Crin	Rogue employee	The potential that an employee of the firm could use the	3	5	All staff are required to complete AML, Anti-Bribery and	2	3	6
Internal	InfoSec	Data Loss	Loss of company and / or client data	4	5	System is backed up on a daily basis, with snap-shots da	2	3	6
Internal	InfoSec	Systems Loss	Loss of systems	5	3	System in cloud-based and virtually hosted. Soft restora	3	2	6
Internal	InfoSec	Service Loss (DDOS)	Cyber attack rendering service unreachable by clients	5	3	Data centre has defence mechanisms in place to respor	3	2	6
Internal	InfoSec	Lack of Training	Poor training leadings to system compromise through pc	4	5	IT functions are outsourced to specialist third parties. Ir	3	2	6
Financial	Financial Risk	Liquidity	Firm does not hold sufficient realisable funds to meet its	5	5	The firm maintains same-day funds equivalent to one m	2	3	6
Financial	Financial Risk	Credit Risk	Creditors fail to honour obligations to the firm.	3	4	The firm practices strict credit control policies. The firm	2	3	6
Internal	Operational	Failure of DR	Disaster Recovery Plan overly optimistic and not effectiv	4	3	Elements of DR regularly tested. Staff required to read a	2	2	4
Client	InfoSec	Systems Loss	Complete systems failure leading unable to conduct bus	3	4	Strong IT systems and back ups and can arrange tempori	1	4	4
Client	InfoSec	Data Loss	Client data is lost from a virus or other event	2	5	Strong Systems security and back ups	1	4	4
Provider	Operational	Bankrupcy	A major provider is declared bankrupt	3	4	All major providers are reviewed on an annual basis, an	1	4	4
Provider	InfoSec	Personal Data breach	Provider discloses data to a 3rd party	3	5	strict privacy and security policies in place	1	4	4
Internal	InfoSec	Lack of Investment	Underfunding leading to low resourcing and low system	5	3	Systems are fully resourced and the IT budget reviewed	2	2	4
Internal	InfoSec	Poor Planning	Poor planning leading to low resourcing and low system	5	5	IT business plan reviewed annually	2	2	4
Financial	Financial Risk	Capital Adequacy	Firm's capital breaches minimum regulatory requiremer	5	3	Capital is reviewed by senior management on a monthly	2	2	4
Internal	InfoSec	Personal Data breach	Loss of client or staff personal data	4	2	No sensitive personal data kept for clients. Staff records	3	1	3
Client	Regulatory	Regulatory Breach	Significant breach leading to visit	3	3	Experienced management team with robust systems an	1	2	2
Internal	Business	Poor Decisions	Senior management, through inactivity or error, fails to r	4	4	The firm is confident that it has employed senior manag	1	2	2
Regulator	Legal	Litigation	Action or inaction leading to legal proceedings	4	3	Staff education, constant monitoring of client satisfactio	1	2	2
Financial	Financial Risk	Market Risk	Market movements lead to loss of funds	5	4	The firm holds no material positions in non-base curren	2	1	2
Provider	InfoSec	Theft	Equipment theft	3	2	Office is physically secure. Staff take laptops home. All h	1	1	1



CalRisk

COMPLYPORT
COMPLIANCE LEADERSHIP

Arrangements for Managing Compliance

Context

- Compliance objectives
- Scope: geographical, organisational, 3rd parties
- Requirements / obligations (Legal, Regulatory, Contractual, Own Rules)

Leadership

- Policy: commitments
- Organisational Roles, Responsibilities and Authorities
- Compliance function responsibilities

Arrangements for Managing Compliance (cont)

Planning

- Identify risks to compliance programme, actions to address these risks
- Compliance objectives for each function
- Who will be responsible for what element of compliance
- What will need to be done to achieve compliance
- What training will be required at each level / function
- What technology will be required to record and report
- How will compliance be monitored, measured and reported

Arrangements for Managing Compliance (cont)

Do

- Conduct Training (Ensure employees understand the need to comply)
- Implement (changes to) processes
- Document – ICAAP, ILAA

Check

- Monitor compliance with obligations / policy / procedures
- Report results, is the compliance programme working?

Act

- Address any non-compliance, improve / modify processes as necessary

Checklist: Risk Management

- Organisational Objectives
- Policy
- Scope
- RM Objectives
- Risk Appetite
- Risk Criteria
- Resources (Finance, People, Systems)
- Standards and Obligations
- Roles & Responsibilities
- RM Process
- Training
- Information System
- Reporting
- Key Risk Indicators

CalQRisk

COMPLYPORT
COMPLIANCE LEADERSHIP

Checklist: Compliance Management

- Compliance Objectives
- Policy
- Scope
- Regulations
- Obligations
- Behavioural Rules
- Resources (Fin. & People)
- Roles & Responsibilities
- Training
- Monitoring Programme
- Audit
- Information System
- Reporting
- Performance Indicators

Things You May be Interested in

SOLUTION

Risk Framework

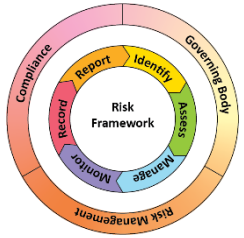
ComplyRisk gives you an out-of-the-box risk framework. A pre-populated *risk framework* providing you with all you need to build up a solid Pillar 2 methodology with defendable conclusions supporting considered Pillar 2 provisions and narrative.

Key features:

- Pre-populated (with relevant Pillar 2 risks)
- Supported by Compliance Experts
- Powered by CalQRisk enterprise risk engine

Key Components:

- Identified Risks
- Risk Assessment
- Task Management
- Monitoring
- Incidents Recording
- Dashboard Reporting



A major component of ICAAP (and ILAA), ready to go

Enquire Now

TRAINING

SM&CR

With 9 December 2019 falling next Monday, firms need to ensure their staff are appropriately trained in the Senior Management and Certification Regime ("SM&CR").

For most firm staff training can be split into two categories; (i) SMF holders and (ii) Certified and Conduct staff.

We have put together two face to face training sessions that can be delivered at your offices.

Conduct rules for Certified staff training
This training covers the Conduct Rules for individuals and how they apply to them in their roles. We tailor the training to your firm as well as the individuals attending The course lasts 1 hour.

Training for Senior Managers
This training focuses on the Senior Managers regime, the Certification regime and the conduct rules. Training lasts 1.5 hours.

Both sessions are also tailored to enable the firm to comply with the requirements in COCON 2.3.2 and FSMA 64B.

Enquire Now

Questions

Richard Revill, Risk Lead, Complyport Ltd – richard.revill@complyport.co.uk

Gerard Joyce, CTO and Director of Risk Management, CalQRisk Ltd - gjoyce@calqrisk.com

CalQRisk

COMPLYPORT
COMPLIANCE LEADERSHIP