Engineering Progression Framework

Navigation

A quick orientation

This framework is here to make engineering progression clearer and more consistent across **[Company Name]**.
It's designed to be practical and easy to use, not something that sits on a shelf. The aim is to give engineers and managers a shared understanding of what progression looks like, what's expected at each level, and how people can grow over time. At its core, this framework is built on the belief that strong technology outcomes come from strong people and healthy team culture.
A few core ideas shape how this framework works:

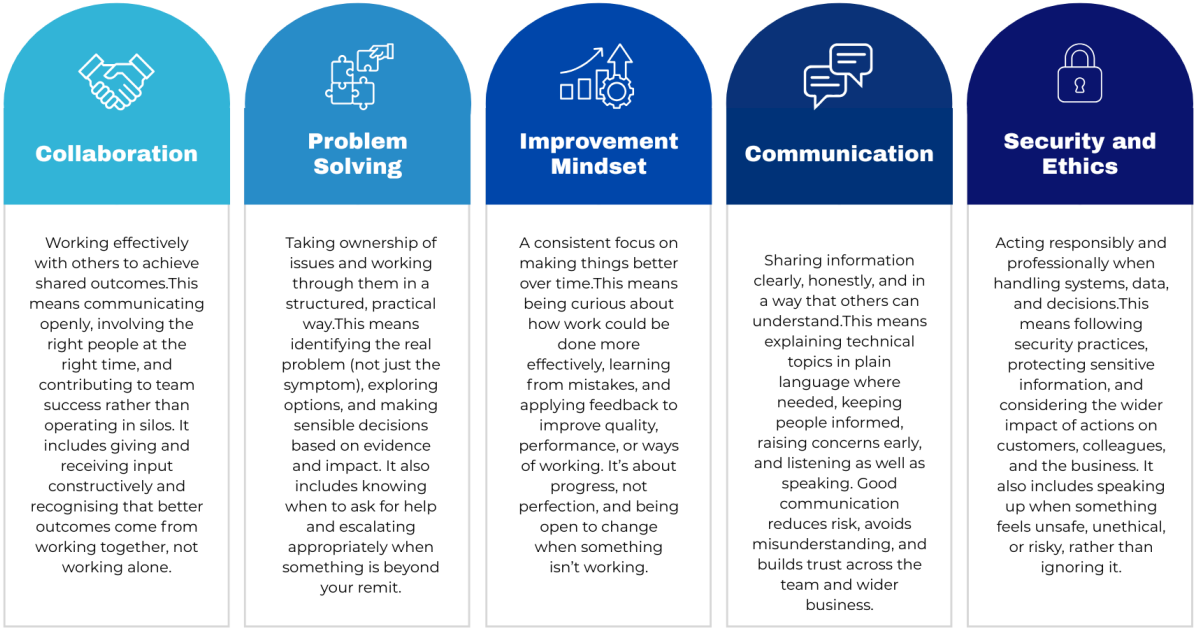
- We've anchored the framework in **SFIA (Skills Framework for the Information Age)**. SFIA is a widely used industry framework that gives us a common language for engineering capability and progression. Using it helps create clarity and consistency, especially across different teams and businesses, while avoiding reinventing the wheel.
- Rather than inventing our own definitions from scratch, SFIA gives us a solid, proven foundation. We then layer our own context and expectations on top, so the framework stays relevant, usable and grounded in real engineering work.
- The focus is on helping people understand how engineering roles evolve over time, **not on creating rigid rules or tick-box assessments**. This framework is designed to **support great career progression conversations and building a high performing team culture**.
- **Progression in this framework is driven by increasing responsibility, autonomy, influence and complexity, rather than tenure or job title alone**. As you progress as an engineer, so does your autonomy *(level of supervision)*, influence *(who and what your work affects)*, the complexity *(ambiguity and scale of problems you're trusted to solve)* of your role, and the business skills *(context, judgement and organisational awareness)* needed to operate successfully.
- This framework isn't about covering every possible task an engineer might take on. It's about making the meaningful differences between levels clear, especially as responsibility, autonomy and scope increase over time.
- **Engineers are not expected to demonstrate equal depth across every skill.** The framework recognises that different roles and strengths show up in different ways.

This framework exists to support you doing the word you do, recognising that clarity, trust and good conversations are essential to sustainable engineering **individual and team performance.**

How we work matters

While the framework describes skills, levels and responsibility, progression is **not just about *what* you do. It's also about *how* you work with others, how you approach problems, and how you contribute to a healthy, high-performing team.**

Across all roles and levels, we expect engineers to demonstrate five core behaviours. These behaviours are referenced throughout the framework and form part of how performance and progression conversations are approached in practice:



How progression shows up in practice

Progression in this framework is defined by increasing responsibility and scope. **Impact is the visible result of the responsibility** you're taking on.

As you progress, the problems you take ownership of become more complex, your influence widens, and the outcomes you're accountable for matter more to the team and the business. What that looks like will **vary by role and discipline**, but progression always involves taking responsibility for outcomes at the right level.

Looking at impact helps avoid turning this framework into a checklist. Rather than focusing on whether specific tasks have been completed, we look at how you operate day to day and **the difference that creates for the business**.

In practice, evidence of progression often shows up through things like:

- **Choosing work that meaningfully moves the team, product or business forward, in line with the scope of your role.**
- **Identifying opportunities to improve engineering outcomes and making those opportunities visible so they can be discussed and prioritised.**
- **Consistently delivering, contributing to shared goals and earning trust as a reliable, high-quality engineer.**
- **Applying the right level of complexity, keeping things simple where possible.**
- **Building systems and services that are resilient, well tested and able to scale as the business grows.**

Used this way, the framework supports conversations, helping you and your manager ground the level and skill expectations, in clear, observable examples.

How to use this framework

This framework is designed to **support clear, honest conversations about progression between you and your manager**. It's most useful when it's treated as a shared reference point, rather than something to be "applied" or assessed against in isolation.
Here are a few practical ways to use it.

Before a 1:1 or progression conversation

- Use the level descriptions to reflect on how you're currently operating day to day.
- Notice where you feel confident operating at your current level, and where you may already be taking on responsibility associated with the next level.
- Use the skills and examples as prompts to gather concrete evidence of how you work, the decisions you make, and the outcomes you own.

During conversations

- Use the framework as a shared language to talk about scope, responsibility and expectations.
- Focus on how you're operating in practice, rather than trying to "score" yourself against individual skills.
- Be open about where you're stretching, where you feel blocked, and what support might help you grow.

For development and growth

- Treat the framework as a guide for direction, not a checklist to complete.
- You're not expected to demonstrate equal depth across every skill. Different roles, strengths and opportunities will shape where you focus.

- Development often looks like gradually taking on more complex problems, broader influence, or greater ownership, rather than learning something entirely new.

Progression isn't automatic, and it doesn't happen just because time has passed. Moving between levels requires a conversation, and in some cases an appropriate role or opportunity to be available. Sometimes you may be ready to operate at the next level before a formal move is possible; other times, a clear gap in scope or responsibility may need to be addressed first.

When making progression decisions, you and your manager should be able to clearly explain:

- **how you're operating today compared to the expectations of the next level**
- **what evidence shows you're ready to take on greater responsibility and scope**
- **what would help you continue to grow, whether or not a role change is immediately available**

Used this way, the framework supports thoughtful progression conversations, rather than forcing premature decisions or rigid assessments.

The next section describes each engineering level in more detail, including how responsibility and expectations change as you progress.

Engineering Levels

Associate Engineer

At this level, the focus is on learning the role, building foundational skills, and working confidently within clear instructions and supervision. Associate Engineers at level 1 work under close supervision and follow established procedures. The work is well defined and routine in nature. This level is about developing core skills and knowledge through training, hands-on experience and day-to-day practice.

SFIA Skill	Skill description
Customer service support (CSMG)	● Handles routine customer enquiries and requests by following established procedures. ● Accurately records customer interactions and maintains relevant records. ● Escalates more complex issues to appropriate team members or departments when required.
Content design and authoring (INCA)	● Contributes to the creation of content under instruction. ● Supports the configuration of content items and files. ● Carries out pre-planned testing activities under supervision and records findings as directed.

Infrastructure operations (ITOP)	● Supports routine infrastructure tasks and basic troubleshooting under close supervision. ● Monitors infrastructure health and reports on component status to help maintain operational continuity.
Incident management (USUP)	● Follows agreed procedures to identify, log and categorise incidents. ● Uses provided tools to support the incident management process. ● Collects information as instructed and escalates incidents in line with documented procedures.
Functional testing (TEST)	● Executes defined manual functional test scripts under supervision to verify basic software functionality. ● Sets up test environments, uses basic automated tools where provided, records results and reports issues.
Non-functional testing (NFTS)	● Executes defined non-functional test scripts under supervision, focusing on system characteristics such as performance. ● Sets up basic test environments and uses standard tools to carry out prescribed tests.

Engineer

At this level, the focus is on building confidence and capability through hands-on work, supporting others, and solving routine problems while working under routine supervision. Engineers at this level continue to learn actively through training and on-the-job experience.
Engineers at level 2 provide assistance to others, work under routine supervision, and use their discretion to address routine problems. They actively develop their skills and knowledge through training and practical experience.

SFIA Skill	**Skill description**
Software design (SWDN)	● Creates and documents detailed designs for simple software applications or components. ● Applies agreed modelling techniques, standards, patterns and tools. ● Contributes to the design of components within larger software systems, ensuring alignment with overall design requirements, including security. ● Reviews own work.
Programming / software development (PROG)	● Designs, codes, verifies, tests, documents, amends and refactors simple programs or scripts. ● Applies agreed standards, tools and basic security practices to produce well-engineered outcomes.

	● Reviews own work.
Database administration (DBAD)	● Executes operational procedures, runs automation scripts, and carries out routine maintenance and monitoring of databases. ● Adjusts automation tasks as instructed to meet operational database standards. ● Reports on database performance, addresses issues directly where possible, or escalates to others for resolution.
Deployment (DEPL)	● Assists with deploying software releases and updates under routine supervision. ● Executes defined deployment processes and procedures using appropriate tools and techniques. ● Monitors deployed applications and reports issues. ● Assists with rolling back deployments when required.

Senior Engineer

At this level, the focus is on working more independently under general supervision, using judgement to plan and deliver work, and taking responsibility for quality and timeliness. Senior Engineers at level 3 handle a broader range of problems, support others through collaboration and knowledge sharing, and continue to deepen their expertise.

SFIA Skill	**Skill description**
Software design (SWDN)	● Undertakes complete design of moderately complex software applications or components. ● Applies agreed standards, guidelines, patterns and tools. ● Assists, as part of a team, in the design of components of larger software systems. ● Specifies user and/or system interfaces. ● Creates multiple design views to address different stakeholder concerns. ● Addresses functional and non-functional requirements, considering all relevant factors, including security. ● Assists in the evaluation of options and trade-offs.

	● Collaborates in reviews of work with others as appropriate.
Programming / software development (PROG)	● Designs, codes, verifies, tests, documents, amends and refactors moderately complex programs or scripts. ● Applies agreed standards, tools and security measures to achieve a well-engineered result. ● Monitors and reports on progress. ● Identifies issues related to software development activities. ● Proposes practical solutions to resolve issues. ● Collaborates in reviews of work with others as appropriate.
Database administration (DBAD)	● Provisions, installs and configures databases. ● Ensures the maintenance and reliability of databases. ● Monitors databases for load, performance and security events. ● Reports metrics and resolves operational issues. ● Executes standard operational procedures, including backups and restorations. ● Automates routine database administration tasks to specification using standard scripts and tools.
Deployment (DEPL)	● Deploys software releases and updates to production environments. ● Uses deployment tools and techniques to ensure consistent deployments. ● Monitors and troubleshoots deployment processes. ● Performs rollbacks of deployments in case of issues or failures. ● Collaborates with release management and operations teams.
Information management (IRMG)	● Applies information management standards and procedures. ● Supports information handling processes, including data capture, storage, retrieval and disposal. ● Performs data quality checks. ● Resolves routine data issues or escalates as required.
Information security (SCTY)	● Applies information security policies, standards and guidelines. ● Uses security controls and tools to protect information assets. ● Identifies and reports security events, issues or vulnerabilities. ● Supports their resolution.
Penetration testing (PENT)	● Follows standard approaches to design penetration testing activities. ● Executes penetration testing activities.

	● Researches and investigates attack techniques. ● Recommends ways to defend against identified attack techniques. ● Analyses and reports on penetration testing activities, results, issues and risks.
Customer service support (CSMG)	● Provides customer service support for standard or routine issues. ● Uses established procedures to respond to customer enquiries, requests and complaints. ● Records actions and outcomes. ● Escalates unresolved issues as appropriate.
Application support (ASUP)	● Provides application support for moderately complex incidents and problems. ● Investigates issues using agreed procedures and tools. ● Diagnoses and resolves issues. ● Monitors application performance. ● Escalates issues where necessary.
Content design and authoring (INCA)	● Designs and creates content using agreed standards, tools and templates. ● Works from defined requirements. ● Reviews content for accuracy, clarity and completeness. ● Maintains content in line with agreed processes.
System software administration (SYSP)	● Provisions system software components. ● Installs and configures system software. ● Maintains system software components. ● Monitors system software performance. ● Resolves operational issues. ● Automates routine administration tasks using standard tools and scripts.
Change control (CHMG)	● Applies change control procedures to assess changes. ● Authorises and supports the implementation of changes. ● Maintains change records. ● Supports communication of change activity. ● Identifies risks and issues. ● Escalates where appropriate.
Infrastructure operations (ITOP)	● Carries out infrastructure operations tasks, including monitoring, maintenance and fault resolution. ● Uses agreed tools and procedures to ensure availability and performance.

	● Escalates complex issues as required.
Asset management (ASMG)	● Maintains asset records. ● Supports asset tracking and reconciliation activities. ● Identifies discrepancies. ● Supports resolution in line with agreed procedures.
Demand management (DEMM)	● Supports demand management activities. ● Collects, analyses and maintains demand information. ● Produces reports. ● Supports communication with stakeholders.
Digital content management (DCMA)	● Applies digital content management procedures. ● Maintains content repositories. ● Supports publishing, archiving and retrieval activities using agreed tools and standards.
Incident management (USUP)	● Investigates incidents using agreed procedures and priorities. ● Resolves incidents. ● Coordinates incident resolution activities. ● Communicates status to stakeholders. Escalates major incidents as required.
Functional testing (TEST)	● Designs functional test cases. ● Executes functional test cases. ● Uses agreed tools and techniques to record and report results. ● Identifies defects. ● Supports defect resolution activities.
Non-functional testing (NFTS)	● Designs non-functional tests, including performance and reliability testing. ● Executes non-functional tests. ● Uses agreed tools and environments to record results. ● Analyses and reports results.
Quality assurance (QUAS)	● Applies quality assurance processes and checks. ● Reviews work products for compliance with standards and procedures. ● Identifies quality issues. ● Supports corrective actions.

Business process testing (BPTS)	● Designs tests to validate business processes across systems and services. ● Executes tests. ● Records results. ● Identifies issues impacting end-to-end process performance.

Lead Engineer

At this level, the focus is on working independently and taking responsibility for delivering clear, defined outcomes. Lead Engineers at level 4 use substantial judgement when handling complex work, plan and coordinate activities, and influence others within their team or function. They also contribute to improving ways of working and make sure outcomes meet required standards and objectives.

SFIA Skill	**Skill Description**
Software design (SWDN)	● Designs and architects complex software applications, components and modules. ● Uses appropriate modelling techniques that align with agreed software design standards, guidelines, patterns and methodologies. ● Produces and communicates multiple design views to address stakeholder concerns and to meet functional and non-functional requirements, including security. ● Identifies, evaluates and recommends design alternatives and trade-offs. ● Models, simulates or prototypes proposed software behaviours to support approval and effective software construction. ● Reviews, verifies and improves own designs against specifications, and leads reviews of others' designs.
Programming / software development (PROG)	● Designs, codes, verifies, tests, documents, amends and refactors complex programs/scripts and integration software services. ● Contributes to the selection of the software development methods, tools, techniques and security practices. ● Applies agreed standards, tools and security measures to produce well-engineered outcomes. ● Participates in reviews of own work and leads reviews of colleagues' work.

Solution architecture (ARCH)	● Contributes to developing solution architectures within specific business, infrastructure or functional areas. Identifies and evaluates alternative architectures and assesses trade-offs in cost, performance and scalability. ● Determines and documents architecturally significant decisions. ● Produces specifications for cloud-based or on-premises components, tiers and interfaces so they can be translated into detailed designs. ● Supports projects and change initiatives by preparing technical plans and applying design principles. ● Aligns solutions with enterprise and solution architecture standards, including security.
Database administration (DBAD)	● Uses technical expertise to maintain and optimise databases, carrying out updates and using automation tools. ● Configures tools and creates scripts to automate database tasks. ● Maintains operational procedures and checks they are followed, including compliance with security policies. Uses database management tools to monitor load and performance. ● Investigates database operational and security issues and supports their resolution. ● Provides reports and improvement proposals to stakeholders. ● Contributes to planning and implementing database maintenance and updates and implements agreed changes and routines.
Deployment (DEPL)	● Plans and carries out deployments of complex software releases and updates. ● Manages continuous deployment using automation tools and techniques. ● Develops and maintains deployment processes, procedures and scripts. ● Monitors and improves deployment processes for efficiency and reliability. ● Ensures deployed applications meet availability, performance and security requirements. ● Works with cross-functional teams to support successful deployments.
Information management (IRMG)	● Applies information management standards and procedures. ● Designs and implements information handling processes, including data capture, storage, retrieval and disposal. ● Ensures data quality and compliance with relevant policies and standards. ● Supports stakeholders in using information effectively.
Information security (SCTY)	● Applies information security policies, standards and guidelines. ● Selects and applies security controls and techniques to protect information assets.

	● Investigates and resolves security incidents and supports vulnerability remediation. ● Contributes to risk assessments and security improvement initiatives.
Penetration testing (PENT)	● Designs and carries out penetration testing activities. ● Researches and investigates attack techniques and recommends ways to defend against them. ● Analyses and reports on penetration testing activities, results, issues and risks.
Customer service support (CSMG)	● Manages the delivery of customer service support for a service or group of services. ● Handles complex or escalated customer issues and ensures they are resolved. ● Monitors service performance and identifies opportunities for improvement.
Application support (ASUP)	● Provides application support for complex incidents and problems. ● Investigates and resolves issues across multiple systems. ● Works with other teams and suppliers to restore service and improve application reliability.
Content design and authoring (INCA)	● Designs, creates and maintains content to meet user needs. ● Applies content standards, style guidelines and accessibility requirements. ● Reviews and improves content based on feedback and performance data.
System software administration (SYSP)	● Provides technical leadership in system software administration. ● Plans, installs, configures and maintains system software components. ● Automates administration tasks and resolves complex operational issues.
Change control (CHMG)	● Assesses, authorises and supports the implementation of changes. ● Ensures risks, impacts and dependencies are understood and managed. ● Maintains change records and ensures change activities are communicated effectively.
Infrastructure operations (ITOP)	● Plans and carries out infrastructure operations activities. ● Monitors infrastructure performance and availability. ● Investigates and resolves complex infrastructure issues and supports service continuity.
Asset management (ASMG)	● Manages asset records and tracking activities. ● Ensures assets are controlled, maintained and compliant with policies. ● Investigates discrepancies and supports asset optimisation activities.
Demand management (DEMM)	● Analyses and manages demand for services. ● Works with stakeholders to forecast demand and assess impacts on capacity and resources. ● Supports prioritisation and planning decisions.

Digital content management (DCMA)	● Manages digital content repositories and publishing processes. ● Ensures content is organised, maintained and accessible. ● Applies governance and standards across the digital content lifecycle.
Incident management (USUP)	● Manages the investigation and resolution of incidents. ● Coordinates incident response activities and communications. ● Ensures incidents are resolved within agreed service levels and supports major incident management.
Functional testing (TEST)	● Designs, executes and evaluates functional tests. Selects appropriate test techniques and tools. ● Identifies defects, supports their resolution and contributes to improving test processes.
Non-functional testing (NFTS)	● Designs, executes and analyses non-functional tests, including performance, reliability and security testing. ● Reports results and supports the resolution of issues that affect system quality.
Quality assurance (QUAS)	● Applies quality assurance methods and processes. ● Reviews work products for compliance with standards. Identifies quality risks and supports continuous improvement initiatives.
Business process testing (BPTS)	● Designs and executes tests to validate end-to-end business processes. ● Analyses results and identifies issues that affect business outcomes and service performance.

Principle Engineer

At this level, the focus is on taking broad responsibility for significant areas of work. Principal Engineers at level 5 provide technical leadership across teams and functions, apply expert judgement to complex and ambiguous problems, and shape standards, approaches and priorities. They also mentor others to build capability within the team and across the organisation.

SFIA Skill	**Skill description**
Software design (SWDN)	● Leads the design of complex software systems. ● Ensures designs align with organisational standards and strategic objectives. ● Establishes design principles, patterns and standards. ● Evaluates and approves design decisions and trade-offs.

	● Ensures designs address functional and non-functional requirements, including security, performance and scalability.
Programming / software development (PROG)	● Takes technical responsibility for significant software development activities. ● Defines development standards, tools and techniques. ● Reviews and approves complex code and designs. ● Leads improvements to development practices. ● Ensures secure, high-quality software delivery.
Solution architecture (ARCH)	● Leads the development of solution architectures for major initiatives. ● Defines architectural principles and standards. ● Evaluates and selects technologies and platforms. ● Ensures alignment between business strategy, enterprise architecture and solution design. ● Influences stakeholders at senior levels.
Database administration (DBAD)	● Provides technical leadership for database strategy, architecture and operations. ● Defines database standards and practices. ● Oversees performance, resilience, security and compliance. ● Leads resolution of complex database issues. ● Drives continuous improvement.
Deployment (DEPL)	● Defines and governs deployment strategies and practices. ● Leads the design and improvement of automated deployment pipelines. ● Ensures deployments meet organisational requirements for availability, performance and security. ● Influences release and operational practices.
Information management (IRMG)	● Defines and governs information management strategy, standards and policies. ● Ensures effective management of information assets across the organisation. ● Advises senior stakeholders on information use, value, risk and compliance.
Information security (SCTY)	● Provides leadership on information security strategy, architecture and controls. ● Assesses and manages significant security risks. ● Influences organisational security policies and practices. ● Leads response to major security incidents. ● Drives security improvement initiatives.
Penetration testing (PENT)	● Leads penetration testing strategy and activities.

	● Defines testing approaches and standards. ● Oversees complex testing engagements. ● Ensures findings are translated into effective risk mitigation actions. ● Advises senior stakeholders on security posture and risks.
Customer service support (CSMG)	● Leads customer service support strategy and service improvement initiatives. ● Ensures services meet business and user needs. ● Manages performance, escalations and senior stakeholder relationships.
Application support (ASUP)	● Provides leadership for application support services. ● Defines support models, standards and escalation processes. ● Oversees resolution of complex or high-impact issues. ● Drives improvements in application stability and service quality.
Content design and authoring (INCA)	● Leads content strategy and standards. ● Ensures content meets user needs, accessibility requirements and organisational objectives. ● Influences stakeholders on content quality, governance and continuous improvement.
System software administration (SYSP)	● Provides leadership for system software architecture and administration. ● Defines standards and approaches for reliability, security and automation. ● Oversees resolution of complex system issues. ● Drives operational excellence.
Change control (CHMG)	● Leads change control strategy and governance. ● Ensures organisational changes are assessed, prioritised and implemented effectively. ● Manages risk and impact at an organisational level. ● Influences senior stakeholders.
Infrastructure operations (ITOP)	● Leads infrastructure operations strategy and service delivery. ● Ensures infrastructure supports business objectives, resilience and performance requirements. ● Oversees major incidents. ● Drives operational improvement initiatives.
Asset management (ASMG)	● Defines asset management strategy, standards and governance. ● Ensures assets are managed effectively across their lifecycle. ● Advises on optimisation, compliance and risk at an organisational level.

Demand management (DEMM)	● Leads demand management practices and decision-making. ● Works with senior stakeholders to forecast demand. ● Prioritises initiatives and aligns resources with organisational strategy.
Facilities management (DCMA)	● Leads facilities management strategy and service delivery. ● Ensures facilities support organisational objectives, safety and resilience. ● Manages significant suppliers, contracts and risk.
Incident management (USUP)	● Leads incident management strategy and major incident response. ● Ensures effective coordination, communication and resolution of high-impact incidents. ● Drives continual improvement based on incident trends and outcomes.
Functional testing (TEST)	● Defines functional testing strategy, standards and approaches. ● Oversees testing for major systems and initiatives. ● Ensures test coverage, quality and risk mitigation align with organisational objectives.
Non-functional testing (NFTS)	● Leads non-functional testing strategy, including performance, resilience and security testing. ● Ensures risks are identified and addressed early. ● Influences quality and assurance practices across the organisation.
Quality assurance (QUAS)	● Defines and governs quality assurance frameworks and standards. ● Ensures quality is embedded across processes, products and services. ● Advises senior stakeholders on quality risks and improvement priorities.
Business process testing (BPTS)	● Leads business process testing strategy for end-to-end services. ● Ensures processes operate effectively across systems and organisational boundaries. ● Uses testing insights to inform business improvement and risk management.

Distinguished Engineer

At this level, the focus is on leading and directing work at an organisational level. Distinguished Engineers at level 6 set strategy, policies and standards within their domain, make high-impact decisions, and influence senior stakeholders. They are accountable for long-term outcomes and the effectiveness of major systems, services and practices.

SFIA Skill	**Skill description**

Software design (SWDN)	● Sets organisational direction for software design strategy, principles and standards. ● Leads the definition of these approaches. ● Oversees the design of the most complex and critical software systems. ● Ensures designs align with long-term business strategy, technology roadmaps and enterprise architecture.
Programming / software development (PROG)	● Sets organisational policy and strategic direction for software development practices. ● Establishes standards for tools, techniques and secure development. ● Influences adoption of emerging technologies and practices across the organisation.
Solution architecture (ARCH)	● Defines and governs enterprise-wide solution architecture strategy. ● Ensures architectural coherence across major programmes and portfolios. ● Shapes long-term technology direction. ● Advises executive leadership on architectural risk and opportunity.
Database administration (DBAD)	● Sets organisational strategy for database platforms, architecture and governance. ● Ensures enterprise-wide resilience, security and performance of data platforms. ● Influences investment and technology decisions at executive level.
Deployment (DEPL)	● Defines organisational deployment and release strategy. ● Governs deployment practices across portfolios and platforms. ● Ensures deployment approaches support resilience, scalability, security and continuous delivery at scale.
Information management (IRMG)	● Sets organisational information management strategy and governance. ● Ensures information assets are managed effectively, securely and compliantly across the enterprise. ● Advises executive stakeholders on information value, risk and opportunity.
Information security (SCTY)	● Provides authoritative leadership on information security strategy and architecture. ● Shapes organisational security posture and investment. ● Leads response to the most significant security threats and incidents. ● Advises at board level.
Penetration testing (PENT)	● Sets organisational approach to penetration testing and offensive security assurance. ● Ensures testing strategies align with enterprise risk management. ● Advises senior leadership on security weaknesses and organisational resilience.

Customer service support (CSMG)	● Defines organisational customer service strategy and operating model. ● Ensures services align with business priorities and user needs. ● Influences service management practices and performance at executive level.
Application support (ASUP)	● Sets strategy for application support and service continuity across the organisation. ● Ensures alignment between support models, architecture and business-critical services. ● Influences senior stakeholders on service risk and resilience.
Content design and authoring (INCA)	● Sets organisational direction for content strategy, standards and governance. ● Ensures content supports user needs, accessibility requirements and strategic objectives at scale. ● Influences senior stakeholders on content effectiveness and quality.
System software administration (SYSP)	● Defines enterprise-wide strategy for system software platforms and operations. ● Ensures reliability, security and scalability across the organisation. ● Influences technology investment and operational direction.
Change control (CHMG)	● Sets organisational change control policy and governance. ● Ensures effective management of change risk across major programmes and portfolios. ● Advises senior leadership on change impact and organisational readiness.
Infrastructure operations (ITOP)	● Defines enterprise infrastructure operations strategy. ● Ensures infrastructure services support business continuity, resilience and performance at scale. ● Leads response to major operational risks and incidents.
Asset management (ASMG)	● Sets organisational asset management strategy and governance. ● Ensures assets are optimised, compliant and aligned to long-term organisational needs. ● Advises executive stakeholders on cost, risk and value.
Demand management (DEMM)	● Defines organisational demand management strategy. ● Ensures demand aligns with strategic priorities, investment decisions and capacity planning. ● Influences executive decision-making on portfolio direction.
Facilities management (DCMA)	● Sets organisational facilities management strategy and governance. ● Ensures facilities support long-term organisational resilience, safety and operational effectiveness. ● Advises senior leaders on facilities-related risk and investment.
Incident management (USUP)	● Defines organisational incident management strategy and escalation models. ● Leads response to the most critical incidents. ● Ensures lessons learned drive systemic improvement across the organisation.

Functional testing (TEST)	● Sets organisational strategy for functional testing and assurance. ● Ensures testing approaches support enterprise risk management and delivery quality across portfolios.
Non-functional testing (NFTS)	● Defines organisational approach to non-functional testing, including performance, resilience and security. ● Ensures enterprise-wide risks are identified and addressed early.
Quality assurance (QUAS)	● Sets organisational quality strategy and governance frameworks. ● Ensures quality is embedded across systems, services and processes. ● Advises executive leadership on quality-related risk and improvement priorities.
Business process testing (BPTS)	● Defines enterprise approach to business process testing and assurance. ● Ensures end-to-end processes operate effectively across systems, suppliers and organisational boundaries.

CTO

At this level, the focus is on setting the overall vision, direction and governance for technology and engineering across the organisation. CTOs at level 7 are accountable for long-term outcomes, major decisions and the overall impact of technology on business objectives.

SFIA Skill	**Skill description**
Software design (SWDN)	● Sets the vision and direction for software design across the organisation and, where relevant, across the wider sector. ● Establishes and champions enterprise-wide design principles and long-term architectural direction aligned to business strategy and emerging technology trends.
Programming / software development (PROG)	● Sets executive-level strategy for software development capability. ● Determines organisational investment in tools, platforms and practices. ● Shapes long-term capability through workforce strategy, culture and external partnerships.
Solution architecture (ARCH)	● Owns enterprise and cross-enterprise architecture strategy. ● Ensures architectural decisions support organisational purpose, competitiveness and sustainability. ● Represents architectural interests at board level and with external stakeholders.

Database administration (DBAD)	● Sets executive strategy for data platforms, governance and stewardship. ● Ensures data capabilities support long-term organisational goals, regulatory obligations and innovation. ● Sponsors major data initiatives and investments.
Deployment (DEPL)	● Establishes executive direction for release and deployment strategy. ● Ensures deployment practices support organisational agility, resilience and risk appetite. ● Holds accountability for deployment-related risk at board level.
Information management (IRMG)	● Owns organisational information management vision and governance. ● Ensures information assets are treated as strategic resources. ● Is accountable for information-related risk, value and compliance at executive level.
Information security (SCTY)	● Sets organisational cyber and information security strategy and risk posture. ● Is accountable for security governance, investment and executive decision-making. ● Represents security risk at board level and with regulators and partners.
Penetration testing (PENT)	● Sets executive policy for offensive security assurance. ● Ensures penetration testing capability supports organisational risk management and regulatory expectations. ● Uses outcomes to inform board-level security decisions.
Customer service support (CSMG)	● Defines the executive vision for customer service and support capability. ● Ensures services align with organisational purpose, brand and customer expectations. ● Is accountable for service outcomes and organisational reputation.
Application support (ASUP)	● Sets executive strategy for application support and service resilience. ● Ensures critical services are protected and aligned with organisational priorities and risk tolerance.
Content design and authoring (INCA)	● Sets the vision for organisational content capability. ● Ensures content supports trust, accessibility, reputation and strategic communication. ● Holds accountability for content standards and governance.
System software administration (SYSP)	● Sets executive direction for system software platforms and operational capability. ● Ensures long-term sustainability, security and scalability of core platforms. ● Sponsors major platform investment decisions.
Change control (CHMG)	● Owns organisational change governance and risk appetite. ● Ensures change is managed in line with strategic priorities and organisational capacity.

	● Is accountable for systemic change impact and organisational resilience.
Infrastructure operations (ITOP)	● Sets executive strategy for infrastructure operations and resilience. ● Ensures infrastructure underpins organisational continuity, growth and security. ● Is accountable for major operational failures and recovery.
Asset management (ASMG)	● Owns executive strategy for asset stewardship and optimisation. ● Ensures assets deliver long-term value and support sustainability, compliance and organisational strategy.
Demand management (DEMM)	● Sets the executive approach to demand, investment and prioritisation. ● Balances organisational ambition with capacity, funding and risk. ● Influences board-level portfolio decisions.
Facilities management (DCMA)	● Sets executive direction for facilities strategy and resilience. ● Ensures physical environments support organisational wellbeing, safety, sustainability and performance.
Incident management (USUP)	● Owns executive accountability for major incidents and crisis response. ● Ensures incident management capability protects organisational reputation, safety and continuity. ● Leads executive-level learning from crises.
Functional testing (TEST)	● Sets executive expectations for assurance and quality of delivery. ● Ensures functional testing capability supports organisational risk tolerance and confidence in outcomes.
Non-functional testing (NFTS)	● Defines the executive stance on resilience, performance and security assurance. ● Ensures non-functional risks are understood and managed at organisational level.
Quality assurance (QUAS)	● Owns organisational quality vision and governance. ● Ensures quality is embedded in culture, leadership and decision-making. ● Is accountable for quality-related risk and organisational reputation.
Business process testing (BPTS)	● Sets the executive approach to end-to-end process assurance. ● Ensures organisational processes deliver intended outcomes across systems, partners and services.

Product

SFIA Skill	Skill description

Management

Understanding the 22 Skills

This section provides a high-level overview of the engineering skills used throughout the framework.
It explains what each skill covers and how it typically shows up in day-to-day work.
The descriptions are intended as a reference point to support development and progression conversations. They are not exhaustive, and how each skill is applied will vary by role, context and level.

SFIA Skill	Definition of the skill overall	What this skill typically involves (but is not limited to)
Software design (SWDN)	Architecting and designing software to meet specified requirements, ensuring adherence to established standards and principles.	● Designing software applications, components and interfaces, including security considerations ● Thinking about scalability, performance, resilience, security and privacy from the outset ● Using recognised design approaches, patterns and models to shape how systems are built ● Evaluating different design options and making informed trade-offs

		● Considering both functional needs (what the system does) and non-functional needs (how well it performs, how secure it is, how it integrates with other systems) ● Choosing and adapting design tools and techniques based on context, such as cloud-native or distributed systems ● Creating prototypes or simulations to test ideas and support decision-making
Programming / software development (PROG)	Developing software components and services through the application of programming languages, tools and techniques.	● Writing, testing, debugging and documenting software programs and scripts. ● Using agreed programming languages, tools and standards to produce reliable, maintainable code. ● Improving existing code through refactoring to enhance performance, security and maintainability. ● Integrating software components and services. ● Applying secure coding practices and addressing vulnerabilities. ● Reviewing code with others and using feedback to improve quality.
Solution architecture (ARCH)	Developing and communicating high-level solution designs to meet business and technical requirements.	● Turning business requirements into clear solution designs. ● Evaluating and selecting architectural approaches and technologies. ● Defining and documenting solution structures, components and interfaces. ● Addressing non-functional requirements such as performance, security, scalability and resilience. ● Aligning solutions with enterprise architecture standards and strategies. ● Supporting delivery teams through architectural guidance and assurance.
Database administration (DBAD)	Installing, configuring, monitoring and maintaining database management systems to ensure performance, security and availability.	● Installing, configuring and upgrading database software. ● Monitoring database performance, capacity and availability. ● Implementing backup, recovery and security controls. ● Automating routine database administration tasks. ● Investigating and resolving database-related issues. ● Supporting database design and optimisation activities.
Deployment (DEPL)	Planning, executing and managing the deployment of software, systems and	● Planning and coordinating software releases and deployments. ● Automating deployment processes and pipelines. ● Managing configuration and environment dependencies.

	updates into live environments.	● Ensuring deployments meet availability, performance and security requirements. ● Monitoring deployment outcomes and resolving issues. ● Working with development and operations teams to improve deployment practices.
Information management (IRMG)	Managing information to enable effective access, use, sharing, storage and disposal in accordance with policies and standards.	● Applying information management standards and procedures. ● Managing how information is captured, stored, retrieved and disposed of. ● Ensuring information quality, integrity and accessibility. ● Supporting legal, regulatory and organisational compliance. ● Advising stakeholders on effective use and handling of information. ● Supporting governance of information assets across their lifecycle.
Information security (SCTY)	Protecting information and information systems by ensuring confidentiality, integrity, availability and compliance.	● Applying information security policies, standards and controls. ● Assessing risks to information assets and recommending mitigations. ● Implementing and monitoring security controls and technologies. ● Detecting, investigating and responding to security incidents. ● Supporting vulnerability management and remediation. ● Promoting security awareness and good practice.
Penetration testing (PENT)	Identifying and exploiting vulnerabilities in systems, networks or applications to assess security resilience.	● Planning, designing and executing penetration testing activities. ● Researching and applying attack techniques and tools. ● Simulating real-world threats to identify weaknesses. ● Analysing results to assess risks and impacts. ● Documenting findings and recommendations. ● Advising on measures to strengthen security controls.
Customer service support (CSMG)	Managing and delivering customer service support to ensure effective resolution of user requests and issues.	● Handling customer enquiries, requests and complaints. ● Managing escalations and ensuring timely resolution. ● Monitoring service performance and customer satisfaction. ● Identifying trends and opportunities for service improvement. ● Ensuring customer interactions are recorded and managed effectively. ● Contributing to customer service processes and standards.

Application support (ASUP)	Providing support for applications to ensure availability, performance and continuity of service.	● Investigating and resolving application incidents and problems. ● Monitoring application performance and availability. ● Diagnosing faults across applications and related systems. ● Working with development and infrastructure teams. ● Implementing fixes or workarounds. ● Supporting service improvement and stability initiatives.
System software administration (SYSP)	Installing, configuring, operating and maintaining system software to support reliable and secure IT services.	● Installing, configuring and maintaining operating systems and system software. ● Monitoring system performance, capacity and availability. ● Applying patches, upgrades and configuration changes. ● Automating routine system administration tasks. ● Investigating and resolving system software issues. ● Ensuring systems meet security and compliance requirements.
Change control (CHMG)	Managing changes to systems and services to minimise risk and disruption while enabling improvement.	● Assessing, authorising and scheduling changes. ● Evaluating risks, impacts and dependencies. ● Coordinating change implementation and communication. ● Maintaining change records and audit trails. ● Ensuring changes comply with governance and control requirements. ● Reviewing outcomes to support continual improvement.
Infrastructure operations (ITOP)	Operating and maintaining IT infrastructure to ensure availability, performance and resilience of services.	● Monitoring infrastructure components and services. ● Performing routine maintenance and operational tasks. ● Responding to infrastructure-related incidents and issues. ● Ensuring capacity, performance and availability targets are met. ● Supporting continuity and disaster recovery arrangements. ● Working with teams to improve infrastructure operations.
Asset management (ASMG)	Managing IT assets throughout their lifecycle to ensure control, value and compliance.	● Maintaining accurate asset records and inventories. ● Tracking asset ownership, location and status. ● Supporting procurement, deployment and disposal activities. ● Ensuring compliance with asset and licensing policies. ● Identifying discrepancies and supporting resolution.

		• Contributing to asset optimisation and cost control.
Content design and authoring (INCA)	Designing, creating and maintaining content to meet user needs and support effective communication and understanding.	• Researching user needs and content requirements. • Designing, writing and editing content for digital and non-digital channels. • Applying content standards, style guides and accessibility requirements. • Structuring content to support usability and clarity. • Reviewing and updating content based on feedback and analytics. • Working with stakeholders to ensure content accuracy.
Demand management (DEMM)	Managing and influencing demand for products and services to ensure that they are prioritised, planned and delivered effectively.	• Capturing and analysing demand from stakeholders. • Forecasting demand and assessing impacts on capacity and resources. • Prioritising demand in line with organisational objectives. • Balancing demand against available capability and investment. • Communicating demand-related information. • Supporting planning, budgeting and investment decisions.
Facilities management (DCMA)	Managing facilities to ensure they are safe, secure, efficient and effective in supporting organisational needs.	• Managing buildings, accommodation and physical infrastructure. • Ensuring compliance with health, safety and environmental regulations. • Coordinating maintenance, repairs and refurbishments. • Managing suppliers and facilities-related contracts. • Supporting business continuity and resilience planning. • Optimising use of space and facilities.
Incident management (USUP)	Managing the lifecycle of incidents to restore normal service operation as quickly as possible and minimise business impact.	• Detecting, logging and categorising incidents. • Coordinating investigation and resolution activities. • Managing major incidents and escalations. • Communicating incident status to stakeholders. • Conducting post-incident reviews. • Supporting continual service improvement.
Functional testing (TEST)	Testing software or systems to ensure that specified functional requirements are met.	• Designing and executing functional test cases. • Preparing and managing test data and environments. • Recording, analysing and reporting test results. • Identifying and retesting defects. • Supporting defect resolution.

		● Contributing to test planning and improvement.
Non-functional testing (NFTS)	Testing systems to evaluate non-functional characteristics such as performance, reliability, usability and security.	● Designing and executing non-functional tests. ● Assessing performance, scalability, resilience and security. ● Analysing and reporting test results and risks. ● Identifying and addressing non-functional issues. ● Supporting remediation and optimisation. ● Contributing to quality and assurance practices.
Quality assurance (QUAS)	Ensuring that processes, products and services meet defined quality standards and requirements.	● Applying quality assurance methods and standards. ● Reviewing processes, products and services for compliance. ● Identifying quality risks and non-conformances. ● Supporting corrective and preventive actions. ● Contributing to continuous improvement initiatives. ● Promoting quality awareness and good practice.
Business process testing (BPTS)	Testing end-to-end business processes to ensure they operate correctly across systems and services.	● Designing and executing business process test scenarios. ● Validating end-to-end process flows across systems. ● Recording and analysing test results. ● Identifying process-related defects and risks. ● Supporting remediation and re-testing. ● Assuring business outcomes and service performance.

.