BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Skilled Person Panel Lot Descriptions

The Skilled Person Panel is composed of fourteen areas of expertise, referred to as Lots. A summary of each Lot is provided below.

Lot A: Client assets

Advice, skills and technical expertise in client assets.

This will include skills, experience and expertise in areas such as, but not limited to, Client Assets (CASS) and SUP 16 in the appropriate regulator's Handbook, including governance, regulatory reporting and systems and controls arrangements associated with client assets.

Lot B: Governance and individual accountability

Advice, skills and technical expertise in assessing whether firms have effective governance arrangements, and how these support an appropriate culture and/or safety and soundness.

This should include, but not be limited to knowledge of relevant national, European and international regulatory requirements, standards, guidelines and industry best practice and experience and expertise in assessing:

- governance frameworks, board effectiveness, remuneration policies and practices, Senior Managers Regime, Senior Insurance Managers Regime, Certification Regime and Approved Persons Regime, including the assessment of relevant individuals' fitness and propriety and individual accountability;
- firms' business model, strategies, change management programmes (during transition, implementation, delivery), governance arrangements for recovery and resolution plans, firms' risk appetite, policies, procedures, decision making, management information; and whether these are effective in delivering fair outcomes for consumers, market integrity and promoting effective competition and/or safety and soundness.

Lot C: Controls and risk management frameworks

Advice, skills and technical expertise in assessing whether firms have effective controls and risk management frameworks, including identification and control arrangements to pre-empt, identify and mitigate risks in their business models including outsourcing arrangements; taking a risk based approach to deliver fair outcomes for customers and/or safety and soundness.

This should include but not be limited to knowledge of relevant regulatory requirements, standards, guidelines and industry best practice and experience and expertise in assessing:

- internal control effectiveness across the three lines of defence, stress testing frameworks and all types of enterprise-wide risk including but not limited to: operational risk, credit risk, traded risk, liquidity risk, compliance/legal risk, conduct risk, valuation risk and reputational risk management.
- management information (MI) that effectively tracks and monitors risk trends and analysis that would enable pro-active mitigation of risk; thereby minimising risk to business plans, strategic delivery, market impact and customer detriment; including how the MI is used to remedy both emerging and crystallised risk.
- how emerging/crystallised risks are escalated through the risk governance framework.

Lot D: Conduct of business

Advice, skills and technical expertise in assessing quality of advice, sales practices, complaints handling, conduct of business rules and guidance, the fair treatment of customers, arrears management and retail conduct risks associated with each stage of the retail product life-cycle. Ability to adapt their approach and resource where necessary to ensure a proportionate approach to smaller regulated firms.

This will include skills, experience and expertise in a wide variety of product types and in areas such as, but not limited to; COBS, ICOBS, MCOB, BCOBS, CONC, DISP in the FCA handbook the requirements of other legislation such as the Competition Act 1998, PSR and EMR, and expertise in past business reviews and overseeing redress exercises.

Lot E: Financial crime

Advice, skills and technical expertise in financial crime, anti-bribery and corruption, third party payments, market manipulation, insider trading, anti-money laundering and governance of these areas.

This will include skills, experience and expertise in the provision of advice and the investigation of areas including, but not limited to, the Market Abuse Regulation (MAR), the STOR regime, the Money Laundering Regulations, the Bribery Act 2010, relevant SYSC rules, the Joint Money Laundering Steering Group guidance, PSR and EMR.

Lot F: Prudential – Deposit takers, recognised clearing houses and PRA-designated investment firms

Advice, skills and technical expertise in the prudential arrangements for deposit takers, recognised clearing houses and PRA-designated investment firms in the following risk areas:

- credit risk including but not limited to retail; corporate; structured credit and/or the modelling of these risks;
- traded risk including but not limited to market, counterparty credit risk, interest rate risk in the banking book and/or the modelling of these risks;
- liquidity and treasury risk and/or the modelling of these risks;
- operational risk including the measurement/ modelling of these risks;
- recovery and resolution;
- settlement risk.
- Experience is sought in areas including but not limited to capital, stress testing, financial and non-financial resources requirements specified in the PRA rulebook, supervisory statements, and relevant regulatory and accounting requirements, standards, guidelines and industry best practice. The skills, experience and technical expertise should cover business as usual scenarios as well as the impact on capital, financial resources, non-financial resources and liquidity of mergers, acquisitions and transfers of business, and the reporting and calculation of relevant regulatory quantities.

Lot G: Prudential – Insurance

Advice, skills and technical expertise in life and/or non-life insurance in areas including, but not limited to, the following: Solvency II regulation; financial reporting including IFRS and Solvency II reporting; reserving and technical provisions; underwriting, claims handling and pricing; capital modelling – build and review, including the ability to assess insurance firms' validation of internal models; reinsurance modelling and exposure management, including catastrophe risk; actuarial modelling including across credit risk, market risk, operational risk and liquidity risk; asset-liability modelling; insurance Special Purpose Vehicles, insurance linked securities and valuation of assets; merger and acquisition due diligence; and recovery and resolution.

Lot H: Prudential – credit, market, pension and liquidity risk within investment firms, intermediaries and recognised investment exchanges

Advice, skills and technical expertise in regulatory capital, liquidity, and risk management within: investment firms, non-deposit taking mortgage lenders, intermediaries, and recognised investment exchanges. Covering topics such as, but not limited to: risk frameworks, credit risk, market risk, liquidity risk, modelling, stress testing, regulatory reporting, accounting standards and governance of these areas.

This will require skills, experience and expertise in the relevant CRD/CRR requirements, EBA guidelines, EBA RTS and ITS, and the FCA Handbook. The latter includes but it is not limited to IFPRU, BIPRU, MIPRU, IPRU(INV), SUP, SYSC, GENPRU and REC, International Accounting Standards, International Financial Reporting Standards and UK Generally Accepted Accounting Practice.

The skills, experience and technical expertise should include but not be limited to the following risks:

- Non trading book: credit risk, counterparty credit risk, credit valuation adjustment, settlement risk and/or the modelling of these risks
- Trading book: market risk, settlement risk, large exposures and/or the modelling of these risks
- Liquidity risk and treasury risk management and/or the modelling of these risks

Lot I: Prudential – Operational risk, recovery and resolution and wind-down within investment firms, intermediaries and recognised investment exchanges

Advice, skills and technical expertise in the regulatory space for operational risk, recovery and resolution and wind-down within: investment firms, non-deposit taking mortgage lenders, intermediaries, and recognised investment exchanges. Covering topics such as, but not limited to: risk frameworks, regulatory Operational Risk capital, modelling, stress testing, regulatory reporting, and governance of these areas.

This will require skills, experience and expertise in the relevant CRD/CRR requirements, EBA guidelines, EBA RTS and ITS, and FCA Handbook. The latter includes but it is not limited to IFPRU, BIPRU, MIPRU, IPRU(INV), SUP, SYSC, GENPRU and REC, International Accounting Standards, International Financial Reporting Standards and UK Generally Accepted Accounting Practice.

Lot J: Technology and information management

Advice, skills and technical expertise in a wide range of IT subject matters such as:
governance; infrastructure, strategy; risk management; regulatory compliance; cyber & information security, and relevant standards; systems development and maintenance; incident & problem management; project & change management; systems architecture and resilience of systems including business continuity planning; performance & capacity planning; data integrity, quality and migration; governance of outsourced and off-shore activities including cloud services; and regulatory reporting.

Skills and technical expertise in a wide range of technology related subject matters, such as:

- IT strategy and governance;
- IT risk management;
- Cyber and information security;
- Systems architecture, development and maintenance;
- Incident and problem management;
- Project and change management;
- Performance and capacity management;
- Data integrity, quality and migration;
- Service continuity and disaster recovery management;
- Governance of outsourced and off-shore activities (including cloud services); and
- Regulatory compliance and reporting.

- The Supplier is expected to have knowledge of national (and a broader awareness of international) regulatory requirements, standards, guidelines and industry good practice, such as but not limited to:
  - Configuration of IT infrastructure standards such IPSEC
  - IT control frameworks, such as COBIT, ISO standards and ITIL;
  - Cyber and information security standards and frameworks;
  - Project and programme management good practices such as PRINCE2 and MSP;
  - Software development life cycles such as SSA

Lot K: Threat Intelligence

Advice, skills and technical expertise in threat intelligence assessment including:

- Identification of vulnerable functions or systems and their susceptibility to known threats;
- Ranking of threats and acceptable levels of risk, collection and analysis of information pertaining to the identities, goals, motivations, tools and tactics of malicious entities intending to harm or undermine a targeted organisations operations, ICT systems or the information flowing through them;
- Understanding of the threat landscape applicable to financial services organisations and the capabilities and operations of threat actors (for example Advanced Persistent Threats);
- Drawing from specialist intelligence resource to inform opinion.
- Assessment of a regulated firm's own capabilities to obtain, analyse and make use of threat intelligence;
- Review of capability to analyse internal and external sources of information;
- Assessment of threat intelligence products created for consumption by the business.

Knowledge in the following areas (or similar), but not limited to:

- threat intelligence life cycle: direction, collection, analysis and dissemination; and
- ethical and legal restrictions relevant to information collection, and similar considerations (such as forthcoming legislation).

Lot L: CBEST Threat Intelligence

Advice, skills and technical expertise in threat intelligence as stated in Lot K plus CBEST accreditation.

Lot M: Penetration Testing

Advice, skills and technical expertise in:

- Penetration testing, traditional, red/blue/purple team, vulnerability scanning and assessment:
- Architectural approaches including security control layering, domain separation and boundary controls;
- Identification and testing of websites storing publicly accessible content;
- Identification of testing of physical controls used in the protection of offices, data centres, servers, cables;
- Identification and testing of logical controls used in the protection of information, including assessment of whether these are correctly configured and operating effectively;
- Phishing and pharming simulations
  - Identification of targets
  - Exploitation
- Honeypot usage;
- Malware creation and emulation;
- Rogue Wireless node detection;
- Understanding of malware protection, patching processes and operational security controls;
- Approaches to continuous monitoring of vulnerabilities, including enumeration, software flaws, incorrect configurations, breadth and depth of testing:
  - Understanding of testing requirements for systems and software development (black box, grey box, white box)
  - Understanding configuration management and change control

- Identification of covert channels
- Development of test procedures, scoping and approaches for the comparative measurement of vulnerabilities
- Definition of methods used to identify vulnerabilities (technical and logical)
- Definition of methods used to confirm vulnerabilities (exploitative activities/attacks)

- Application and effectiveness of red team testing approaches;
- Knowledge in the following areas (or similar), but not limited to FIPS 199 Categorisation in line with credible threats and vulnerabilities, and/or ISF IRAM2, OWASP, CVE, OVAL, CWE and CVSS;
- Knowledge of ethical and legal restrictions relevant to penetration testing on live systems, and similar considerations (such as forthcoming legislation).

Lot N: CBEST Penetration Testing

Advice, skills and technical expertise in penetration testing as stated in Lot M plus CBEST accreditation.