Customizing AI with Prompts

MGMT 675: Generative AI for Finance

Kerry Back

The Big Idea: It's All Just Text

Every AI customization—skills, slash commands, custom instructions—works the same way: **additional text is added to the prompt** that the model sees.

- **Skills** = instructions for *how* (a system prompt extension loaded when relevant)
- **Slash commands** = triggers that say *do* (typing `/name` loads that skill's instructions into context)
- Same pattern everywhere: Custom GPTs, Copilot instructions, `.cursorrules`, Gems

This deck uses Claude's implementation as the example, but the concepts are universal. Any platform that lets you add instructions to the prompt is doing the same thing.

What is a Skill?

A **skill** is a set of instructions (and optional code) that specializes a general-purpose AI for a specific domain or task. In Claude, it's a folder with a markdown file; other platforms use similar mechanisms.

A Skill Provides

- System prompt (domain knowledge)
- Workflow instructions
- Best practices and constraints
- Python/JavaScript helper scripts
- Reference documentation

The AI Platform Provides

- The LLM (Opus or Sonnet)
- Agent control loop
- File read/write tools
- Code execution sandbox
- Web search capability

Anatomy of a Skill

Skill Folder Structure

```
skills/
  xlsx/
    SKILL.md      <- Main file
    scripts/
      recalc.py
    references/
      schema.md
```

SKILL.md Structure

```
---
name: xlsx
description: "Excel file..."
---

# Requirements for Outputs
- Zero formula errors
- Use formulas, not hardcodes

# Workflows
1. Choose pandas or openpyxl
2. Create/modify file
3. Recalculate formulas
```

SKILL.md: The System Prompt

- **Frontmatter**: Name and description (YAML header)
- **Requirements**: Quality standards and constraints
- **Workflows**: Step-by-step procedures
- **Code Examples**: Patterns for the LLM to follow
- **Error Handling**: How to diagnose and fix problems

The SKILL.md file is automatically injected into Claude's context when working in a project that contains the skill.

Scripts: The Custom Tools

- Python or JavaScript files in `scripts/` folder
- Claude Code can execute them
- Extend Claude's capabilities
- Handle tasks LLM can't do directly

Example Scripts

- `recalc.py` – Recalculate Excel formulas via LibreOffice
- `validate.py` – Check file structure
- `unpack.py` – Extract XML from Office files
- `html2pptx.js` – Convert HTML to PowerPoint

Example: Rice Database Skill

Stand-Alone App

- Custom web application
- Hard-coded SQL generation prompt
- Fixed agent logic in Python
- Single-purpose: query database
- Requires developer to update

Claude Code + Skill

- SKILL.md with database schema
- Connection code examples
- Table descriptions
- **Plus**: Can also make charts, Excel files, Word reports
- User can extend easily

Same database access, but infinitely more flexible

Skill vs Stand-Alone Agent

Feature	Stand-Alone	Skill
Agent logic	Custom code	Claude Code
System prompt	Hard-coded	SKILL.md file
LLM	Your choice	Claude Opus/Sonnet
Tools	Custom built	Scripts + built-in
Maintenance	Developer	Edit markdown
Combine tasks	No	Yes

Skills let you create **specialized agents** without writing agent logic. Claude Code handles the control flow; you just provide the domain knowledge.

Where Skills Live

- **Project skills**: `.claude/skills/` in your project folder
- **User skills**: `~/.claude/skills/` (shared across projects)
- Claude Code automatically loads skills from both locations
- Skills can reference each other (e.g., xlsx skill uses ooxml validation)
- Skills also work in **Claude.ai**, **Chat**, and **Cowork** (details later)

Community Skills Repository: github.com/VoltAgent/awesome-agent-skills
200+ skills from official teams and the community

Creating Your Own Skill

1. Create folder: `.claude/skills/my-skill/`
2. Create `SKILL.md` with:
   - YAML frontmatter (name, description)
   - Domain knowledge and instructions
   - Code examples and workflows
3. Optionally add `scripts/` folder with helper code
4. Start using Claude Code – skill is automatically loaded

Example: Earnings Call Skill

In-Class Exercise: Personal Task List Skill

Create a skill that manages a personal task list organized by categories. Claude will add, complete, and review tasks—following *your* format automatically.

SKILL.md (Sketch)

```
---
name: tasks
description: "Manage my personal
  task list"
---

# File Layout
- research/tasks.md
- teaching/tasks.md
- admin/tasks.md
- personal/tasks.md

# Task Format
- [ ] [#tag] Description
      | added YYYY-MM-DD
- [x] [#tag] Done task
      | done YYYY-MM-DD

# Behaviors
- "add task" -> append to file
```

Try It

1. Create .claude/skills/tasks/SKILL.md
2. Define your categories (work, personal, school, . . .)
3. Define your format (checkboxes, tags, dates)
4. Start Claude Code and say: "Add 'buy groceries' to my personal tasks"
5. Then: "What's pending?"

Why This Works

- Claude creates the folder and files for you
- Follows your format every time—no drift
- Natural language in, structured markdown out
- **You defined the system by writing a prompt**

Skills Across Claude Formats

Skills are not limited to Claude Code. The same skill can be deployed and used across Claude.ai, Claude Desktop, and Claude Code.

Format	How to Install	How to Invoke
Claude.ai (web)	Upload ZIP in Settings $\rightarrow$ Capabilities	Automatic or /name
Chat (Desktop)	Same as Claude.ai (shared account)	Automatic or /name
Cowork (Desktop)	Install as a plugin via sidebar	Automatic or /name
Code tab (Desktop)	Place in .claude/skills/	Automatic or /name
Claude Code CLI	Place in .claude/skills/	Automatic or /name
VS Code extension	Place in .claude/skills/	Automatic or /name

- **Automatic**: Claude loads the skill when it detects a relevant task
- /name: You invoke it explicitly (e.g., /investment-memo)
- Skills in ~/.claude/skills/ are shared across all your projects

Deploying Skills: Three Methods

Claude.ai / Chat

1. ZIP your skill folder
2. Go to **Settings** → **Capabilities**
3. Click **Upload skill**
4. Toggle it **ON**
5. Requires code execution enabled

Pro, Max, Team, Enterprise

Cowork

1. Click **Plugins** in sidebar
2. Browse official plugins or click **Upload plugin**
3. Plugins bundle skills + connectors + slash commands
4. 11 official plugins available

Pro, Max, Team, Enterprise

Code / CLI / VS Code

1. Create folder: .claude/skills/name/
2. Add SKILL.md
3. Optionally add scripts/
4. Done—auto-detected

Pro, Max (via Claude Code)

Using Skills: Examples Across Formats

Skills and Slash Commands

Typing /name simply loads that skill's instructions into the AI's context—it's just a prompt. Every skill has a **name** that becomes a **slash command**.

How It Works

- A skill's name is set in the YAML frontmatter of SKILL.md
- Type /name to invoke it explicitly
- Or just describe your task—Claude loads the skill automatically when it detects a match
- Automatic loading works in all modes (Claude.ai, Chat, Cowork, and Code)

Examples

- /xlsx — invoke the Excel skill
- /earnings-call — invoke an earnings call analysis skill
- /investment-memo — invoke a memo-writing skill
- /commit — invoke a git commit skill

These appear alongside built-in commands like /clear and /compact when you type /.

Skills vs. Subagents

A **skill** is a reference manual Claude follows in your conversation. A **subagent** is a separate worker you dispatch independently.

	Skill	Subagent
What it is	Instructions + scripts	A separate agent
Analogy	Giving Claude a playbook	Handing a task to a colleague
Runs where	Same conversation	Its own context window
Works in	Claude.ai, Chat, Cowork, Code	Claude Code only
Defined in	SKILL.md	AGENT.md
Created with	Manual or /agents	/agents
Best for	Standards, templates, workflows	Delegating well-defined tasks

- **Use a skill** when you want Claude to follow specific standards *while you work with it interactively*
- **Use a subagent** when you want to *hand off* a self-contained task (e.g., "analyze these 10 files")
- They combine naturally: a subagent can have skills loaded, giving it both independence and domain expertise

What is a Plugin?

A **plugin** is a *packaged collection* of skills, agents, hooks, and MCP servers that can be shared across teams and projects. Think of it as the distribution format for skills.

A Plugin Can Include

- Skills (SKILL.md files)
- Agents (AGENT.md files)
- Hooks (auto-run on events)
- MCP servers (external tools)
- LSP servers (language analysis)

Why Use Plugins?

- Share skills with your team
- Namespace prevents conflicts
- Semantic versioning
- Install from marketplaces
- Bundle multiple components

Anatomy of a Plugin

Directory Structure

```
my-plugin/
  .claude-plugin/
    plugin.json     <- Manifest
  skills/
    code-review/
      SKILL.md
    documentation/
      SKILL.md
  agents/
    reviewer.md
  hooks/
    hooks.json
  .mcp.json
```

plugin.json (Required)

```json
{
  "name": "my-plugin",
  "description": "What it does",
  "version": "1.0.0",
  "author": {
    "name": "Your Name"
  },
  "repository":
    "github.com/user/plugin",
  "license": "MIT"
}
```

Skills vs. Plugins

Aspect	Standalone Skill	Plugin
Best for	Personal workflows	Team / community sharing
Invocation	/skill-name	/plugin:skill-name
Location	.claude/skills/	Own directory with manifest
Components	Skills only	Skills + agents + hooks + MCP
Versioning	None built-in	Semantic versioning
Distribution	Copy the folder	Marketplace or /plugin install

Practical workflow: Start with a standalone skill for quick prototyping. When you're ready to share, wrap it in a plugin by adding a `.claude-plugin/plugin.json` manifest.

Installing and Managing Plugins

Plugin Ecosystem

The plugin ecosystem is growing rapidly. Plugins are available for code quality, external integrations, development workflows, and domain-specific tasks.

Example Plugin Categories

- Code review and linting
- Git workflow automation
- Database connectors (MCP)
- API integrations (Slack, Jira, . . .)
- Documentation generators
- Testing frameworks

Resources

- Plugins documentation
- Discover & install plugins
- Plugin marketplaces
- Skills documentation
- Agent Skills Standard

Example: The Finance Plugin

Anthropic's official **finance plugin** bundles skills, MCP connectors, and slash commands for accounting and FP&A workflows—a concrete example of a plugin in the wild.

Plugin Structure

```
finance/
  .claude-plugin/
    plugin.json
  .mcp.json          <- Snowflake,
                        BigQuery, ...
  commands/
    journal-entry/
    reconciliation/
    income-statement/
    variance-analysis/
    sox-testing/
  skills/
    accounting/
      SKILL.md
```

Slash Commands

- `/finance:journal-entry` — accruals, fixed assets, payroll with debits/credits
- `/finance:reconciliation` — compare GL to bank or subledger
- `/finance:income-statement` — period-over-period comparison
- `/finance:variance-analysis` — decompose budget vs. actual gaps
- `/finance:sox-testing` — SOX compliance workpapers

Data Connectors (MCP)

- Snowflake, Databricks, BigQuery

What is Variance Analysis?

Variance analysis compares **budgeted** (planned) figures to **actual** results and decomposes the differences into actionable drivers. It is the core analytical task in FP&A (Financial Planning & Analysis).

Why It Matters

- Every public company does it quarterly
- Boards and investors ask "why did we miss?"
- Drives re-forecasting and capital allocation
- Required for SOX internal controls

Key Decompositions

- **Revenue**: volume vs. price vs. mix
- **COGS**: volume vs. unit cost
- **SG&A**: headcount vs. rate vs. discretionary
- **Operating income**: revenue variance + cost variance

Revenue variance = **Volume effect** + **Price effect** + **Mix effect**

Variance Analysis: Example Data

Scenario: You are an FP&A analyst at a consumer products company. Q1 actuals just closed. The CEO wants to know why operating income missed budget by $1.3M.

	Budget	Actual	Variance	$ Var
Revenue				
Units sold	100,000	95,000	−5,000	
Avg price	$50.00	$51.00	+$1.00	
Total Revenue	*$5,000,000*	*$4,845,000*		*($155,000)*
Cost of Goods Sold				
Unit cost	$30.00	$32.00	+$2.00	
Total COGS	*$3,000,000*	*$3,040,000*		*($40,000)*
Gross Profit	*$2,000,000*	*$1,805,000*		*($195,000)*
SG&A				
Salaries (50 FTEs @ $15K/mo)	$750,000	$780,000		($30,000)
Marketing	$500,000	$575,000		($75,000)
Rent & facilities	$200,000	$200,000		—
Total SG&A	*$1,450,000*	*$1,555,000*		*($105,000)*
Operating Income	**$550,000**	**$250,000**		**($300,000)**

Unfavorable variances shown in parentheses. Data is simplified for illustration.

Decomposing the Variances

Using the Plugin: `/finance:variance-analysis`

With the finance plugin installed, you type one command and provide the data:

Prompt

`/finance:variance-analysis`

"Here is our Q1 budget vs. actuals spreadsheet. Decompose the $300K operating income miss into volume, price, cost, and discretionary spending drivers. Produce a waterfall chart and a summary memo for the CFO."

What the Plugin Does

1. **Skill activates**: domain knowledge about variance decomposition formulas
2. **MCP connector** pulls data (or reads the uploaded spreadsheet)
3. **Decomposes** revenue into volume + price; COGS into volume + rate
4. **Generates** waterfall chart (budget → adjustments → actual)
5. **Writes** CFO-ready memo in Word format with tables and chart

This is one slash command replacing what typically takes an FP&A analyst 2–4 hours.

The "SaaSpocalypse": Market Reaction to Plugins

On January 30, 2026, Anthropic released 11 open-source plugins for Claude. Within days, **$285 billion** in market cap evaporated from software, legal tech, and financial services stocks.

Hardest-Hit Stocks

Company	Drop
LegalZoom	−20%
Thomson Reuters	−16%
RELX (LexisNexis)	−14%
Wolters Kluwer	−13%
Xero (accounting)	worst day since 2013
Intuit	> −10%
Salesforce	−7%
ServiceNow	−7%
Adobe	−7%
GS Software Basket	−6%
Indian IT (Infosys, TCS, . . .)	−6 to 8%

Why It Happened

- Plugins showed AI could replicate *core workflows* of specialized enterprise software
- Legal plugin: contract review, NDA triage, compliance checks
- Finance plugin: close management, reconciliation, variance analysis
- **No proprietary code**—just markdown instructions + database connectors
- Investors asked: "Why pay $50K/yr for software when a plugin does it?"

The Counterargument

- Plugins are "research preview"—not production-ready

Summary

Claude Code

- General-purpose agent
- LLM + Agent Logic + Tools
- Works out of the box

Skills

- Specialize Claude Code
- System prompt + scripts
- Easy to create and modify

Plugins

- Package and share skills
- Bundle multiple components
- Install from marketplaces

All AI customization is prompt engineering

Skills, plugins, Custom GPTs, Copilot instructions, `.cursorrules`—same pattern, different platforms